Penerapan *Digital Signature* dengan QR Code Untuk Verifikasi Dokumen Transkrip Akademik

ABSTRAK

Dalam perkembangan teknologii yang begitu cepat, pemanfaatan jaringan internet meningkat pesat juga. Sehingga kejahatan dalam pemalsuan maupun penyadapan data tidak dapat dipungkiri. Salah satu dokumen penting yang sering dilakukan modifikasi atau pemalsuan adalah transkrip akademik. ditambah dengan permasalahan yang dimana dalam setiap pengecekan dokumen membutuhkan waktu yang lama. Oleh karena itu, banyak instansi yang membutuhkan aplikasi yang dapat menjamin keamanan dan keaslian sebuah dokumen sehingga menghindari terjadinya duplikat maupun modifikasi. Dan supaya setiap instansi yang akan melakukan pengecekan keaslian sebuah dokumen tidak perlu menunggu waktu yang lama untuk mendapatkan informasi yang diinginkan. Sistem pengamanan yang diterapkan ialah penerapan digital signature menggunakan metode RSA. sehingga dalam melakukan verifikasi waktu yang diperlukan akan lebih efektif dan efisien. Dengan adanya kemudahan tersebut, maka authentication dan data integrity merupakan hal yang sangat penting untuk menjaga kerahasiaan dan keamanan data dokumen transkrip akademik dari pihak tidak bertanggung jawab yang turut berkomunikasi guna memanfaatkan data untuk kepentingan pribadi. Pada permasalahan tersebut adapun cara untuk melakukan tindakan pencegahan yaitu dengan mengubah pesan menjadi sebuah kode. Ilmu pengetahuan yang dapat diterapkan untuk menjaga authentication dan data integrity tetap dalam keadaan aman yaitu kriptografi pada digital signature.

Hasil penelitian ini adalah sistem digital signature untuk memverifikasi surat keterangann keaslian dokumen transkrip akademik dengan penerapan metode RSA (R. Rivest, A. Shamir, dan L. Adleman). Pemanfaatan algoritma SHA-1 akan melindungi pesan saat proses distribusi yaitu dengan menghitung nilai hash pada dokumen transkrip akademik dan algoritma RSA dapat memberikan jaminan othentikasi pengirim maupun penerima dokumen.

Kata Kunci: *Transkrip Akademik, Tanda tangan digital, SHA-1*

1. **Judul Penelitian:**
   Penerapan *Digital Signature* dengan QR Code Untuk Verifikasi Dokumen Transkrip akademik

2. **Ruang Lingkup:**
   - Pemograman Internet
   - Dasar Pemograman

3. **Tujuan:**
   Dalam perancangan tugas akhir terdapat beberapa tujuan diantaranya yaitu:
   1. Mengurangi pemalsuan dokumen transkrip akademik
   2. Membantu proses verifikasi dokumen Transkrip akademik
   3. Meningkatkan efektivitas dan efisiensi proses tanda tangan

4. **Latar Belakang:**

   Teknologi informasi memiliki dampak yang sangat besar bagi kehidupan manusia hampir di semua kalangan masyarakat. Dibalik berkembang pesatnya teknologi informasi terdapat sistem yang membuat era manual menjadi lebih digital. Seiring berkembangnya teknologi informasi, sering terjadi penyalahgunaan dokumen terutama dokumen cetak. Dokumen merupakan salah satu data yang sangat penting karena merupakan sumber informasi yang dibutuhkan oleh individu, kelompok, organisasi, lembaga dan negara. Tanpa dokumen, seseorang kehilangan informasi yang akan digunakan untuk kebutuhan di masa mendatang. Pemalsuan dokumen mudah dilakukan oleh oknum yang tidak bertanggung jawab dengan meniru bentuk dan isi dokumen tersebut. Salah satu teknologi informasi yang dapat mengurangi pemalsuan dokumen adalah penggunaan kode QR (Quick Response Code) untuk mengidentifikasi dan memverifikasi dokumen.

   Verifikasi dokumen adalah proses verifikasi keaslian dan keabsahan dokumen yang diterima. Di era digital, otentikasi dokumen lebih mudah dengan teknologi kode QR. Kode QR adalah kode matriks dua dimensi yang dapat menyimpan informasi berupa teks, URL, atau informasi lainnya. Saat mensertifikasi dokumen, kode QR digunakan sebagai tanda tangan digital yang menautkan dokumen asli ke dokumen elektronik.

   Verifikasi dokumen berbasis kode QR adalah solusi inovatif yang menyederhanakan proses verifikasi dokumen. Metode ini lebih efisien dan efektif daripada metode kontrol dokumen tradisional. Otentikasi dokumen berbasis kode QR telah diterapkan di berbagai bidang seperti pendidikan, bisnis dan manajemen. Dengan autentikasi dokumen berbasis kode QR, proses verifikasi dokumen menjadi lebih cepat, mudah, dan efisien.

5. **Rumusan Masalah Dan Batasan Masalah:**

   5.1.Rumusan Masalah

   Rumusan masalah pada tugas akhir ini adalah sebagai berikut:
   1. Bagaimana merancang dan membuat sistem penerapan *Digital signature* berbasis QR Code?
   2. Bagaimana Analisa hasil perancangan *website*?

   5.2.Batasan Masalah

   Dalam pelaksanaan dan pembuatan penelitian ini, ada beberapa batasan masalah yang dibatasi oleh peneliti sebagai berikut:
   - Informasi Web yang dibuat pada tugas akhir ini hanya menampilkan data primer mengenai dokumen transkrip akademik dan data sekunder berupa pengujian sistem yang dilakukan oleh sekolah

- Web berfokus pada proses pembuatan kode signature dan proses verifikasi dokumen transkrip akademik
- Web hanya berfokus pada dokumen dengan format PDF.

6. Tinjauan Pustaka:

6.1.Penelitian yang Pernah Dilakukan

Pada penelitian sebelumnya, telah dilakukan oleh **Orlando Yosefyius Pardamean Naibaho, Nurcahyo Budi Nugroho, Nur Yanti Lumban Gaol, 2021,** yaitu penerapan *digital signature* menggunakan metode DSA untuk verifikasi surat keterangan keaslian ijazah di SMA RK Swasta Lubuk Pakan. Prinsipnya yaitu untuk menjamin keamanan sehingga menghindari terjadinya duplikat maupun modifikasi ijazah. Penggunaan sistem pengamanan yang diterapkan ialah penerapan digital signature menggunakan metode DSA.

Dalam penelitian yang dilakukan oleh peneliti, sistem keamanan berpusat pada dokumen akademik SMA RK swasta Lubuk Pakan yang difokuskan pada ijazah. Informasi tersebut dikemas dalam bentuk artikel dan divisualkan pada web yang dihasilkan. Pada web yang dihasilkan dari penelitian peneliti terdapat tampilan yang dapat membantu user untuk pembentukan *digital signature* surat keterangan keaslian ijazah tersebut dan kemudian dikonversikan ke QR Code.[1]

6.2.Teori Penunjang

6.2.1.Sistem Informasi

Sistem adalah jaringan untuk melakukan beberapa aktivitas atau mencapai tujuan tertentu. Pada saat yang sama, informasi adalah data yang diolah dalam bentuk yang penting bagi penerimanya dan memiliki nilai nyata atau yang dirasakan dalam pengambilan keputusan saat ini atau masa depan (Widyanti dan Wardati, 2013). Jadi, sistem informasi adalah kumpulan data yang diolah menjadi bentuk yang lebih berguna dan bermakna bagi penerimanya (Mohammad Subhan, 2012). Salah satu bentuk visualisasi sistem informasi adalah situs web (website), yang merupakan alamat (URL), yang merupakan tempat penyimpanan data dan informasi berdasarkan topik tertentu, dan URL itu sendiri adalah sarana untuk menentukan lokasi sistem Informasi. Sistem informasi tentang web server. [2]

6.2.2.Tanda Tangan Digital

Semakin banyak orang dan organisasi menggunakan dokumen digital daripada kertas dalam operasi bisnis sehari – hari mereka. Mengurangi ketergantungan pada dokumen kertas untuk melindungi lingkungan. Tanda tangan digital mendukung perubahan ini dengan memastikan validitas dan keaslian dokumen digital.[3]

Secara umum, tanda tangan digital merupakan model matematis yang unik untuk mengidentifkasi seseorang di dunia digital[4]. Tanda tangan digital adalah stemple yang diautentikasi secara elektronik terenkripsi pada data digital seperti email, makro, atau dokumen elektronik. Tanda tangan menegaskan bahwa Informasi tersebut berasal dari penanda tangan dan belum diubah[3].

Tanda tangan digital digunakan untuk memberikan kekuatan dan pengaruh hukum terhadap dokumen elektronik dan transaksi elektronik. Seperti yang tertuang dalam Pasal 11 UU ITE. Dokumen PDF tanda tangan digital dapat ditandatangani menggunakan Adobe Reader DC (gratis). Sehingga seseorang dapat membuat dokumen hukum secara digital tanpa harus menggunakan kertas lagi. TTD juga dapat digunakan untuk login dan melakukan transaksi di aplikasi (e-government, e-banking, e-commerce dan e-services lainnya). Sayangnya, belum ada aplikasi yang siap menggunakan sertifikat digital ini. Aplikasi yang

menggunakan sertifikat digital saat ini sedang dibuat di layanan publik. Diharapkan akan segera diimplementasikan pada tahun2017 [4].

6.2.3.Sertifikat Digital

Untuk membuat tanda tangan digital sertifikat tanda tangan diperlukan untuk bukti identitas sendiri. Jika seseorang mengirim makro atau juga dokumen yang ditandatangani secara digital Kirim sertifikat dan kunci publik. Sertifikat menerbitkan otoritas sertifikat (CA), seperti SIM dan dapat dicabut. Sertifikat biasanya berlaku selama satu tahun setelah tanda itu tangan perlu diperbarui atau dapat dilanjutkan sertifikat penandatanganan baru [3].

6.2.4.Kriprografi

Menurut Schneider [5], kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta otentik data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya. Ada empat tujuan ilmu kriptografi menurut Wahana Komputer [6] yaitu :

a) Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi informasi dari siapa pun kecuali yang memiliki otoritas.
b) Integrasi data, berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integrasi data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan substitusi data lain ke dalam data yang sebenarnya.
c) otentikasi, berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diotentikasi keaslian isi datanya, waktu pengiriman, dan lainlain.
d) *Non-Repudiation*, yang berarti begitu pesan terkirim, tidak akan dapat dibatalkan atau tidak dapat disangkal.

6.2.5.Fungsi Hash

Fungsi *Hash* sering disebut dengan fungsi *Hash* satu arah (*one-way function*). *Message digest*, *fingerprint*, fungsi kompresi dan *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan Panjang variabel dan mengubahnya ke dalam urutan biner dengan Panjang yang tetap. Fungsi *Hash* biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benarbenar berasal dari orang yang diinginkan. [7]

6.2.6.Website

Website adalah keseluruhan halaman-halaman web
yang terdapat dalam sebuah domain yang mengandung informasi. Sebuah *website* biasanya dibangun atas banyak halaman *web* yang saling berhubungan. Hubungan antara satu halaman *web* dengan halaman *web* yang lainnya disebut dengan *hyperlink*, sedangkan teks yang dijadikan media penghubung disebut *hypertext.* Istilah lain yang sering ditemui sehubungan dengan *website* adalah *homepage*. *Homepage* adalah halaman awal sebuah domain [8]

6.2.7. QR Code

QR-Code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2dimensi yang tercetak kedalam suatu media yang lebih ringkas. QR-Code adalah barcode 2-dimensi yang diperkenalkan pertama kali oleh perusahan Jepang Denso-Wave pada tahun 1994. Barcode ini pertama kali digunakan untuk pendataan invertaris produksi suku cadang kendaraan dan sekarang sudah

digunakan dalam berbagai bidang. QR adalah singkatan dari Quick Response karena ditujukan untuk diterjemahkan isinya dengan cepat. QR-Code merupakan pengembangan dari barcode satu dimensi, QR-Code salah satu tipe dari barcode yang dapat dibaca menggunakan kamera handphone. (Rouillard, 2008).

QR-Code mampu menyimpan semua jenis data, seperti data angka/numerik, alphanumerik, biner, kanji/kana. Selain itu QR-Code memiliki tampilan yang lebih kecil daripada barcode. Hal ini dikarenakan QR-Code mampu menampung data secara horizontal dan vertikal, jadi secara otomatis ukuran dari tampilannya gambar QR-Code bisa hanya seperspuluh dari ukuran sebuah barcode. Tidak hanya itu QR-Code juga tahan terhadap kerusakan, sebab QRCode mampu memperbaiki kesalahan sampai dengan 30% tergantung dengan ukuran atau versinya. Oleh karena itu, walaupun sebagian simbol QR-Code kotor ataupun rusak, data tetap dapat disimpan dan dibaca. Tiga tanda berbentuk persegi di tiga sudut memiliki fungsi agar simbol dapat dibaca dengan hasil yang sama dari sudut manapun. (Wave, 2010).

6.2.8. Algoritma Tanda Tangan Digital

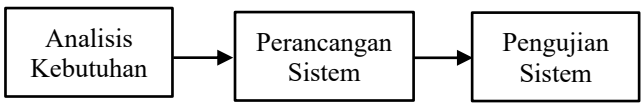
Salah satu aplikasi lain dari kriptografi kunci asimetrik adalah tanda tangan digital. Tanda tangan digital di sini bukanlah tanda tangan yang discan, melainkan suatu bilangan yang diolah secara matematis sehingga menghasilkan kesimpulan bahwa suatu dokumen masih asli atau bukan (Isnaeni, 2016:35). Dalam tanda tangan digital, dikenal tiga proses, yakni proses pembuatan kunci, proses menandatangani dokumen digital dan proses verifikasi tanda tangan digital. Proses pembuatan kunci menghasilkan kunci publik dan kunci rahasia. Kemudian kunci privat digunakan untuk menandatangani dokumen digital, sedangkan kunci publik digunakan untuk memverifikasi tanda tangan digital. Tanda tangan digital dan tanda tangan konvensional memiliki fungsi sama, yaitu otentikasi (menjamin keaslian dokumen). [9]

Beberapa algoritma tanda tangan digital yang telah dikembangkan antara lain tanda tangan digital algoritma R. Rivest, A. Shamir dan L. Adleman (RSA), metode ElGamal, dan metode kurva eliptik.

Dari ketiga algoritma yang disebutkan diatas, yang akan dibahas dalam penelitian ini yaitu algoritma R. Rivest, A. Shamir dan L. Adleman (RSA) karena langkah yang digunakan sederhana serta tingkat keamanan sangat tinggi.

7. Metodologi

Metodologi penelitian diperlukan agar penelitian disusun sedemikian rupa sehingga hasil yang diperoleh sesuai dengan tujuan penelitian. Sistem yang akan dibangun adalah sistem tanda tangan digital, yang tujuannya untuk memudahkan penggunaan tanda tangan dalam bentuk digital.



Gambar 1. Perancangan Sistem

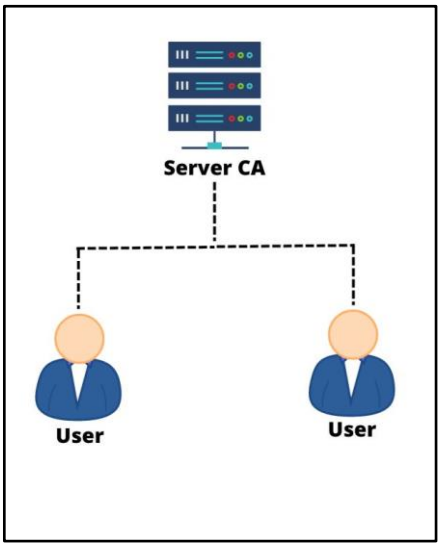
7.1. Analisa Kebutuhan

Analisis kebutuhan digunakan untuk menentukan kebutuhan yang muncul dari permasalahan yang ada, sehingga rancangan sistem yang dibangun sesuai dengan kebutuhan. Persyaratan analisis masalah yang dilakukan adalah sebagai berikut:

a) *Server* CA
   Server CA dibutuhkan untuk menyimpan data dan sertifikat dari *user* yang telah terdaftar
b) Web *Admin*
   Web *Admin* dibutuhkan untuk melakukan pendaftaran terhadap *user* yang dioperasikan oleh seorang admin.
c) Web *Public*
   Web *Public* dibutuhkan untuk menerbitkan sertifikat digital oleh *user* yang telah melakukan pendaftaran.

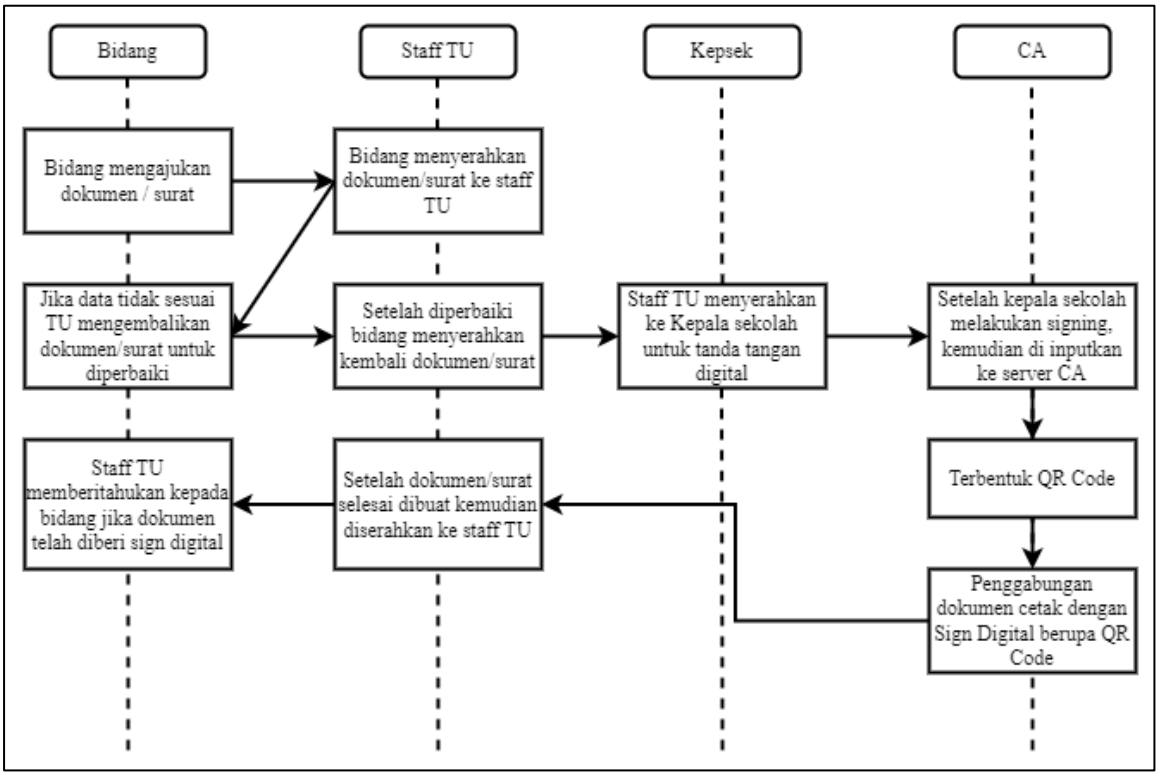
7.2. Perancangan Sistem

Dalam penelitian ini diperlukan perancangan dan rekayasa sistem sebagai acuan penelitian dan tujuannya adalah untuk menentukan desain atau diagram dari sistem yang akan dibangun. Pada tahap perancangan sistem ini terdapat dua tahap yaitu perancangan konseptual dan perancangan fisik. Berdasarkan hasil analisis kebutuhan, diagram sistem tanda tangan digital ditunjukkan pada Gambar berikut ini.



Gambar 2. Gambaran CA

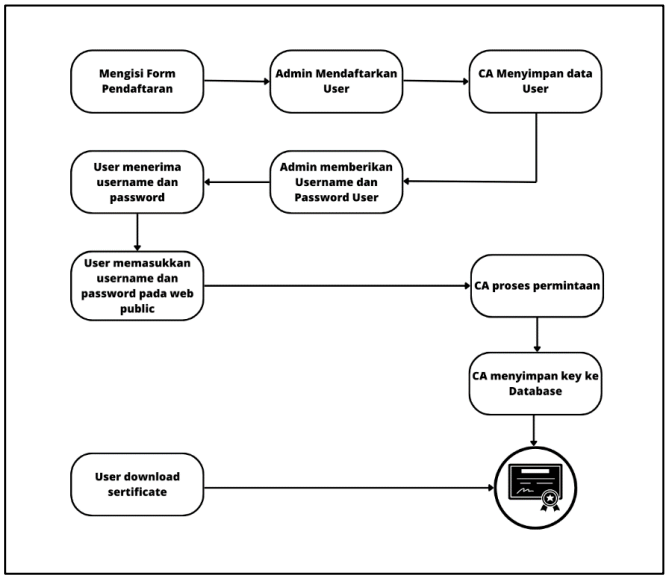
Pada tahap perancangan sistem akan dibuat gambaran arsitektur umum secara keseluruhan. Berikut adalah topologi rancangan umum sistem.



Gambar 3. Topologi rancangan umum sistem

Dari gambar 3 menjelaskan tentang alur sistem secara keseluruhan. Pengguna sistem terdiri dari bidang dan staff Tata Usaha (TU). Bidang yang terlibat dengan surat/dokumen sebelum diserahkan ke staff Tata Usaha (TU). Setelah bidang mengajukan dokumen, selanjutnya Staff TU akan menyerah ke kepala sekolah untuk proses signing. Kemudian dari kepala sekolah akan di inputkan ke server CA untuk membangun QR Code. Setelah dokumen yang diinputkan sudah dilengkapi dengan QR Code, maka akan dikirimkan ke staff tata usaha yang kemudian akan dikirimkan ke bidang.

7.2.1.Proses pernerbitan Sertifikat Digital



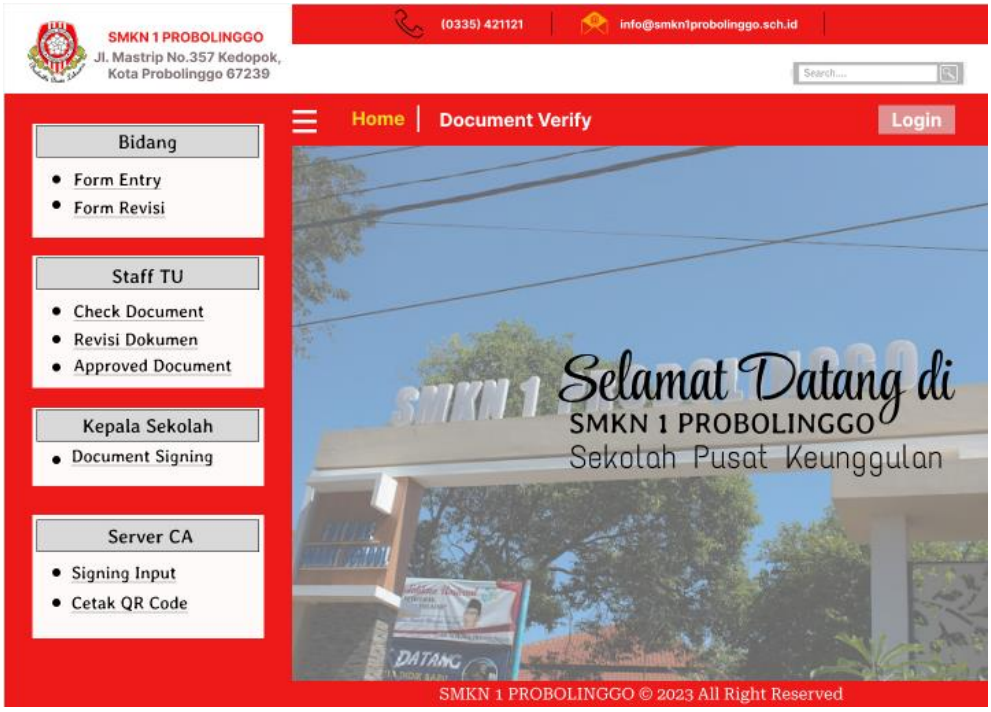
Gambar 4. Alur Proses mendapatkan Sertifikat Digital

Gambar. 4 menjelaskan bahwa bidang terlebih dahulu harus mengisi formulir permohonan untuk mendapatkan sertifikat tanda tangan digital. Setelah bidang mengisi formulir, administrator mendaftarkan pengguna di situs web administrator sistem berdasarkan informasi yang diisi pengguna di formulir. Pengguna kemudian diberikan nama pengguna dan kata sandi untuk mengunduh sertifikat digital dalam format p12 dari jaringan publik yang disediakan, dengan ketentuan bahwa pengguna hanya dapat mengunduh file p12 seperti yang ditentukan oleh administrator.

7.2.2.Perancangan Pembuatan Web

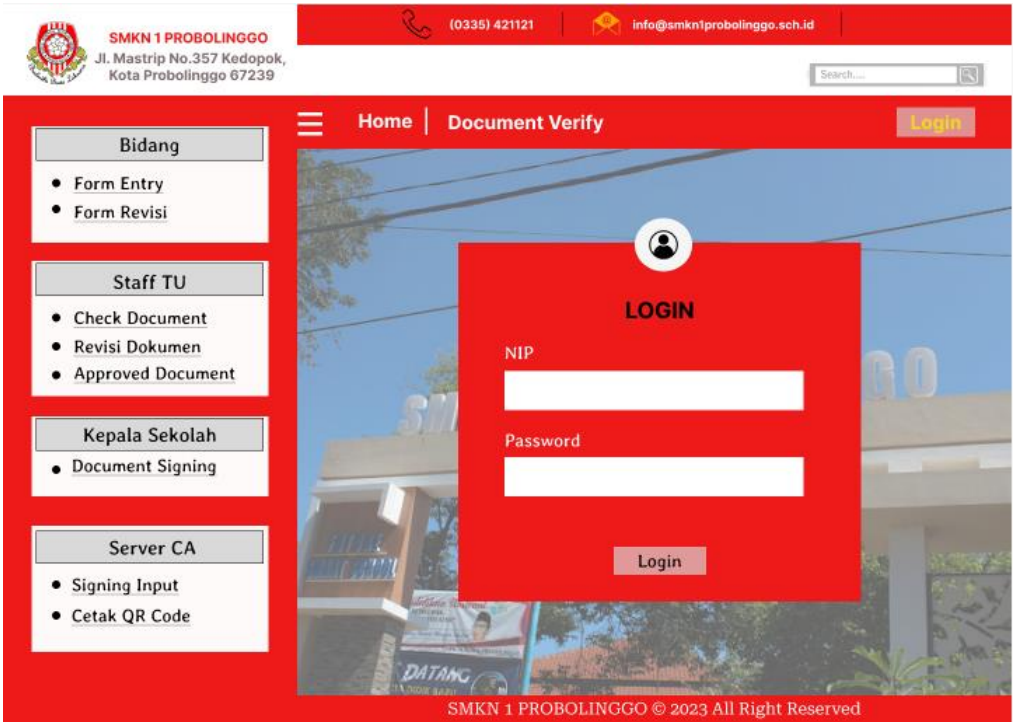
Untuk rancangan desain web tertera pada gambar 5 hingga gambar 13

Gambar. 5 merupakan tampilan halam utama yang mana nantinya ketika setiap kali web sistem dijalankan akan terdapat tampilan awal seperti pada gambar dibawah ini:



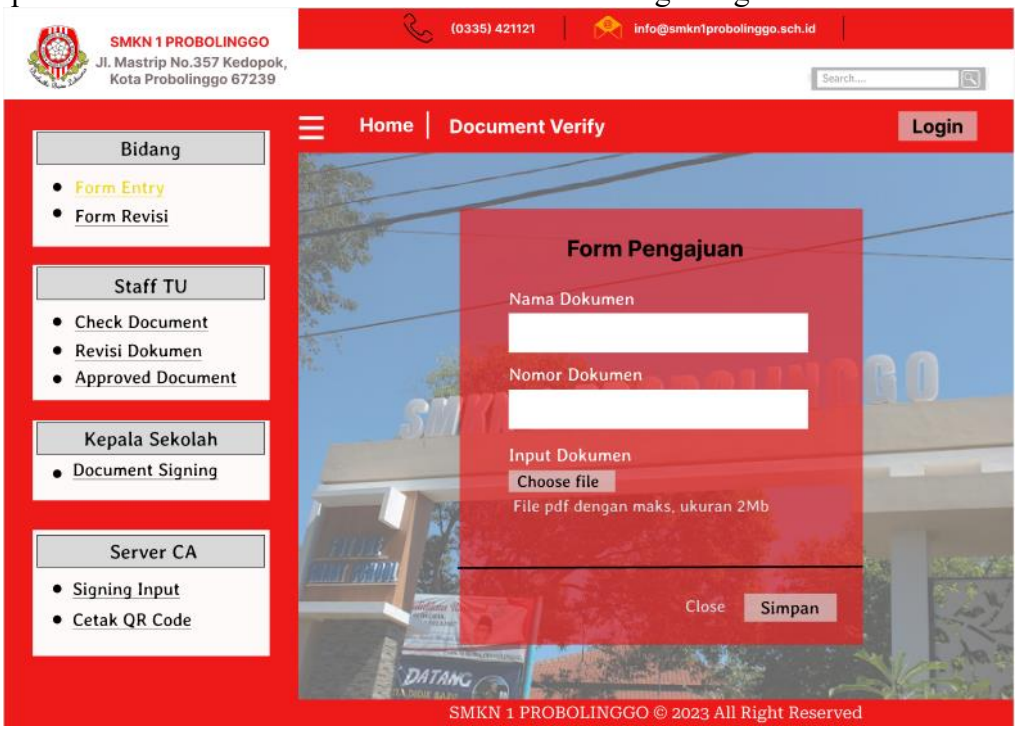
Gambar 5. Tampilan Halaman Utama

Gambar.6 merupakan tampilan menu login yang dibuat untuk membatasi akses hak akses user lain. Untuk dapat masuk ke menu – menu yang terdapat pada web, maka harus login terlebih dahulu dengan menginputkan NIP dan Password yang telah tersimpan pada database.



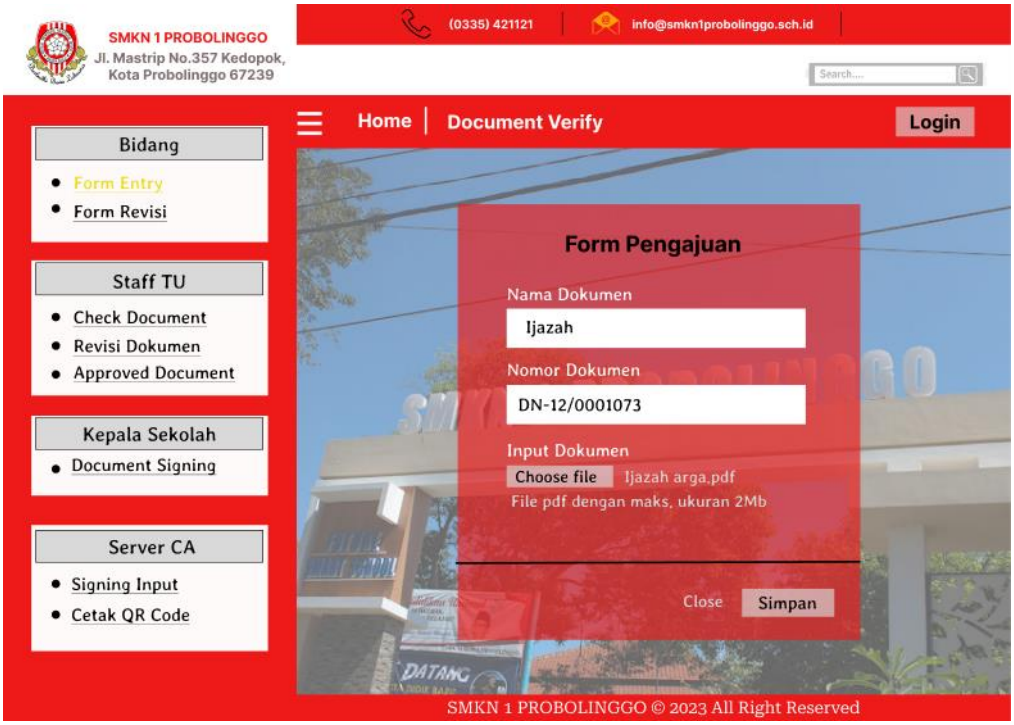
Gambar 6. Tampilan Form Login

Gambar.7 merupakan tampilan form pengajuan. Pada tampilan ini bidang dapat meninputkan data dari dokumen transkrip akademik yang akan diajukan kepada staff TU untuk kemudian diberikan tanda tangan digital.



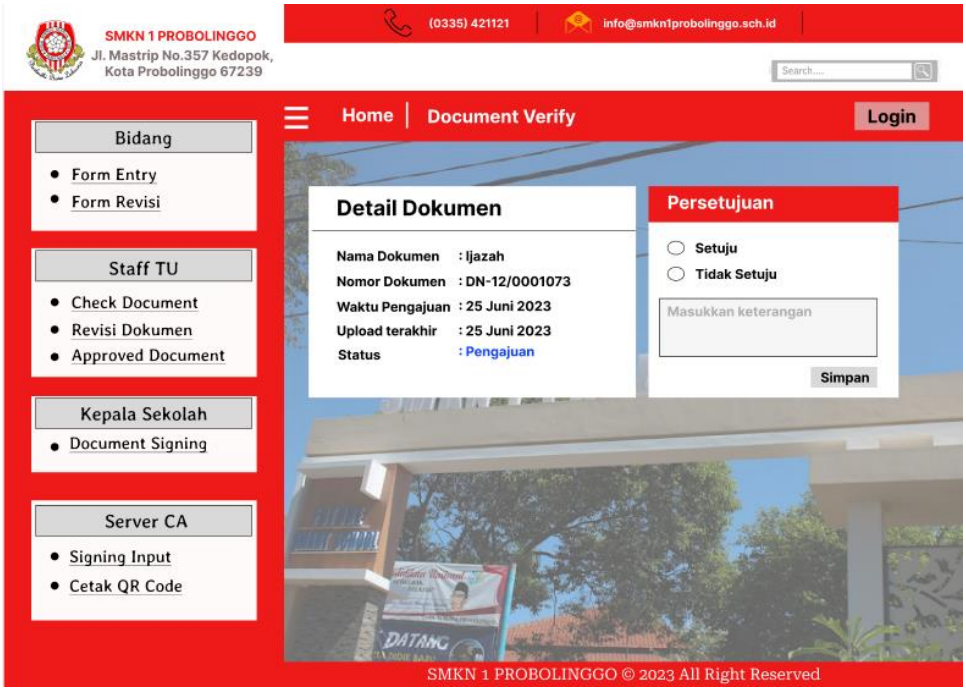
Gambar 7. Tampilan Form Pengajuan Surat

Gambar.8 merupakan tampilan form yang sudah diisi oleh bidang yang mana nantinya form tersebut akan dicek oleh staff tata usaha.



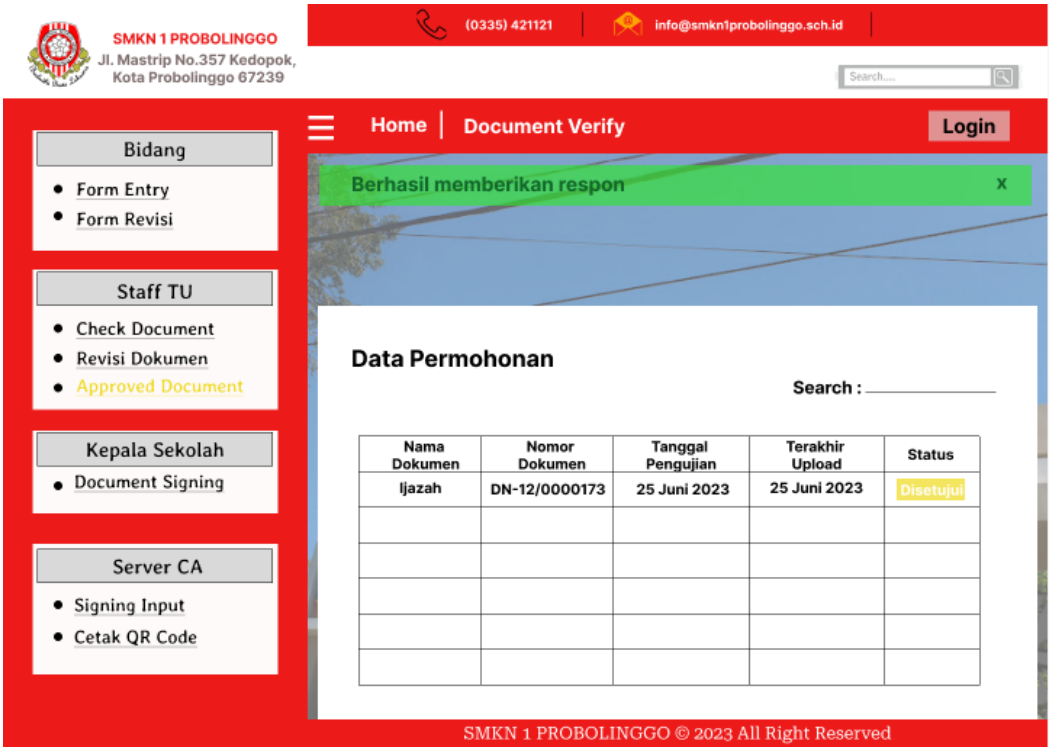
Gambar 8. Tampilan form yang sudah diisi

Gambar.9 merupakan halaman detail surat permohonan yang nantinya diakses oleh staff tata usaha. Staff tata usaha melakukan pengecekan terhadap surat permohonan, jika data tidak sesuai maka staff tata usaha mengembalikan form tersebut untuk direvisi dan jika data sudah sesuai maka staff tata usaha aka menyetujui dan akan mengirimkan ke kepala sekolah untuk diberi tanda tangan



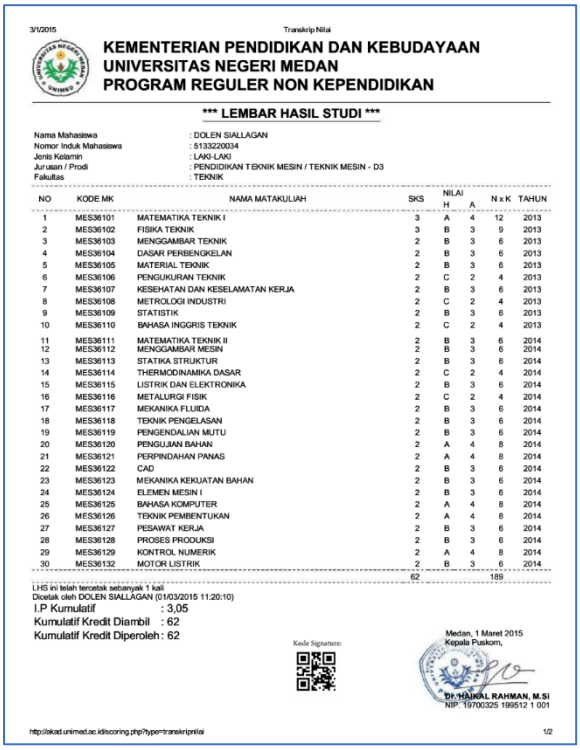
Gambar 9. Halaman Detail Surat Permohonan

Gambar.10 merupakan tampilan status berhasil memberikan respon. Tampilan ini merupakan tampilan dokumen yang sudah disetujui oleh Staff TU dan kemudian dilanjutkan untuk diberi tanda tangan digital serta pembangunan QR Code oleh server CA



Gambar 10. Status berhasil memberikan respon

Gambar. 11 merupakan contoh dokumen transkrip akademik yang sudah diberi sign digital berupa QR Code yang nantinya bidang dapat mengunduh file tersebut berupa file pdf.



3/1/2015 Transkrip Nilai

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS NEGERI MEDAN
PROGRAM REGULER NON KEPENDIDIKAN

***** LEMBAR HASIL STUDI *****

Nama Mahasiswa : DOLEN SIALLAGAN
Nomor Induk Mahasiswa : 5133220034
Jenis Kelamin : LAKI-LAKI
Jurusan / Prodi : PENDIDIKAN TEKNIK MESIN / TEKNIK MESIN - D3
Fakultas : TEKNIK

NO	KODE MK	NAMA MATAKULIAH	SKS	NILAI H	NILAI A	N x K	TAHUN
1	MES36101	MATEMATIKA TEKNIK I	3	A	4	12	2013
2	MES36102	FISIKA TEKNIK	3	B	3	9	2013
3	MES36103	MENGGAMBAR TEKNIK	2	B	3	6	2013
4	MES36104	DASAR PERBENGKELAN	2	B	3	6	2013
5	MES36105	MATERIAL TEKNIK	2	B	3	6	2013
6	MES36106	PENGUKURAN TEKNIK	2	C	2	4	2013
7	MES36107	KESEHATAN DAN KESELAMATAN KERJA	2	B	3	6	2013
8	MES36108	METROLOGI INDUSTRI	2	C	2	4	2013
9	MES36109	STATISTIK	2	B	3	6	2013
10	MES36110	BAHASA INGGRIS TEKNIK	2	C	2	4	2013
11	MES36111	MATEMATIKA TEKNIK II	2	B	3	6	2014
12	MES36112	MENGGAMBAR MESIN	2	B	3	6	2014
13	MES36113	STATIKA STRUKTUR	2	B	3	6	2014
14	MES36114	THERMODINAMIKA DASAR	2	C	2	4	2014
15	MES36115	LISTRIK DAN ELEKTRONIKA	2	B	3	6	2014
16	MES36116	METALURGI FISIK	2	C	2	4	2014
17	MES36117	MEKANIKA FLUIDA	2	B	3	6	2014
18	MES36118	TEKNIK PENGELASAN	2	B	3	6	2014
19	MES36119	PENGENDALIAN MUTU	2	B	3	6	2014
20	MES36120	PENGUJIAN BAHAN	2	A	4	8	2014
21	MES36121	PERPINDAHAN PANAS	2	A	4	8	2014
22	MES36122	CAD	2	B	3	6	2014
23	MES36123	MEKANIKA KEKUATAN BAHAN	2	B	3	6	2014
24	MES36124	ELEMEN MESIN I	2	B	3	6	2014
25	MES36125	BAHASA KOMPUTER	2	A	4	8	2014
26	MES36126	TEKNIK PEMBENTUKAN	2	A	4	8	2014
27	MES36127	PESAWAT KERJA	2	B	3	6	2014
28	MES36128	PROSES PRODUKSI	2	B	3	6	2014
29	MES36129	KONTROL NUMERIK	2	A	4	8	2014
30	MES36132	MOTOR LISTRIK	2	B	3	6	2014
			62			189	

LHS ini telah tercetak sebanyak 1 kali
Dicetak oleh DOLEN SIALLAGAN (01/03/2015 11:20:10)
I.P Kumulatif : 3,05
Kumulatif Kredit Diambil : 62
Kumulatif Kredit Diperoleh : 62

Kode Signature:

Medan, 1 Maret 2015
Kepala Puskom,

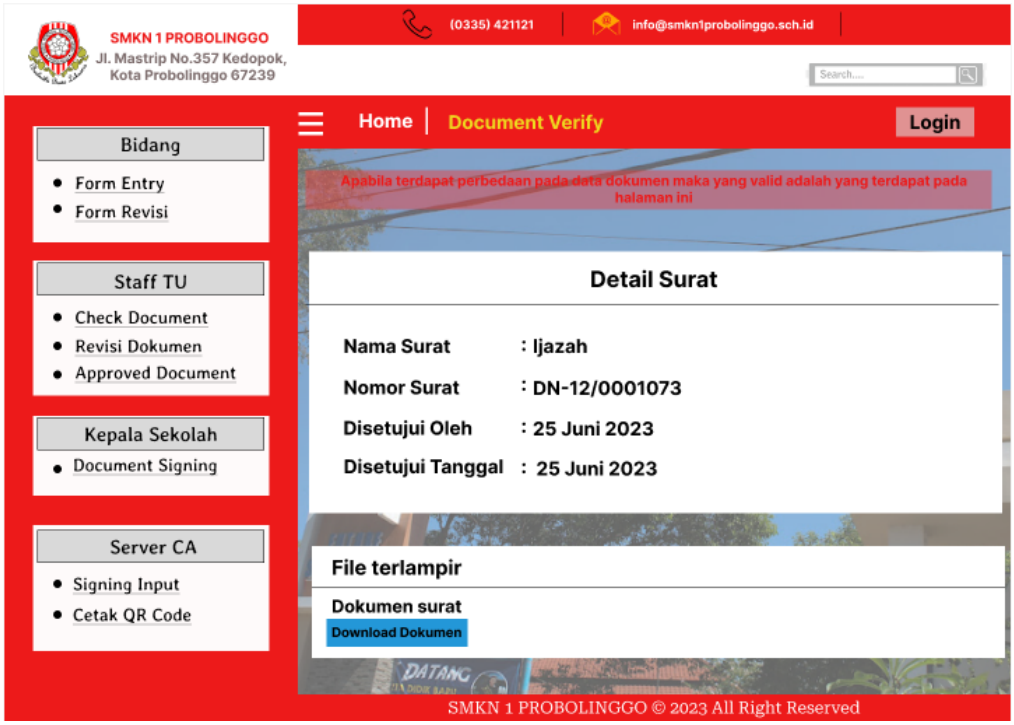
DR. HAIKAL RAHMAN, M.SI
NIP. 19700325 199512 1 001

http://akad.unimed.ac.id/scoring.php?type=transkripnilai 1/2

Gambar 11. Output Sistem Digital Signature

Gambar 12. Scan QR Code

Pengecekan dengan memasukkan digit kode verifikasi dari hasil scan pada google lens atau barcode scanner ke form verifikasi dapat dilihat sebagai berikut:



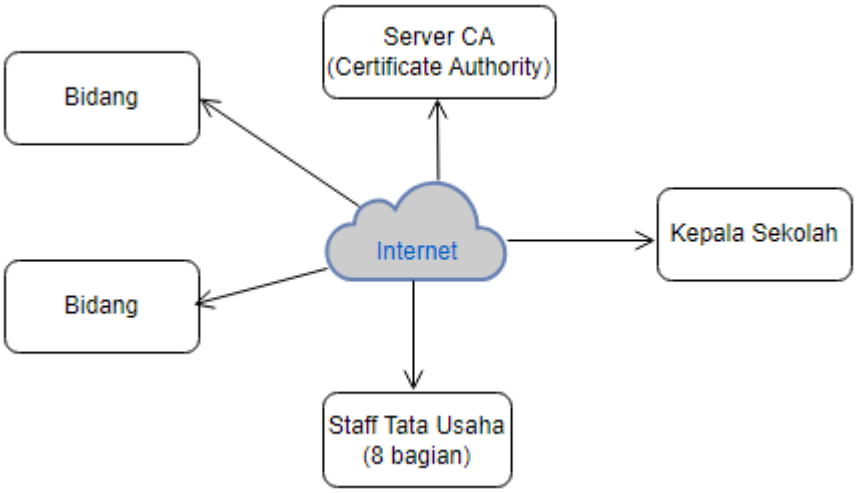
Gambar 13. Verifikasi keaslian Transkrip Nilai

Jika kode verifikasi dan layanan yang dimasukkan sudah benar dan tercatat, maka keaslian Transkrip Akademik asli tetap terjaga dengan menampilkan keterangan setail surat dan menunjukkan sertifikat keaslian ijazah. Jika nomor konfirmasi dan kode layanan yang dimasukkan salah, sistem akan menampilkan informasi “Sertifikat tidak asli” dan form konfirmasi kembali.

7.3. Pengujian Sistem

Pengujian sistem adalah elemen kritis dari jaminan kualitas sitem dan mempresentasikan kajian pokok dari spesifikasi, desain dan pengkodean. Pengujian dilakukan untuk memenuhi persyaratan kualitas sistem yang dibagun, dengan cara membuat skenario pengujian dan mengeksekusi program berdasarkan skenario tersebut untuk mencari kesalahan kode program, lalu melakukan verifikasi terhadap sistem untuk melihat kesesuaian fungsi yang ada pada sistem tersebut.[10]. Adapun tahapan – tahapan pengujian sistem sebagai berikut.

7.3.1. Topologi Pengujian Sistem



Gambar 14. Topologi pengujian sistem

Dari topologi diatas dapat dilihat web server yang digunakan dalam penelitian ini yaitu menggunakan web server internet karena web server internet dapat digunakan oleh semua yang orang yang memiliki akses ke perangkat yang terhubung ke internet. Kemudian web server dapat diakses oleh bidang untuk menginputkan data pada dokumen yang akan diberi sign digital berbasis QR Code. Setelah itu web server juga digunakan oleh staff tata usaha untuk memeriksa data yang telah diinputkan oleh bidang. Jika data tidak sesuai atau terdapat format yang salah terhadap data maka staff tata usaha mengembalikan kembali ke bidang. Setelah data diperiksa dan siap untuk diberi sign digital maka staff TU memberikan akses ke kepala sekolah untuk memberi sign pada dokumen tersebut yang kemudian nati diteruskan ke server CA untuk membangun QR Code pada dokumen yang terverifikasi.

Setelah perancangan dan pembuatan sistem, maka langkah selanjutnya yaitu melakukan pengujian dan analisa terhadap sistem yang telah dibuat. Pengujian ini dilaksanakan untuk mengetahui apakah sistem sudah bekerja sesuai dengan rancangan yang telah direncanakan. Pengujian ini terdiri dari:

a. Program berjalan lancar
b. Kenyamanan pengguna web

Kemudian untuk metode pengujian yang digunakan pada penelitian ini adalah metode *Black Box*. Metode pengujian *Black Box* adalah metode pengujian yang menguji fungsionalitas sistem (wibisono & Baskoro, 2002). Metode tersebut dilakukan untuk memastikan apakah fungsi berjalan dengan benar jika diberikan masukan yang bervariasi.

7.3.2. Skenario Pengujian

Pada penelitian ini terdapat beberapa hal yang akan diuji diantaranya, Integrasi tanda tangan digital dengan QR Code, Server Certificate Authority, Performansi sistem. Parameter yang akan diuji diantaranya, lama waktu yang diperlukan oleh sistem ketika diberikan inputan berberapa macam ukuran dokumen serta berapa banyak bidang dan staff TU yang menangani. Kemudian beberapa hal yang akan diuji tersebut ditampilkan dalam bentuk tabel sebagai berikut.

Tabel 1. Integrasi Tanda Tangan Digital berupa QR Code

Ukuran Dokumen	Signing (time)	Verification (time)
100Kb		
250Kb		

Pengujian pada tabel.1 yaitu pengujian untuk melihat berapa lama server membuat QR code dengan berbagai macam ukuran dokumen yang berawal dari proses signing hingga verification.

Tabel 2. Server CA

Ukuran Dokumen	Server Generate	Server Verified
100Kb		
250Kb		
…		
n		

Pengujian pada tabel.2 yaitu pengujian untuk server CA yang mana parameter yang diuji yaitu jika ukuran dokumen 100kb berapa lama server generate bekerja dan berapa lama server verified bekerja. Kemudian dilakukan pengujian untuk beberapa macam ukuran dokumen transkrip akademik.

Tabel 3. Perfomansi Sistem yang digunakan oleh bidang

Jumlah Bidang	Total Time Process
1 bidang	
3 bidang	
…	
n	

Pengujian pada tabel.3 yaitu pengujian yang dilakukan untuk performansi sitem yang digunakan oleh bidang. Parameter yang diuji pada tabel ini yaitu total waktu yang diperlukan untuk mengakses sebuah sistem jika terdapat 1 bidang yang menangani. Kemudian dilakukan uji coba juga berapa lama performasi sistem jika ditangani oleh lebih dari satu bidang.

Tabel 4. Perfomansi Sistem yang digunakan oleh Staff Tata Usaha

Jumlah Bidang	Total Time Process
1 Staff	
3 Staff	
…	
n	

Pengujian pada tabel.4 yaitu pengujian yang dilakukan untuk performansi sitem yang digunakan oleh Staff tata usaha. Parameter yang diuji pada tabel ini yaitu total waktu yang diperlukan untuk mengakses sebuah sistem jika terdapat 1 staff tata usaha yang menangani. Kemudian dilakukan uji coba juga berapa lama performasi sistem jika ditangani oleh lebih dari satu staff tata usaha.

8. Hasil yang diharapkan

Hasil yang diharapkan yaitu web sistem untuk input data user dan hasil kode signature berupa QR Code yang dapat dijadikan pedoman bagi admin untuk mengetahui dokumen tersebut asli atau palsu, sebagai upaya untuk mengurangi pemalsuan dokumen transkrip akademik dengan divisualkan dalam bentuk digital signature berbasis QR Code. Selain itu, hasil dari proyek akhir yang akan dibuat berupa QR Code dengan tujuan untuk mengurangi pemalsuan dokumen serta mempermudah dalam melakukan pengecekan data pada transkrip akademik. Sistem yang digunakan dalam pembuatan QR Code ada beberapa algoritma dalam pembentukan tanda tangan digital, diantaranya: RSA (Rivest-ShamirAdleman) Signature Scheme, ElGamal Signature Scheme, Schnorr Signature Scheme, dan DSA (Digital Signature Algorithm). Pada hasil proyek akhir ini saya menggunakan algoritma RSA karena langkah yang digunakan sederhana serta tingkat keamanan sangat tinggi. algoritma ini membutuhkan penambahan fungsi hash pada proses penandatanganan yang akan digunakan untuk mereduksi pesan asli menjadi suatu message digest (nilai hash) yang berupa string pendek dengan panjang tetap sesuai ketentuan masing-masing. Dengan begitu hasil proyek akhir QR Code ini akan menghasilkan informasi dari dokumen Transkrip Akademik. Dengan dilakukan scan QR Code klta dapat melihat informasi apakah dokumen tersebut asli atau palsu.

9. Relevansi

Pengerjaan penelitian ini relevan dengan Embedded Digital Signature-based QR-Code & Its Implementation of eSign Document untuk membantu mempermudah sebuah instansi meningkatkan efektifitas dan efisiensi proses tanda tangan serta dapat memastikan keabsahan dari dokumen bertanda-tangan dengan bantuan teknologi QR Code. Dengan output dalam bentuk Web, sehingga admin dapat dengan mudah mengaplikasikan dan input data sesuai dengan yang tertera pada web.

10. Jawal Kegiatan

Proses tugas akhir ini akan dilaksanakan sesuai dengan jadwal kegiatan yang tertera pada tabel.5 sebagai berikut: