Perancangan Sistem Tanda Tangan Digital (*Digital Signature*)

Muh. Taufiqurrahman[1)], Irawan[2)], Irfan Syamsuddin[3)]
[1,2,3]Program Studi Teknik Komputer dan Jaringan, Jurusan Teknik Elektro, Politeknik Negeri Ujung Pandang
Makassar, Indonesia
taufiqr29@poliupg.ac.id
irawan@poliupg.ac.id
irfans@poliupg.ac.id

Abstrak

Tanda tangan digital mampu mengidentifikasi pengirim dan membuktikan keaslian dari pemilik dokumen digital yang memudahkan pihak yang melakukan perjanjian untuk menandatangani dokumen digital. Namun, pada saat pengiriman dokumen digital melalui internet sangat rentan terjadinya penyadapan sehingga dibutuhkan sebuah sistem yang dapat menerbitkan sertifikat digital yang digunakan dalam proses penanda tanganan dokumen digital untuk memverifikasi dokumen pada saat pertukaran data melalui internet. Sistem dirancang dengan menggunakan perangkat lunak EJBCA sebagai Server RootCA. Adapun proses yang dilakukan untuk menerapkan sistem tanda digital, yaitu penerbitan sertifikat digital, penandatanganan dokumen digital, dan verifikasi dokumen. Hasil dari penelitian ini berupa Server CA, web admin dan web *public*. Adapun *file* sertifikat yang dihasilkan oleh sistem dapat digunakan untuk menanda tangani beberapa *file* dokumen digital seperti *file* Doc, PDF, dan Email.

Keywords: Tanda tangan digital, sertifikat digital, dokumen digital

I. PENDAHULUAN

Tanda tangan digital (*digital signature*) merupakan sebuah skema matematis yang secara unik mengidentifikasikan pengirim dan membuktikan keaslian dari pemilik sebuah pesan atau dokumen digital sehingga sebuah tanda tangan digital menjadi bukti bahwa sebuah pesan atau dokumen yang diterima berasal dari pengirim yang telah diketahui [1].

Tanda tangan digital biasanya digunakan pada penandatanganan surat perjanjian antara pihak yang melakukan perjanjian yang tidak dapat bertemu langsung sehingga dokumen tersebut dikirim melalui internet [2].

Namun, pada saat proses pengiriman dokumen digital melalui internet sangat rentan terhadap kemungkinan modifikasi sehingga sulit membuktikan keaslian dokumen tersebut [3]. Oleh karena itu dibutuhkan sebuah sistem untuk membuktikan keaslian identitas pengirim dan isi dokumen digital atau pesan yang dikirim [1].

Berdasarkan masalah yang disebutkan maka dibuat sebuah sistem tanda tangan digital yang dapat menerbitkan sertifikat digital sebagai sarana penanda tanganan dokumen digital yang mampu menjamin keaslian dokumen digital atau pesan yang dikirim melalui internet.

II. KAJIAN LITERATUR

a. Tanda Tangan Digital

Semakin banyak orang dan organisasi yang memilih menggunakan dokumen digital daripada dokumen kertas untuk melakukan transaksi sehari-hari. Dengan menurunkan ketergantungan pada dokumen kertas sehingga dapat melindungi lingkungan. Tanda tangan digital mendukung perubahan ini dengan memberikan jaminan tentang validitas dan keaslian dokumen digital [4].

Secara garis besar Tanda Tangan Digital adalah sebuah skema matematis yang memiliki keunikan dalam mengidentifikasikan seorang (subjek hukum) di dunia digital [5].

Tanda tangan digital adalah stempel otentik elektronik yang dienkripsi pada informasi digital seperti pesan email, makro, atau dokumen elektronik. Tanda tangan mengonfirmasi bahwa informasi berasal dari penanda tangan dan belum diubah [4].

Tanda Tangan Digital digunakan untuk memberikan kekuatan hukum dan akibat hukum yang sah pada dokumen elektronik dan transaksi elektronik. Seperti yang tercantum pada pasal 11 UU ITE. Tanda Tangan Digital dapat menandatangani dokumen PDF dengan menggunakan *Adobe Reader DC* (*free*). Sehingga seseorang dapat membuat dokumen legal digital, tanpa harus menggunakan kertas lagi. TTD juga dapat digunakan untuk *login* dan bertransaksi pada aplikasi (*eGovernment, eBanking, eCommerce,* dan *eServices* lainnya). Sayangnya belum ada aplikasi yang siap menggunakan sertifikat digital ini. Aplikasi yang dapat menggunakan sertifikat digital sedang dalam proses pembuatan oleh layanan publik. Diharapkan pada tahun 2017 segera digunakan [5].

b. Sertifikat Digital

Untuk membuat sebuah tanda tangan digital diperlukan sertifikat tanda tangan, yang membuktikan identitas seseorang. Saat seseorang mengirim makro atau dokumen yang ditandatangani secara digital, juga akan mengirim sertifikat dan kunci *public*. Sertifikat dikeluarkan oleh otoritas sertifikasi (CA) dan seperti surat izin mengemudi, dan dapat dicabut. Sertifikat biasanya berlaku selama satu tahun, setelah itu, penanda tangan harus memperbaharui, atau dapat mengambil sertifikat tanda tangan yang baru [4].

c. Certificate Authority (CA)

Certificate Authority atau disingkat CA adalah lembaga yang menerbitkan sertifikat digital, menandatangani sertifikat untuk memverifikasi validitasnya dan melacak sertifikat yang telah dicabut atau kedaluwarsa [5].

CA merupakan entitas yang serupa dengan notaris publik. Entitas ini menerbitkan sertifikat digital, menandatangani sertifikat untuk memverifikasi validitasnya dan melacak sertifikat yang telah dicabut atau kedaluwarsa [4].

Komponen-komponen pada CA [6] :

a) *RootCA* : Suatu *RootCA* adalah CA dengan level tertinggi yang menandatangani sertifikatnya sendiri (*self-signed certificate*), dan biasanya disebut *Trusted Root.*
b) *Registration Authority* (RA) : RA mempunyai fungsi-fungsi yang sesuai dengan CP/CPS, antara lain menerima permintaan sertifikat dan memvalidasinya, mengirim permintaan ke CA, menerima sertifikat yang diterbitkan oleh CA dan mengirim sertifikat pada *user*/entitas yang benar. RA khususnya bermanfaat untuk skala aplikasi *public key infrastructure* berada di lokasi yang berbeda secara geografi.
c) *Certificate Revocation List* (CRL) : CRL digunakan untuk membuat daftar sertifikat yang sudah dibatalkan/dicabut. Sertifikat dapat dicabut dengan berbagai alasan, mulai dari pencabutan secara administratif sudah habis masa berlakunya dan tidak diperpanjang lagi maupun ketika kunci privat sudah tidak aman lagi. Beberapa metode di mana CA dapat membatalkan sertifikat adalah: *Periodic Publication Mechanisms*, di dalamnya termasuk penggunaan CRL dan *Certificate Revocation Trees* (CRT). *Online Query Mechanism*, termasuk *Online Certificate Status Protocol* (OCSP) dan *Online Transaction Validation Protocol* (OTVP). OCSP digunakan untuk mendapatkan informasi pembatalan sertifikat secara *online*, dan OTVP digunakan untuk validasi secara *online*.
d) *End-entity* : *End-entity* adalah *user*/pengguna yang telah melakukan pendaftaran dan memiliki sertifikat yang telah dihasilkan oleh server CA.

d. Kriptografi

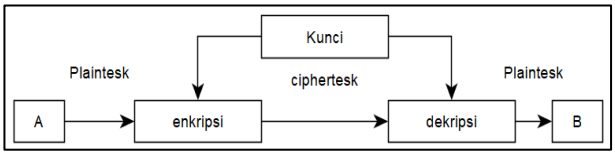
Menurut Schneider [7], kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta otentik data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya. Ada empat tujuan ilmu kriptografi menurut Wahana Komputer [8] 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 lain-lain.
d) *Non-Repudiation*, yang berarti begitu pesan terkirim, tidak akan dapat dibatalkan atau tidak dapat disangkal.

e. Algoritma Kriptografi Simetris

Kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi [9]. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu *bit* atau satu *byte* data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau *byte* data [9].

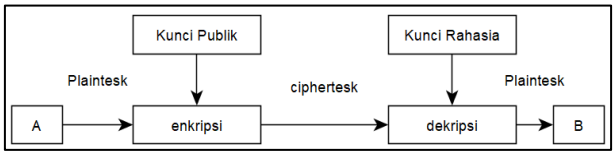
Kriptografi simetris merupakan kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapa pun yang memiliki kunci tersebut – termasuk pihak-pihak yang tidak diinginkan – dapat membuat dan membongkar rahasia *ciphertext*. Problem yang paling jelas di sini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan. Contoh algoritma kunci simetris yang terkenal adalah DES (*Data EncryptionStandard*) dan RC-4, sebagaimana ditunjukkan pada gambar 2.1 berikut [9].



Gambar 2.1 Algoritma Kriptografi simetris

f. Algoritma Kriptografi Asimetris

Pada pertengahan tahun 70-an Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi asimetris yang merevolusi dunia kriptografi. Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi [9]. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci *private* untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya [9].



Gambar 2.2 Algoritma Kriptografi asimetris

g. 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 benar-benar berasal dari orang yang diinginkan [10].

h. Enterprise Java Bean Certificate Authority

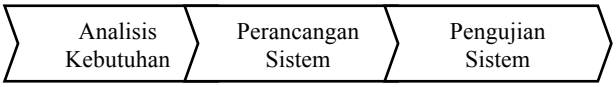
Enterprise Java Bean Certificate Authority atau EJBCA merupakan *Certificate Authority* (CA) berbasis PKI (*Publik Key Infrastructure*) dan menggunakan teknologi *Java* (JEE). EJBCA dapat digunakan secara mandiri (berdiri sendiri) atau terintegrasi dengan aplikasi lain, berdasarkan komponen CA JBCA. EJBCA sesuai untuk membangun infrastruktur PKI untuk perusahaan besar dan organisasi. EJBCA adalah *software* PKI yang kuat, *fleksibel*, kinerja teratur, dan *platform* independen [11]

i. *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 [12].

III. METODOLOGI PENELITIAN

Metodologi penelitian diperlukan agar penelitian dapat terstruktur sehingga hasil yang diperoleh sesuai dengan tujuan penelitian. Sistem yang akan dibangun merupakan sistem tanda tangan digital (*digital signature*) yang bertujuan untuk memudahkan penggunaan tanda tangan dalam bentuk digital.



Gambar 3.1 Struktur Penelitian

a. Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengetahui kebutuhan yang bersumber dari masalah yang ada sehingga perancangan sistem dibangun sesuai dengan kebutuhan. Adapun kebutuhan dari analisis masalah yang telah dilakukan adalah sebagai berikut :

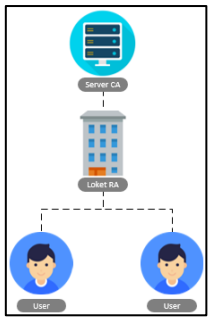
a) *Server* CA
Server CA dibutuhkan untuk menyimpan data dan sertifikat dari *user* yang telah mendaftar.

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.

b. Perancangan Sistem

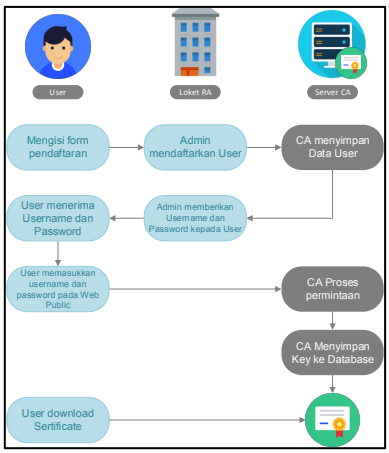
Pada penelitian ini diperlukan sebuah desain dan perancangan sistem sebagai acuan penelitian dan bertujuan untuk menentukan desain atau skema dari sebuah sistem yang akan di bangun. Pada tahap perancangan sistem ini terdiri dari dua tahapan yaitu, perancangan konseptual dan perancangan fisik. Berdasarkan hasil analisis kebutuhan, maka skema sistem tanda tangan digital dapat dilihat pada gambar 3.2 di bawah ini.



Gambar 3.2 Gambaran Arsitektur CA

c. Proses penerbitan Sertifikat Digital

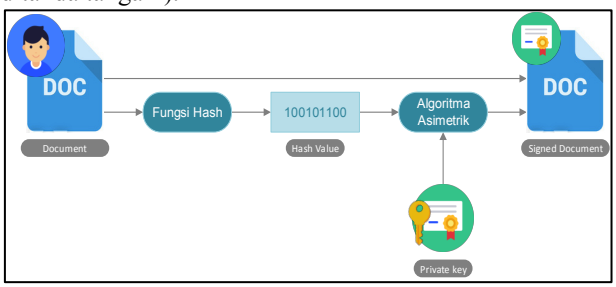
Gambar 3.3 menjelaskan bahwa untuk mendapatkan sertifikat tanda tangan digital, *user* terlebih dahulu harus pergi ke loket pendaftaran untuk mengisi formulir pendaftaran. Setelah *user* mengisi formulir maka admin akan mendaftarkan user pada halaman web admin berdasarkan data yang diisi user pada formulir tersebut. Setelah itu *user* akan diberikan *username* dan *password* untuk mengunduh *file* sertifikat digital yang berformat p12 pada web *public* yang telah disediakan, dengan catatan *user* hanya dapat mengunduh *file* p12 tersebut sebanyak yang telah ditentukan oleh admin.



Gambar 3.3 Alur proses mendapatkan sertifikat digital

d. Proses Penanda Tanganan Dokumen Digital

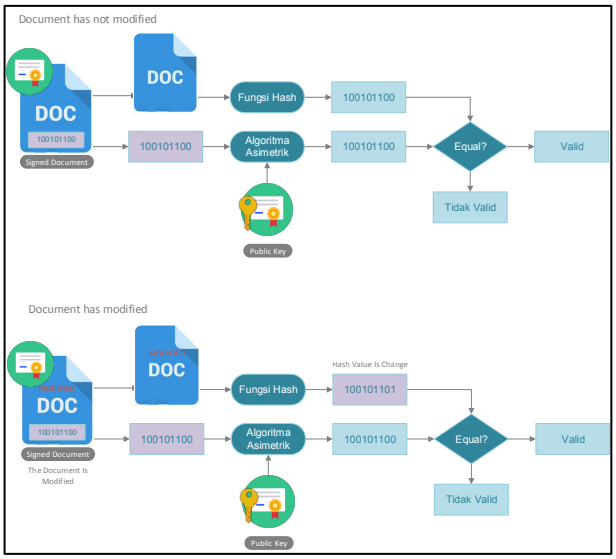
Gambar 3.4 menjelaskan proses *signed* sebuah dokumen, sebuah *file* asli yang akan diberikan tanda tangan digital pertama-tama akan digunakan fungsi *hash* untuk mendapatkan nilai *hash* dari *file* tersebut. Kemudian nilai *hash* dari *file* tersebut akan di enkripsi dengan menggunakan *private key* dari penanda tangan menjadi nilai *signature*. Setelah itu nilai *signature* tersebut akan disisipkan ke dalam *file* asli beserta dengan sertifikat digital dari si penanda tangan yang kemudian menghasilkan sebuah *file* baru. *File* baru tersebutlah yang dimaksud dengan *digital signed file* (*file* yang telah ditanda tangani).



Gambar 3.4 Diagram Proses Signed Data

e. Proses Verifikasi Dokumen dengan Tanda tangan digital

Gambar 3.5 menjelaskan bagaimana proses untuk melakukan verifikasi dari sebuah *file* yang telah diberikan tanda tangan digital (*ciphertext*), proses pertama yang dilakukan adalah dengan membagi dua *file* yang telah diberikan tanda tangan dengan mengeluarkan nilai *signature* dari *file* tersebut, kemudian nilai *signature* tersebut akan di deskripsi dengan menggunakan *public key* dari pengguna sehingga menghasilkan sebuah nilai *hash* (*message digest*)., setelah itu *file* yang telah dikeluarkan nilai *signature*-nya akan digunakan fungsi *hash* untuk mendapatkan nilai *hash* (*message digest*). Untuk mengetahui apakah *file* tersebut ditanda tangani oleh pemilik tanda tangan yang asli dengan menyamakan nilai *hash* dari *file* tersebut dengan nilai *hash* dari hasil dekripsi nilai *signature*.



Gambar 3.5 Diagram Proses Verifikasi Data Dokumen

f. Pengujian Sistem

Pengujian dilakukan dengan menggunakan metode *Blackbox* dan terdiri dari tiga bagian yaitu pengujian terhadap web admin, web *public* dan pengujian terhadap sertifikat digital yang akan digunakan untuk membuat tanda tangan digital pada sebuah dokumen.

IV. HASIL DAN PEMBAHASAN

a. Hasil

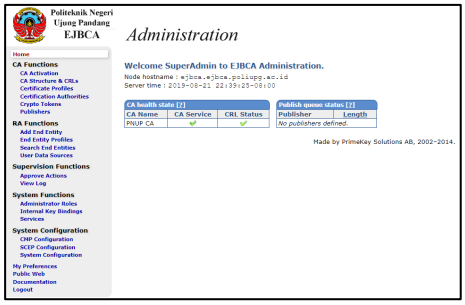
Sistem ini terdiri dari sebuah web admin yang digunakan untuk melakukan pengolahan data pengguna dan web *public* yang digunakan pengguna untuk mengunduh *file sertificate* digital dengan format *Personal Information Exchange* (.p12).

a) Web Admin

Web admin merupakan web yang hanya dapat diakses oleh administrator untuk melakukan pengolahan data pengguna seperti menambah, mengubah, dan menghapus pengguna. Web admin terdiri dari beberapa halaman seperti halaman utama, halaman profil pengguna, dan halaman penambahan pengguna.

1. Halaman utama admin

Halaman ini merupakan halaman awal dari web admin sistem tanda tangan digital yang memiliki konten utama yaitu, informasi *hostname* dan waktu dari server, informasi CA (*Certificate Autority*) yang sedang aktif seperti ditunjukkan pada Gambar 4.1.



Gambar 4.1 utama web admin

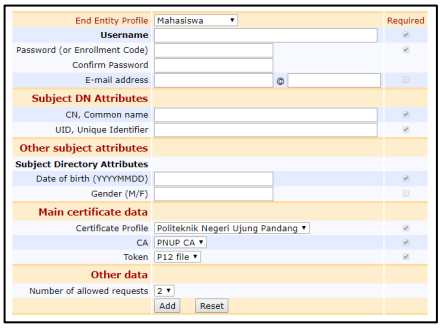
2. Halaman profil pengguna

Halaman profil pengguna berisi tentang daftar jenis profil yang dapat digunakan oleh pengguna seperti yang di tunjukkan pada gambar 4.2.

Gambar 4.2 halaman jenis profil CA

3. Halaman penambahan pengguna

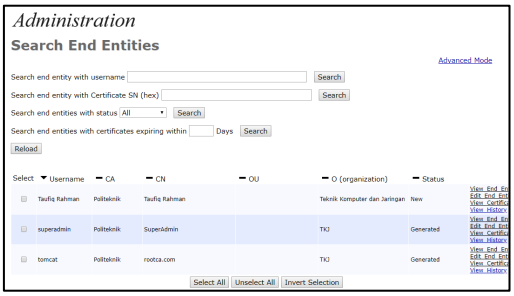
Halaman penambahan pengguna berisi tentang isian yang digunakan administrator untuk melakukan penambahan pengguna. Adapun data yang harus diisikan oleh administrator yaitu data yang terdapat pada profil pengguna yang dipilih sebagaimana yang ditunjukkan pada gambar 4.3.



Gambar 4.3 halaman penambahan data pengguna

4. Halaman Pencarian Pengguna

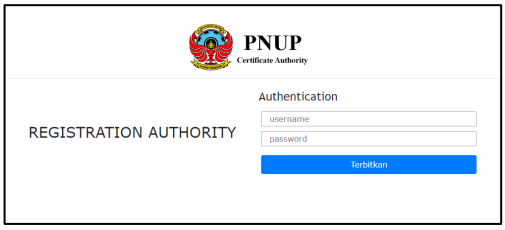
Halaman ini merupakan halaman pencarian pengguna yang telah terdaftar.



Gambar 4.4 pencarian pengguna

5. Web *User*

Web *user* atau web *public* merupakan halaman yang diakses oleh pengguna untuk mengunduh *file* sertifikat digital dengan memasukkan *username* dan *password* yang telah diberikan oleh administrator



Gambar 4.5 halaman pengguna

b. Pengujian

a) Pengujian Administrator

Tabel 4.1 Pengujian Administrator

Data Masukan	Kesimpulan
Mengakses halaman admin	Berhasil
Menampilkan halaman awal web admin	Berhasil
Menambahkan profil pengguna baru	Berhasil
Mengubah isian profil pengguna baru	Berhasil
Menambahkan Pengguna baru	Berhasil
Melakukan pencarian berdasarkan *username*	Berhasil
Melakukan pencarian berdasarkan *serial number*	Berhasil
Melakukan pencarian berdasarkan status sertifikat pengguna	Berhasil
Melakukan pencarian dengan menggunakan masa berlaku sertifikat	Berhasil

b) Pengujian Pengguna

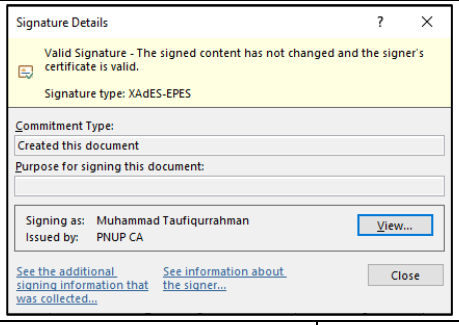
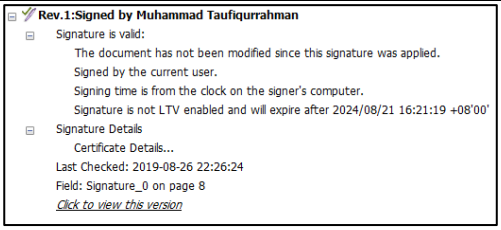
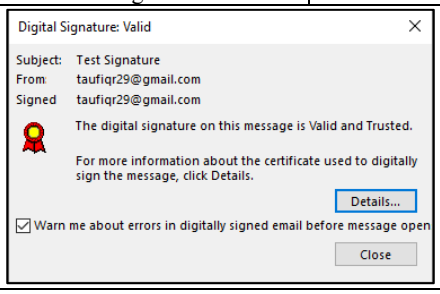
Tabel 4.2 Pengujian Pengguna

Data Masukan	Kesimpulan
memasukkan *username* dan *password*	Berhasil
Mengunduh sertifikat RootCA	Berhasil
Menerbitkan sertifikat digital	Berhasil
Notifikasi kesalahan *username* dan *password*	Berhasil

c) Pengujian Sertifikat Digital

Pengujian ini di lakukan dengan tiga bagian. Adapun yang pertama yaitu dengan menanda tangani dokumen digital berupa *file* doc, pdf dan email.

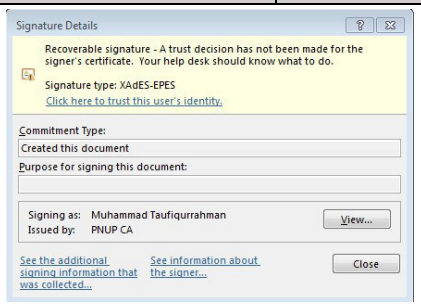
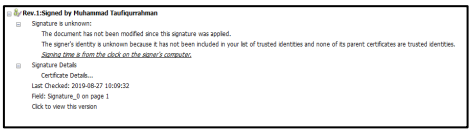
Tabel 4.3 Pengujian Sertifikat Digital Valid

No.	Data Masukan	Kesimpulan
1	Signed file Doc dengan office 2019	Berhasil
		
2	Signed file PDF dengan Foxit Reader	Berhasil
		
3	Signed email dengan outlook	Berhasil
		

Adapun pengujian yang kedua yaitu apabila perangkat yang digunakan belum atau tidak terinstal *Trusted Certificate* dari sertifikat digital yang digunakan, maka hasil proses validasi menjadi tidak valid seperti yang terdapat pada Tabel 4.4

Tabel 4.4 Pengujian Sertifikat Digital Tidak Valid

No.	Data Masukan	Kesimpulan
1	Tanda tangan tidak valid pada file Doc	Berhasil

No.	Data Masukan	Kesimpulan
		
2	Tanda tangan tidak valid pada file PDF	Berhasil
		
3	Tanda tangan tidak valid pada Email	Berhasil
		

Adapun pengujian yang ketiga yaitu pengujian pada file doc dan PDF dengan ukuran yang berbeda sebanyak tiga kali dan menampilkan hasil rata-rata dari waktu yang di perlukan untuk menanda tangan. Adapun hasilnya dapat dilihat pada Tabel 4.5 di bawah ini.

Tabel 4.5 Pengujian pada ukuran file yang berbeda

No.	Data Masukan	Ukuran (MB)	Pengujian Waktu (Detik)			Rata-rata
			1	2	3	
1	File Doc	101MB	1.56	1.59	2.28	1.81
2	File Doc	152MB	1.77	2.11	1.72	1.87
3	File Doc	231MB	3.01	3.12	3.13	3.09
4	File PDF	10MB	5.40	4.10	3.72	4.41
5	File PDF	102MB	12.92	14.78	12.55	13.42
6	File PDF	505MB	36.78	38.65	35.33	36.92

Berdasarkan hasil pengujian pada Tabel 4.5 yaitu lama waktu yang dibutuhkan untuk menanda tangani sebuah dokumen, dapat dilihat bahwa perbedaan antara file Doc dan PDF cukup signifikan, hal ini terjadi karena file Doc yang telah diberikan tanda tangan digital tidak membuat file baru yang terpisah dari file orisinalnya sehingga tanda tangan digital hanya disisipkan ke dalam file Doc tersebut dan membuat waktu penanda tangan menjadi relatif lebih cepat, sedangkan untuk dokumen PDF akan membuat sebuah dokumen baru yang terpisah dari file orisinalnya sehingga waktu yang dibutuhkan untuk menanda tangani file PDF relatif lama dari pada file Doc, hal ini juga berpengaruh berdasarkan ukuran file PDF tersebut.

V. KESIMPULAN

Berdasarkan hasil perancangan dan pengujian dapat ditarik kesimpulan sebagai berikut :

a) Sistem tanda tangan digital dapat diimplementasikan untuk menerbitkan sertifikat digital.
b) Sertifikat digital yang diterbitkan oleh sistem dapat digunakan sebagai sarana tanda tangan pada dokumen digital berupa *file* Doc, PDF, dan Email.

REFERENSI

[1] A. G. P. Suratma and A. Azis, "*Techno , ISSN 1410 - 8607 Tanda Tangan Digital Menggunakan Qr Code Dengan Metode Advanced Encryption Standard Digital Signature Using QR Code By Advanced Encryption Standard Method Abdul Gani Putra Suratma , Abdul Azis,*" vol. 18, no. 1, pp. 59–68, 2017.

[2] H. F. Isnaini and K. Karyati, "*Penerapan skema tanda tangan Schnorr pada pembuatan tanda tangan digital,*" Pythagoras J. Pendidik. Mat., vol. 12, no. 1, p. 57, 2017.

[3] R. A. Azdy, "*Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA,*" *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, pp. 184–191, 2016.

[4] Microsoft, "*Tanda Tangan dan Sertikat Digital,*" 2016. [Online]. Available: https://support.office.com/id-id/article/Tanda-tangan-dan-sertifikat-digital-8186cd15-e7ac-4a16-8597-22bd163e8e96#top. [Accessed: 22-Jun-2018].

[5] KOMINFO, "*Tanda Tangan Digital,*" 2016. [Online]. Available: https://sivion.rootca.or.id/. [Accessed: 09-Apr-2018].

[6] I. Rahayu and M. Mahabas, "*Perbandingan Aplikasi Public Key Infrastructure Pada Windows Server 2003 Dan Ejbca,*" pp. 262–265, 2009.

[7] B. Schneier, *Applied Cryptography*, vol. 1, no. [32. 1996.

[8] W. Komputer, *The Best Encryption Tools*. Elex Media Komputindo, 2013.

[9] Basri, "*Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi,*" J. Ilm. Ilmu Komput., vol. 2, no. 2, pp. 2442–4512, 2016.

[10] D. Ariyus, "*Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi.,*" Journal of Chemical Information and Modeling. pp. 1689–1699, 2008.

[11] A. Lutfi, "*implementasi keamanan jaringan dengan membangun server certificate authority ca menggunakan ejbca,*" Pelayanan Kesehat., vol. 2013, no. Dm, pp. 3–13, 2010.

[12] Yuhefizar, *CMM Website Interaktif MCMS Joomla(CMS)*. 2009.