Website Tanda Tangan Digital Terpusat menggunakan ECDSA dan SHA-3 pada Masa Pandemi COVID-19 untuk Menjamin Keaslian Dokumen

Muhammad Zunan Alfikri - 13518019
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13518019@std.stei.itb.ac.id

***Abstract*—Pandemi COVID-19 menyebabkan semua orang menjadi *Work From Home*(WFH). Akibatnya banyak dokumen yang dihasilkan secara online, mulai dari sertifikat, dokumen jual beli, transkrip nilai, surat perjanjian, dan dokumen-dokumen lainnya. Dokumen digital tentunya lebih mudah direkayasa dan diragukan keabsahannya. Oleh sebab itu, diperlukan suatu sistem yang dapat menjamin suatu keaslian dokumen yang dikeluarkan oleh suatu lembaga atau organisasi. Pada makalah ini, penulis mengusulkan sebuah solusi yaitu dengan menggunakan website tanda tangan digital terpusat untuk menandatangani dokumen dan cek keabsahan dokumen menggunakan *Eliptic Curve Digital Signature Algorithm*(ECDSA). Website ini dapat digunakan pada masa pandemi untuk menjamin keaslian suatu dokumen.**

***Keywords*—Dokumen, ECDSA, tanda tangan digital, website tanda tangan digital terpusat.**

I. PENDAHULUAN

Pandemi COVID-19 di Indonesia sudah berlangsung sejak Maret 2020. Hal tersebut menyebabkan pemerintah mengeluarkan kebijakan untuk Pembatasan Sosial Berskala Besar(PSBB) di berbagai daerah dan menghimbau para perusahaan untuk melakukan *Work From Home* (WFH). Selain itu, pemerintah melalui Kementrian Pendidikan juga mengumumkan bahwa sekolah dan perguruan tinggi harus melakukan pembelajaran jarak jauh secara online.

Dalam pelaksanaan WFH dan pembelajaran online, berbagai dokumen yang awalnya dipertukarkan lewat media fisik seperti perjanjian kontrak, sertifikat, raport, dan nota pembayaran menjadi dipertukarkan lewat media online. Dokumen yang dipertukarkan harus terjamin keasliannya, keabsahannya, pengirimnya dan tidak di ubah oleh pihak lain.

Namun, pertukaran dokumen menggunakan media online memunculkan beberapa persolan. Persoalan pertama yaitu karena pertukaran dokumen dilakukan melalui jaringan, maka pihak ketiga dapat mengubah konten dari dokumen tersebut sehingga dokumen tersebut telah berbeda dari dokumen aslinya. Persoalan kedua yaitu dokumen dapat dipalsukan oleh pihak yang tidak bertanggungjawab. Misalnya piagam penghargaan palsu yang meyatakan bahwa suatu pihak telah memenangkan kejuaraan. Hal tersebut tentu merugikan pihak yang dipalsukan dokumennya.

Oleh karena itu, pada makalah ini penulis mengusulkan sebuah solusi yaitu Website Tanda Tangan Digital Terpusat menggukanan ECDSA pada Masa Pandemi COVID-19. Website ini menggunakan tanda tangan digital untuk menjamin keaslian dan anti penyangkalan dari dokumen. Dengan menggunakan website ini, harapannya pengirim dan penerima dokumen merasa aman dan terjamin keaslian dokumennya.

II. DASAR TEORI

A. Tanda Tangan Digital

Tanda tangan digital (*digital signature*) merupakan tanda tangan yang digunakan untuk data digital. Tanda tangan digital bukan tanda tangan tulisan tangan yang digital namun nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda tangan digital berbeda-beda pada setiap dokumen. Tanda tangan digital digunakan untuk menyelesaikan aspek keamanan autentikasi, keaslian pesan dan anti penyengkalan.

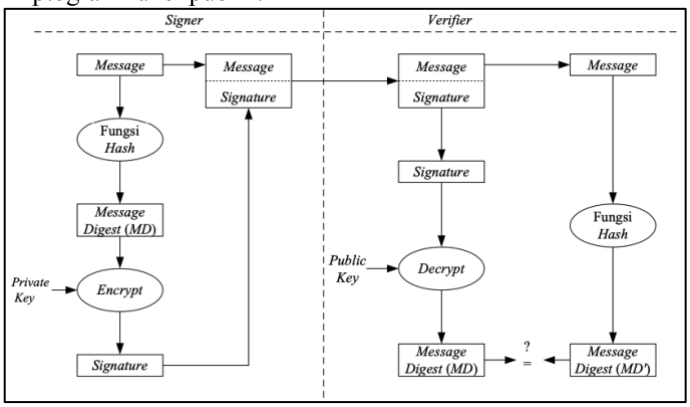
Tanda tangan digital memiliki beberapa karakteristik yaitu :

1. Tanda tangan adalah bukti yang autentik
2. Tanda tangan tidak dapat dilupakan
3. Tanda tangan tidak dapat dipindah untuk digunakan ulang
4. Dokumen yang telah ditandatangani tidak dapat diubah
5. Tanda tangan tidak dapat disangkal.

Dalam menandatangani pesan atau dokumen, tedapat dua metode yang digunakan pada tanda tangan digital. Metode yang pertama yaitu dengan cara mengenkripsi pesan dan metode yang kedua yaitu menggunakan kombinasi fungsi hash (hash function) dan kriptografi kunci public.

Penandatanganan dengan cara mengenkripsi dapat dilakukan dengan menggunakan kriptografi kunci simetri dan kriptografi kunci publik. Pada makalah ini, penulis menggunakan metode yang kedua yaitu kombinasi fungsi hash dan kriptografi kunci publik karena konten dari dokumen yang akan ditandatangani harus dapat dibaca terlebih dahulu tanpa perlu memvalidasinya(hal tersebut tidak dapat dicapai menggunakan metode yang pertama).

Berikut ini alur menggunakan metode fungsi *hash* dan kriptografi kunci publik.



Gambar I. Metode Penandatanganan dengan Fungsi *Hash* dan Kriptografi Kunci-Publik

B. DSS (*Digital Signature Standard*)

DSS adalah bakuan (*standard*) untuk tanda tangan digital. DSS diresmikan pada bulan Agustus 1991 oleh NIST (*The National Institute of Standard and Technology*). DSS terdiri dari dua komponen yaitu algoritma tanda tangan digital (*Digital Signature Algorithm*) dan fungsi hash standard (*Secure Hash Algotithm* (SHA)).

Secara umum proses tanda tangan digital dapat dibedakan menjadi 3 yaitu pembangkitan pasangan kunci, pemberian tanda tangan digital (*signing*), dan verifikasi terhadap keabsahan tanda tangan digital tersebut (*verifying*).

Pembangkitan pasangan kunci menghasilkan 2 kunci yaitu kunci publik dan kunci privat. Kunci privat digunakan pihak pengirim untuk menandatangani pesan yang akan dikirim. Kunci publik digunakan pihak penerima untuk memastikan keabsahan tanda tangan yang dikirim dari pihak pengirim.

Signing merupakan proses penandatanganan dokumen digital. Pesan yang hendak dikirim diubah terlebih dahulu menjadi bentuk yang ringkas yang disebut message digest. Message digest (MD) diperoleh dengan cara mentransformasikan pesan M menggunakan fungsi hash satu-arah (*one-way*) H,

$$MD = H(M) \quad (1)$$

Pesan yang sudah diubah menjadi message digest oleh fungsi hash tidak dapat dikembalikan lagi menjadi bentuk semula walaupun digunakan algoritma dan kunci yang sama (itulah sebabnya dinamakan fungsi hash satu-arah). Sembarang pesan yang berukuran apapun diubah oleh fungsi hash menjadi message digest yang berukuran tetap (umumnya 128). Selanjutnya, message digest MD dienkripsikan dengan algoritma kunci-publik menggunakan kunci rahasia (SK) pengirim menjadi tanda tangan S,

$$S = ESK(MD) \quad (2)$$

Pesan M disambung (append) dengan tanda tangan S, lalu keduanya dikirim melalui saluran komunikasi. Dalam hal ini, kita katakan bahwa pesan M sudah ditandatangani oleh pengirim dengan tanda tangan digital S.

Verifying merupakan proses verifikasi tanda tangan yang telah diterima oleh pihak penerima. Pesan M dan tanda tangan digital S yang dikirim melalui saluran komunikasi akan diterima oleh pihak penerima. Di tempat penerima, pesan diverifikasi untuk dibuktikan keotentikannya dengan cara berikut : Tanda tangan digital S di dekripsi dengan menggunakan kunci publik (PK) pengirim pesan, menghasilkan message digest semula, MD, sebagai berikut:

$$MD = DPK(S)$$

Pengirim kemudian mengubah pesan M menjadi message digest MD' menggunakan fungsi hash satu-arah yang sama dengan fungsi hash satu-arah yang sama dengan fungsi hash yang digunakan oleh pengirim. Jika MD' = MD, berarti pesan yang diterima otentik dan berasal dari pengirim yang benar.

Proses pembuktian keotentikan tanda tangan digital ini dijelaskan sebagai berikut:

1. Apabila pesan M yang diterima sudah berubah, maka MD' yang dihasilkan dari fungsi hash berbeda dengan MD semula. Hal ini berarti bahwa pesan sudah tidak asli lagi (*data integrity*).
2. Apabila pesan M tidak berasal dari orang yang sebenarnya, maka message digest MD yang dihasilkan dari persamaan 3 berbeda dengan message digest MD' yang dihasilkan pada proses verifikasi (hal ini karena kunci publik yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci rahasia pengirim). Bila MD = MD', ini berarti pesan yang diterima adalah pesan yang asli (*message authentication*) dan orang yang mengirim adalah orang yang sebenarnya (*user authentication*). Karena proses signing menggunakan kunci rahasia pengirim maka pengirim pesan tidak dapat menyangkal aktivitas yang telah dilakukannya (*nonrepudiation*).

C. ECC dan ECDSA

ECC (*Elliptic Curve Cryptography*) adalah suatu pendekatan implementasi algoritma kriptografi kunci publik. ECC memanfaatkan elliptic curve pada suatu medan finite. Secara umum, suatu elliptic curve pada medan galois GF(p) dapat dinyatakan menggunakan persamaan berikut:

$$y^2 = x^3 + ax + b \bmod p$$

dengan parameter a, b, dan p tersebut merupakan parameter dari suatu elliptic curve.

ECC ini dapat diterapkan sebagai perluasan untuk algoritma-algoritma kriptografi yang lain, misalnya:

1. ECDSA (*Elliptic Curve Digital Signature Algorithm*).
2. ECDH (*Elliptic Curve Diffie-Hellman*).
3. ECEG (*Elliptic Curve ElGamal*).

ECDSA (*Elliptic Curve Digital Signature Algorithm*) adalah suatu implementasi DSA (*Digital Signature Algorithm*) yang memanfaatkan *elliptic curve cryptography*. Terdapat 2 proses bagian utama dalam ECDSA, yaitu proses *sign* atau *generate signature* dan *verify* atau verifikasi signature.

Pada ECDSA terdapat beberapa parameter lain sebagai tambahan parameter elliptic curve yang digunakan (a, b, p), yaitu:

1. G, elliptic curve base point, yang menjadi generator subgroup pada elliptic curve yang dipakai.
2. n yang merupakan orde dari elliptic curve. Hubungan antara n, G, dan O (elemen identitas) dapat dinyatakan dalam persamaan n x G=O.
3. d yang merupakan private key yang digunakan dalam

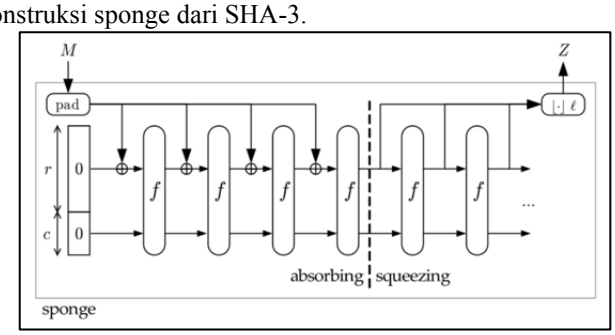
ECDSA.

4. Q yang merupakan public key yang digunakan dalam ECDSA. Sebagai catatan hubungan antara d, Q, dan G dapat dinyatakan dalam persamaan d x G=Q.

D. Fungsi *Hash* SHA-3

SHA-3 atau *Secure Hash Algorithm*-3 (SHA-3) adalah keluarga fungsi pada data biner berdasarkan algoritma KECCAK yang dipilih NIST sebagai pemenang Kompetisi Algoritma Hash Kriptografi SHA-3. Standar ini juga menentukan keluarga KECCAK-p dari permutasi matematika, termasuk permutasi yang mendasari KECCAK, untuk memfasilitasi pengembangan fungsi kriptografi berbasis permutasi tambahan.

Keluarga SHA-3 terdiri dari empat fungsi hash kriptografi yang disebut SHA3-224, SHA3-256, SHA3-384, dan SHA3-512, dan dua fungsi keluaran yang dapat diperpanjang (XOF), yang disebut SHAKE128 dan SHAKE256. Berikut adalah konstruksi sponge dari SHA-3.



Gambar 2. Konstruksi Spone SHA-3

Dalam proses hashing SHA-3, terdapat 3 fase yaitu :

1. Praproses
   Praproses dilakukan dengan menerapkan multi-rate padding dengan menambahkan suffix untuk pesan yang sudah dibagi menjadi blok-blok berukuran rate. Untuk sebagian besar aplikasi, pesannya disejajarkan dengan byte, yaitu, len(M) = 8m untuk bilangan bulat non negatif m. Dalam kasus ini, jumlah total byte, yang dilambangkan dengan q, yang ditambahkan ke pesan ditentukan sebagai berikut dengan m dan rate r:
   $$q = (r/8) - (m \bmod (r/8))$$
2. *Absorbing*
   Langkah-langkah yang dilakukan pada fase ini adalah:
   a. Untuk setiap blok masukan Pi berukuran r-bit, XOR-kan dengan r-bit pertama dari state S, lalu hasilnya dimasukkan ke dalam fungsi permutasi f untuk menghasilkan state baru S.
   b. Bila semua blok masukan selesai diproses, konstruksi spons beralih ke fase pemerasan(*squeezing*).
3. *Squeezing*
   Langkah-langkah yang dilakukan pada fase ini adalah:
   a. Message digest akan disimpan di dalam Z.
   b. Inisialisasi Z dengan string kosong (*null string*).
   c. Selagi Panjang Z belum sama dengan d, r-bit pertama dari state S disambungkan (*append*) ke Z.
   d. Jika Panjang Z masih belum sama dengan maka dimasukkan ke dalam fungsi permutasi f menghasilkan state baru S.

   C bit terakhir dari state tidak pernah terpengaruh secara langsung oleh blok masukan dan tidak pernah mengeluarkan luaran selama fase pemerasan. Hal ini untuk mencegah terjadinya kolisi.

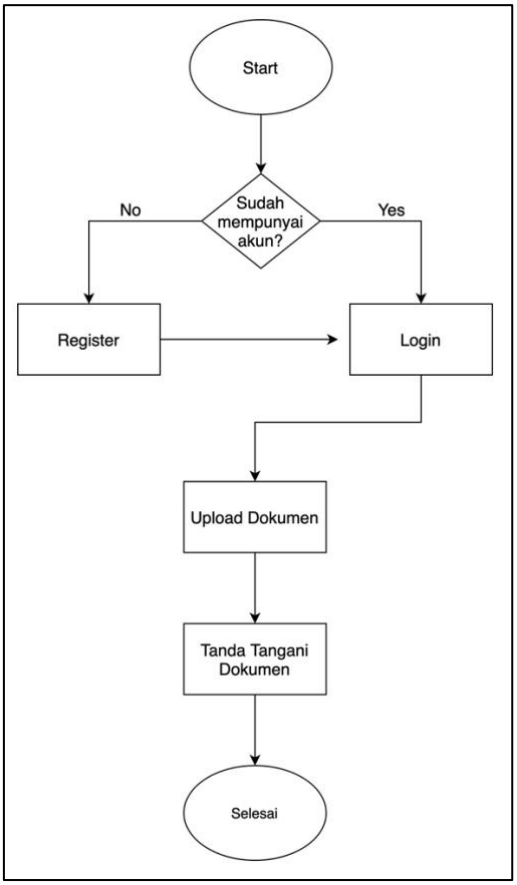
III. RANCANGAN SOLUSI

Solusi yang penulis tawarkan merupakan platform berbasis website yang digunakan untuk menandatangani dokumen dan memvalidasi dokumen.

Algoritma yang digunakan untuk menandatangani dan memvalidasi dokumen yaitu SHA-3 dan ECDSA. ECDSA digunakan karena ECDSA memiliki sifat ringan dalam komputasi dibandingkan algoritma RSA. Jika pengunjung website dan dokumen yang akan di tandatangani maupun di validasi banyak, maka website akan tetap mampu mengakomodasi permintaan dari pengguna.

Website ini memiliki 2 role utama yaitu pihak yang menerbitkan dokumen dan pihak yang memvalidasi dokumen. Berikut ini alur dari kedua pihak:

A. Pihak yang menerbitkan dokumen



Gambar 3. Alur pihak yang menerbitkan dokumen

Pihak yang menerbitkan dokumen biasanya berupa organisasi, Lembaga Pendidikan, atau perusahaan yang sering menerbitkan dokumen.

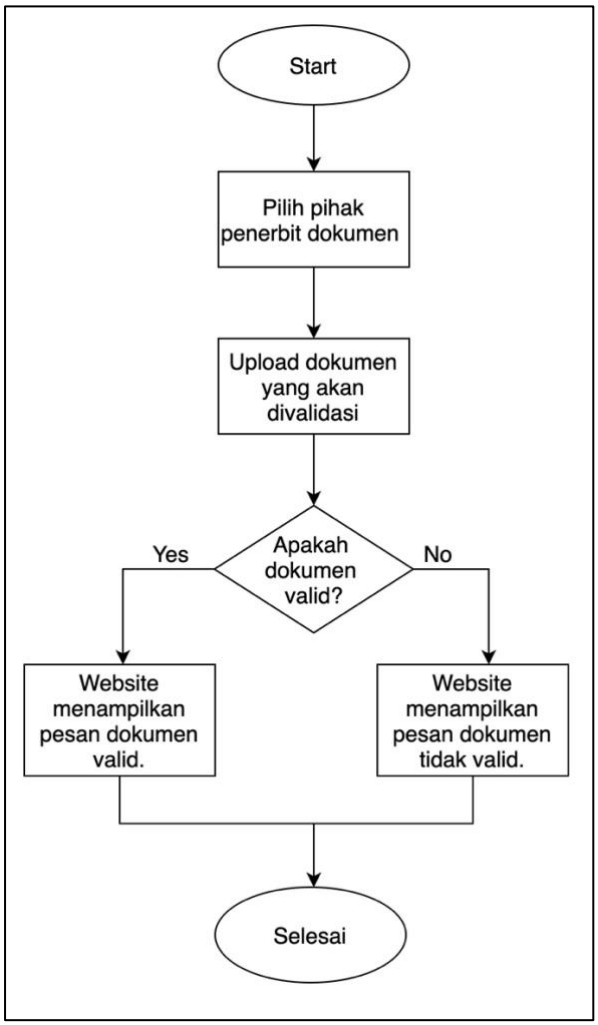
Alur penandatanganan dimulai dari pihak yang menandatangani harus mempunyai akun pada website tersebut. Jika belum mempunyai akun, pengguna harus mendaftarkan

akun terlebih dahulu. Akun ini akan dipasangkan dengan sepasang kunci public dan kunci private pada database. Kunci public dan kunci privat ini berguna untuk menandatangani dan memvalidasi dokumen dari pihak terkait.

Setelah akun berhasil dibuat (yang artinya pengguna sudah memiliki sepasang kunci public dan kunci privat), pengguna dapat login dan memgupload dokumen yang dipilih untuk ditanda tangani. Setiap dokumen yang unik memiliki tanda tangan digital yang berbeda.

Setelah semua file telah teruplod, website akan memproses dan menandatangani file tersebut. Tanda tangan digital akan terletak pada bagian bawah dari dokumen. Setelah proses penandatanganan selesai, pengguna dapat mengunduh file yang telah ditandatangani dan proses penandatangan dokumen selesai.

B. Pihak yang memvalidasi dokumen



Gambar 4. Alur pihak yang memvalidasi dokumen

Pihak yang memvalidasi dokumen yaitu pihak yang memiliki dokumen yang telah ditandatangani dan ingin memastikan apakah dokumen yang dimiliki asli dan tidak ada perubahan.

Proses validasi dokumen dimulai dari pengguna memilih pihak yang menerbitkan dokumen. Pemilihan pihak yang menerbitkan dokumen secara tidak langsung pengguna memilih kunci publik yang bersesuaian untuk memvalidasi dokumen tersebut.

Setelah memilih pihak penerbit dokumen, pengguna diminta untuk mengupload dokumen yang akan divalidasi. Jika dokumen tersebut asli dan pengguna memilih pihak penerbit dokumen yang benar, maka website akan menampilkan pesan dokumen valid. Namun jika dokumen asli tetapi pengguna salah memilih pihak yang mengeluarkan dokumen yang artinya kunci public tidak cocok, maka website akan menampilkan pesan dokumen tidak valid. Begitu juga jika dokumen telah diubah oleh pihak ketiga atau dokumen tidak asli maka website akan menampilkan pesan dokumen tidak valid.

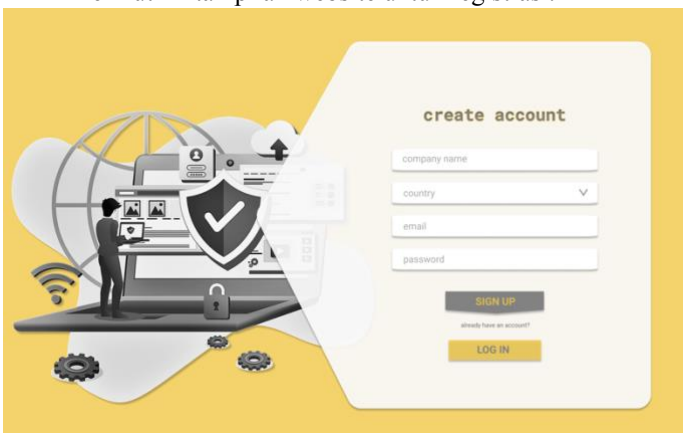
IV. FUNGSIONALITAS WEBSITE DAN *MOCKUP*

Agar website dapat dengan baik digunakan oleh pengguna dan memiliki kredibilitas yang baik, maka website tersebut harus memenuhi berbagai fungsionalitas sebagai berikut :

1. Pengguna dapat melakukan registrasi

   Pengguna yang dapat melakukan registrasi yaitu lembaga-lembaga atau orgasinsasi maupun perusahaan yang memiliki sertifikat dan terpercaya. Registrasi akan di terima oleh admin website jika pengguna telah memenuhi syarat.

   Berikut ini tampilan website untuk registrasi.

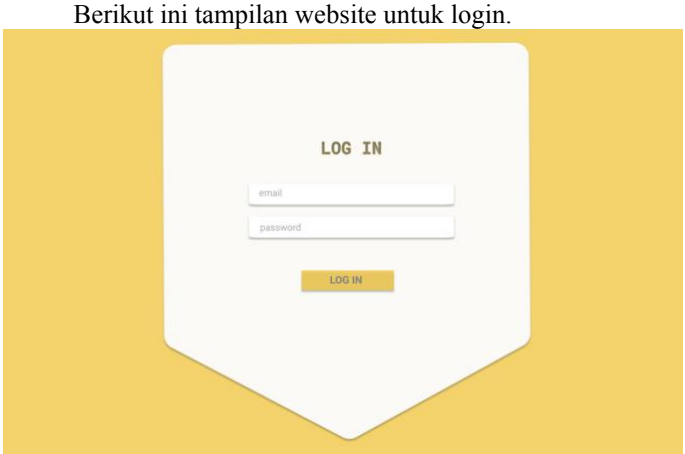


Gambar 5. Tampilan Registrasi

2. Pengguna dapat melakukan login

   Pengguna yang telah memiliki akun dapat login ke website dan melakukan tanda tangan dokumen.

   Berikut ini tampilan website untuk login.

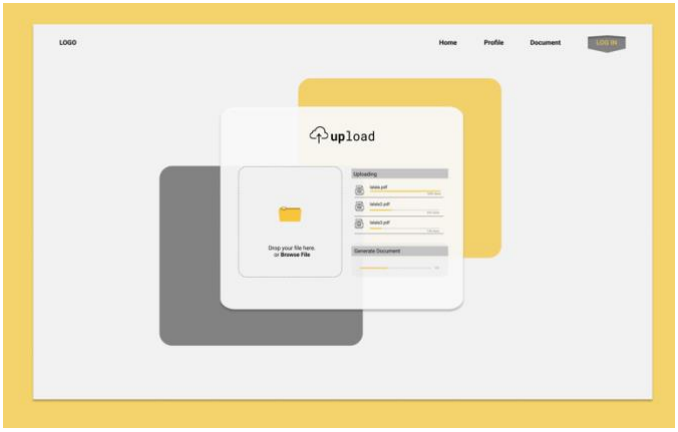


Gambar 6. Tampilan Login

3. Pengguna dapat mengupload dokumen untuk ditandatangani

   Pengguna yang telah login dapat mengupload beberapa file sekaligus dan melakukan penandatangan tehadap dokumen yang telah di upload.

   Berikut ini tampilan website untuk menandatangani dokumen

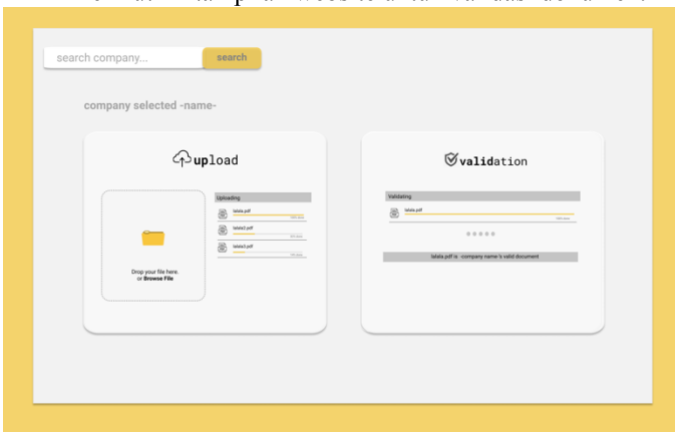


Gambar 7. Tampilan Penandatanganan Dokumen

4. Pengguna dapat mengupload dokumen untuk di validasi

   Untuk memvalidasi dokumen, pengguna tidak perlu login ke website. Pengguna hanya perlu untuk mengupload dokumen yang akan divalidasi dan memilih pihak yang menerbitkan dokumen tersebut.

   Berikut ini tampilan website untuk validasi dokumen.



Gambar 8. Tampilan Validasi Dokumen

5. Pihak pengelola website haruslah pihak yang harus dipercaya.

   Agar pengguna dapat dengan yakin menggunakan website, pengelolah website haruslah pihak yang terpercaya misalnya pemerintah, perusahaan besar seperti google, Microsoft, atau organisasi-organisasi lainnya.

V. Analisis dan Pembahasan

Dari segi alur penandatanganan dan validasi dokumen, website tanda tangan digital terpusat ini cukup mudah untuk dipahami pengguna dan mudah diingat.

Penggunaan ECDSA dibandingkan RSA pada website ini juga dapat menghemat komputasi serta penyimpanan kunci pada database jika dibandingakan dengan RSA. Berikut ini perbandingan kunci RSA dan ECDSA.

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Gambar 9. Perbandingan Panjang Kunci RSA dan ECDSA

Dari tabel yang dirilis oleh NIST tersebut, perbandingan panjang kunci dari RSA dan ECDSA terpaut jauh. Semakin panjang kunci ECC (yang digunakan pada ECDSA) semakin besar juga perbandingannya pada kunci RSA.

Namun, ada beberapa aspek keamanan yang perlu diperhatikan dari pembuatan website ini. Beberapa aspek tersebut diantaranya yaitu aspek penyimpanan kunci public dan kunci privat yang harus aman. Banyak pihak ke tiga yang dapat menyerang website kapan saja dan berusaha membobol database tersebut. Jika database kunci privat dan kunci public bocor ke pihak yang tidak diinginkan, maka hal tersebut sangat berbahaya dan menharuskan pengelola website mereset kunci public dan kunci privat. Akibatnya, dokumen-dokumen lama yang ditandatangani menjadi tidak bisa divalidasi. Untuk menanggulangi database yang bocor, database harus diamankan dengan keamanan berlapis. Misalnya menggunakan VPN(*Virtual Private Network*) jika akan mengakses dan berbagai teknik pengamanan lainnya.

Aspek keaman kedua yang harus diperhatikan yaitu ada beberapa dokumen yang di upload pengguna bersifat konfidensial. Pihak ketiga yang bertanggung jawab bisa saja menyadap jaringan yang digunakan untuk mengirim dokumen dan melihat konten dokumen yang di upload oleh pengguna. Hal tersebut dapat diminimalisir dengan menggunakan SSL (*Secure Socket Layer*) pada jaringannya sehingga pengiriman data melalui network dapat terenkripsi dengan baik.

VI. Kesimpulan

Pada era pandemi seperti sekarang ini, pertukaran dokumen memalui media elektronik menjadi semakin sering dan massif. Dengan adanya website tanda tangan digital terpusat ini, pertukaran dokumen melalui media elektronik menjadi lebih aman dan terjamin. Penggunaan website tanda tangan digital ini dapat memenuhi aspek otentikasi (*authentication*), keaslian pesan (*data integrity*), dan anti-penyangkalan (*nonrepudiation*).

VII. Ucapan Terima Kasih

Puji syukur penulis panjatkan kepada Allah SWT karena atas pertolongan, izin, berkat, rahmat, dan hidayah-Nya, penulis dapat menyelesaikan tugas makalah ini dengan lancar. Pada kesempatan ini, dengan segala kerendahan hati, penulis ingin

menyampaikan ucapan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen Mata Kuliah IF4020 Kriptografi – Sem. I Tahun 2020/2021 IF2211 Strategi Algoritma atas segala ilmu dan bimbingannya. Penulis juga ingin menyampaikan terima kasih kepada kedua orang tua yang selalu memberikan dukungan kepada penulis. Ucapan terima kasih juga penulis ucapkan kepada teman-teman yang telah memberikan bantuan dan dukungan dalam penyusunan makalah ini.

REFERENCES

[1] Johnson, Don. Menezes, Alfred. dkk. 2001. "The Elliptic Curve Digital Signature Algorithm (ECDSA)". Hayward:Certicom.
[2] Munir, Rinaldi. 2020. "SHA-3 (Keccak)". Bandung: Sekolah Teknik Informatika ITB.
[3] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi : Fungsi Hash
[4] Munir, Rinaldi: 2020. Slide Kuliah IF4020 Kriptografi: Tanda-tangan Digital.
[5] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi Algoritma RSA

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Desember 2020

Muhammad Zunan Alfikri
13518019