Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital

http://dx.doi.org/10.28932/jutisi.v7i1.3431
Riwayat Artikel
Received: 22 Februari 2021 | *Final Revision*: 8 Maret 2021 | *Accepted*: 12 Maret 2021

Taufan Abdurrachman[#1], Bernard Renaldy Suteja[✉*2]

[#]*Magister Ilmu Komputer, Universitas Kristen Maranatha*
Jl. Prof. drg. Surya Sumantri No. 65 Kota Bandung
[1]1879016@maranatha.ac.id
[2]bernard.rs@it.maranatha.edu

Abstract — **Currently, the Indonesian government is changing the government system into a Sistem Pemerintahan Berbasis Elektronik (SPBE) or often heard as e-government. With this change in the government system, it has an impact on the various sector of life. One of many sectors is the construction service sector. Lembaga Pengembangan Jasa Konstruksi (LPJK) as a non-structural institution under the Ministry of Public Works and Public Housing issued a letter to the construction services association regarding the development of an integrated application with Sistem Informasi Konstruksi Indonesia (SIKI) LPJK. LPJK and Online Single Submission (OSS) institutions have implemented digital signatures on business entity licensing document. Construction service associations has responded to develop of these regulations by creating an association information system application that implements digital signatures. This research was conducted to apply a digital signature to the validation of the Certificate of Membership using the secure hash algorithm (SHA) and advanced encryption standard (AES) methods generated through the association information system. This application generates a digital signature which is implemented with QR Code. The existence of this application is expected to be a form of support for the government which is making changes to the government system.**

Keywords— **Advanced Encryption Standard; Digital Signature; Secure Hash Algorithm; E-Government.**

I. PENDAHULUAN

Dewasa ini pesatnya perkembangan dalam bidang teknologi informasi dan komunikasi telah mempengaruhi segala aspek kehidupan, salah satunya mendorong pemerintah untuk berinovasi dalam mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel. Saat ini pemerintah Indonesia sedang melakukan perubahan sistem pemerintahan dari sistem pemerintahan konvensional menjadi Sistem Pemerintahan Berbasis Elektronik (SPBE) atau sering dikenal dengan istilah *e-government*.

Untuk mendukung perkembangan dan pemanfaatan dalam bidang teknologi informasi dan komunikasi, pemerintah telah mengeluarkan beberapa peraturan yang bertujuan untuk mengatur dan memberikan rasa aman kepada pihak-pihak yang memanfaatkan perkembangan teknologi tersebut. Adapun peraturan yang telah dikeluarkan untuk menyikapi perkembangan teknologi informasi dan komunikasi sebagai berikut[1][2][3][4]:

- Undang-Undang Nomor 11 Tahun 2008, tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 82 Tahun 2012, tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Undang-Undang Nomor 19 Tahun 2016, tentang Perubahan Undang-Undang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 71 Tahun 2019, tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Sedangkan untuk mengatur penerapan SPBE, pemerintah telah mengelurakan Peraturan Presiden Nomor 95 Tahun 2018, tentang Sistem Pemerintahan Berbasis Elektronik[5].

Untuk para pelaku usaha mulai usaha mikro, kecil, menengah maupun besar, usaha perorangan maupun badan usaha, baik yang baru maupun yang telah lama berdiri, dalam mengurus perizinan berusaha saat ini dapat memanfaatkan *Online Single Submission* (OSS). Lembaga OSS merupakan lembaga pemerintah non kementerian yang menyelenggarakan urusan pemerintah pada bidang koordinasi penanaman modal. Hadirnya lembaga OSS ini didasari oleh diterbitkannya Peraturan Pemerintah (PP) Nomor 24 Tahun 2018, tentang Pelayanan Perizinan

Berusaha Terintegrasi Secara Elektronik. Dokumen perizinan berusaha yang diterbitkan oleh Lembaga OSS dalam bentuk dokumen elektronik disertai dengan tanda tangan elektronik yang dikonversikan dalam bentuk *QR Code*[6].

Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR) saat ini sedang membangun Sistem Informasi Jasa Konstruksi (SIJK) Terintegrasi. Lembaga Pengembangan Jasa Konstruksi (LPJK) yang merupakan lembaga non struktural yang berada di bawah dan bertanggung jawab kepada Menteri, dalam hal ini Menteri Pekerjaan Umum dan Perumahan Rakyat, LPJK menerbitkan Sertifikat Badan Usaha (SBU), Sertifikat Keahlian, dan Sertifikat Keterampilan yang dibutuhkan oleh para pelaku usaha pada sektor jasa konstruksi. Berdasarkan Surat Edaran (SE) Menteri PUPR Nomor 06/SE/M/2019, SBU, Sertifikat Keahlian, dan Sertifikat Keterampilan diterbitkan dalam bentuk elektronik, dihasilkan melalui aplikasi Sistem Informasi Konstruksi Indonesia (SIKI) berbasis web yang digunakan oleh LPJK. Sertifikat dalam bentuk elektronik yang diterbitkan oleh LPJK telah ditandatangani secara digital dan terdapat *QR Code* sebagai jalan untuk melakukan verifikasi keaslian sertifikat tersebut[7]. Hadirnya lembaga OSS dan SIJK terintegrasi ditengah-tengah para pelaku usaha khususnya pada sektor jasa konstruksi menunjukan keseriusan pemerintah dalam mewujudkan SPBE di Indonesia.

LPJK Nasional melalui surat nomor 1241-UM/LPJKN/IX/2020 menghimbau kepada asosiasi yang bergerak pada sektor jasa konstruksi untuk menyiapkan sistem sertifikasi yang dapat terintegrasi dengan SIKI LPJK[8]. Asosiasi Kontraktor Ketenagalistrikan Indonesia (AKLINDO) merupakan salah satu dari 72 asosiasi badan usaha yang bergerak pada sektor jasa kontruksi, AKLINDO mewadahi sejumlah badan usaha yang bergerak pada sektor jasa konstruksi yang tersebar di seluruh wilayah Indonesia. AKLINDO menerbitkan Kartu Tanda Anggota (KTA) yang diberikan kepada badan usaha yang bergabung dengan AKLINDO, KTA ini dibutuhkan oleh badan usaha untuk proses pengajuan SBU di LPJK. Saat ini AKLINDO belum memiliki sistem informasi asosiasi yang dapat terintegrasi dengan SIKI LPJK.

Maka pada penelitian ini, dibangun sistem informasi asosiasi AKLINDO yang dapat terintegrasi dengan SIKI LPJK dan juga dapat menghasilkan KTA disertai dengan tanda tangan digital yang dikoversikan dalam bentuk *QR Code* dari sebuah nilai hasil enkripsi dengan metode AES dan SHA-2, sehingga KTA aman dari tindakan pemalsuan. Dengan adanya sistem informasi asosiasi yang terintegrasi dengan SIKI LPJK diharapkan juga menjadi suatu bentuk dukungan terhadap pemerintah dalam mewujudkan SPBE di Indonesia.

Beberapa permasalahan yang dikaji pada penelitian ini, yaitu sebagai berikut:

1) Bagaimana membuat sistem informasi asosiasi yang mengimplementasikan tanda tangan digital?
2) Bagaimana algoritma AES dan SHA-2 dapat bekerja sebagai metode keamanan pada KTA AKLINDO?

II. KAJIAN TEORI

A. Sistem Informasi

Kebutuhan akan sistem informasi pada asosiasi jasa konstruksi saat ini, mendorong asosiasi untuk membangun sistem informasi yang nantinya dapat terintegrasi dengan SIKI LPJK. Sistem informasi merupakan kombinasi antara perangkat lunak (*software*), perangkat keras (*hardware*), basis data (*database*), jaringan komputer dan komunikasi data serta pengguna (*user*), yang tersusun secara sistematis, saling terhubung untuk mengumpulkan, mengubah, menyimpan, memproses, dan menyebarkan informasi dalam suatu bentuk organisasi[9]. Sistem informasi asosiasi ini dibangun untuk menghasilkan informasi yang dibutuhkan secara terstruktur, sistem informasi asosiasi yang dibangun menghasilkan berupa suatu dokumen KTA yang telah disertai dengan tanda tangan digital dengan bentuk *QR Code*.

B. Kriptografi

Kekuatan dari suatu tanda tangan digital bergantung pada metode kriptografi yang digunakan. Kriptografi (*Cryptography*) merupakan suatu ilmu atau seni yang mempelajari bagaimana cara menyimpan pesan, data dan/atau informasi agar tetap aman saat dikirimkan tanpa mengalami gangguan dari pihak lain[10]. Kriptografi memiliki 4 prinsip fundamental, yaitu[11]:

- Kerahasiaan (*Confidelity*)
- Keutuhan Data (*Data Integrity*)
- Keotentikan (*Authentication*)
- Anti Penyangkalan (*Non-Repudiation*)

Salah satu prinsip fundamental dari kriptografi yang menjadi syarat utama dari tanda tangan digital yaitu anti penyangkalan (*non-repudiation*) yang akan menjamin kebenaran dari suatu dokumen.

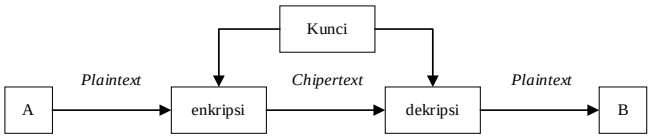
Fungsi yang mendasar dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyandian untuk mengubah pesan atau teks asli yang mudah dimengerti (*plaintext*) menjadi teks atau pesan yang tidak dapat dimengetri (*chipertext*), sedangkan dekripsi adalah proses untuk mengubah *chipertext* menjadi sebuah pesan atau teks asli (*plaintext*).

Berdasarkan jenis kuncinya terdapat 2 (dua) jenis algoritma kriptografi, yaitu:

- Algoritma Kriptografi Simetris (*Symmetric algorithms*)
- Algoritma Kriptografi Asimetris (*Asymmetric algorithms*)

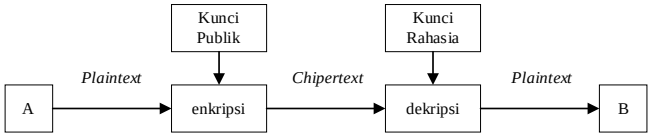
1) *Algoritma Kriptografi Simetris*: Biasa disebut algoritma kriptografi konvensional, merupakan algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsinya. Contoh algoritma kriptografi simetris

adalah RC2, RC4, RC5, RC5, IDEA, OTP, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, GOST, A5, Kasumi, Blowfish, DES, AES, dan lain-lain[11][12]. Gambar 1 menunjukan penggunaan kunci yang sama untuk proses enkripsi dan proses dekripsi[13].



Gambar 1. Proses Kriptografi Simetris

2) *Algoritma Kriptografi Asimetris*: Dikenal sebagai algoritma kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan proses dekripsinya. Pada algoritma ini kunci untuk proses enkripsi disebut dengan kunci publik (*public key*) sedangkan kunci untuk proses dekripsi disebut dengan kunci privat (*private key*). Contoh algoritma kriptografi asimetris adalah ECC, DH, Quantum, Rabin, ElGamal, DSA, RSA, dan lain-lainnya[11][12]. Gambar 2 menunjukan penggunaan kunci yang berbeda untuk proses enkripsi dan proses dekripsi, kunci publik digunakan pada proses enkripsi sedangkan kunci rahasia digunakan pada proses dekripsi[13].



Gambar 2. Proses Kriptografi Asimetris

C. Fungsi Hash

Fungsi *hash* merupakan suatu fungsi yang menerima masukan berupa *string* yang memiliki panjang sembarang dan mengkonversi masukan tersebut menjadi *string* yang memiliki panjang tetap dan umumnya lebih kecil dari panjang semula. Keluaran dari suatu fungsi *hash* disebut dengan *hash value* atau pesan ringkas (*message digest*). Fungsi *hash* merupakan fungsi satu arah yang dapat menghasilkan ciri (*signature*) dari data. Adanya perubahan 1 (satu) bit saja akan mengubah keluaran *hash* secara drastis. Fungsi *hash* biasanya digunakan untuk menjamin integritas dan *digital signature*. Fungsi *hash* bekerja mengubah pesan asli menjadi sebuah *message digest*, *message digest* yang telah dihasilkan tidak dapat dikembalikan menjadi pesan asli kembali[13]. Tabel I. merupakan daftar algoritma fungsi *hash*.

TABEL I
DAFTAR ALGORITMA FUNGSI *HASH*[13]

Algoritma	***Output size***	***Internal state size***	***Blok Size***	***Length Size***	***Word Size***	***Collision***
HAVAL	256/224/192/160/128	256	1024	64	32	*Yes*
MD2	128	384	128	No	8	*Almost*
MD4	128	128	512	64	32	*Yes*
MD5	128	128	512	64	32	*Yes*
PANAMA	256	8736	256	No	32	*With flaws*
RIPEMD	128	128	512	64	32	*Yes*
RIPEMD-128/256	128/256	128/256	512	64	32	*No*
RIPEMD-160/320	160/320	160/320	512	64	32	*No*
SHA-0	160	160	512	64	32	*Yes*
SHA-1	160	160	512	64	32	*With flaws*
SHA-256/224	256/224	256	512	64	32	*No*
SHA-512/384	512/384	512	1024	128	64	*No*
Tiger(2)-192/160/128	192/160/128	192	512	64	64	*No*
VEST-4/8	160/256	176/304	8	80	1	*No*
VEST-16/32	320/512	424/680	8	88	1	*No*
WHIRLPOOL	512	512	512	256	8	*No*

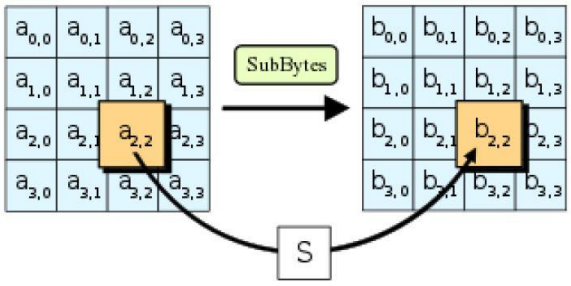
1) *Secure Hash Algorithm* (SHA): Algoritma *Secure Hash Algorithm* (SHA) adalah salah satu fungsi *hash* kriptografi yang dirancang oleh *National Security Agency* (NSA) dan diterbitkan oleh *National Institute of Standards and Technology* (NIST) sebagai *Federal Information Processing Standards* (FIPS) pada tahun 1993. Algoritma SHA dibuat berdasarkan fungsi *hash* MD4 dan desain modelnya menyerupai MD4[14]. Pada penelitian ini menggunakan SHA-256 yang akan menghasilkan *message digest* dengan panjang 256 *bits*.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

D. Algoritma Advanced Encryption Standard (AES)

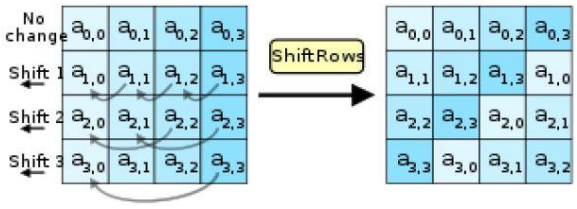
Advanced Encryption Standard (AES) merupakan pengembangan dari algoritma *Data Encryption Standard* (DES). AES disosialisasikan sebagai sebuah standar ekripsi baru pengganti algoritma DES oleh *National Institute of Standard and Technology* (NIST)[15]. AES termasuk dalam algoritma *block cipher* yang memiliki sifat simetris, menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. AES memiliki panjang kunci yang beragam untuk mengenkripsi/ mendekripsi suatu blok berukuran 128 bit. Berdasakan panjang kuncinya, ada 3 (tiga) tipe AES, yaitu: AES-128 dengan panjang kunci 128 bit, AES-192 dengan panjang kunci 192 bit, dan AES-256 dengan panjang kunci 256 bit. Panjang kunci akan mempengaruhi jumlah putaran (*round*) pada proses enkripsi dan dekripsi[16]. Operasi algoritma AES secara garis besar untuk proses enkripsi adalah sebagai berikut[17]:

- *AddRoundKey*, yaitu melakukan XOR antara *state* awal (*plaintext*) dengan *cipher key*, tahap ini disebut *initial round*.
- Putaran sebanyak *Nr* – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
  a. Sub Bytes, yaitu subsitusi *byte* dengan menggunakan tabel subsitusi (S-*box*).



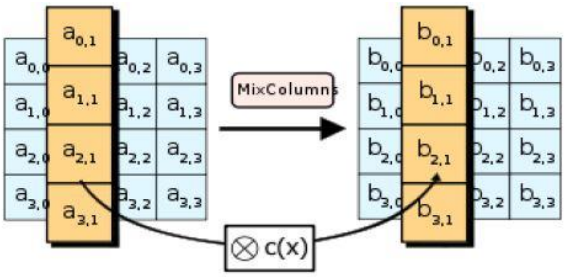
Gambar 3. Transformasi *SubBytes* dengan *S-Box*

  b. ShiftRows, yaitu pergeseran baris-baris *array state* secara *wrapping*, *byte* di setiap baris dari *state* dialihkan putaran ke kiri.



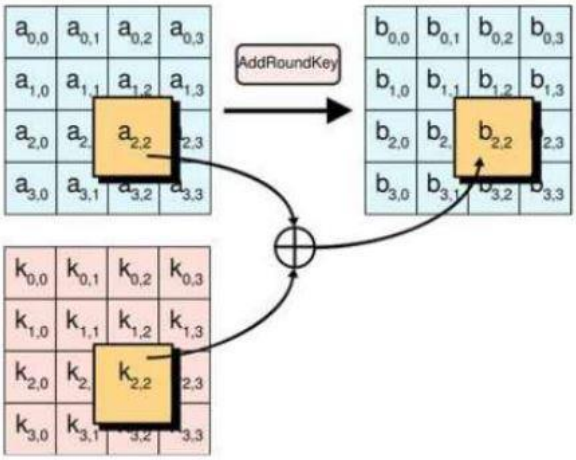
Gambar 4. *ShiftRows*

  c. MixColumns, yaitu mengacak data di masing-masing kolom *array state*. Fungsi *MixColumns* mengambil empat *byte* sebagai masukan dan empat *byte* sebagai keluaran, di mana setiap masukan akan mempengaruhi semua keluaran.



Gambar 5. *MixColumns*

  d. AddRoundKey, yaitu melakukan XOR antara *array state* saat ini dengan *round key*.



Gambar 6. *AddRoundKey*

- *Final Round*, yaitu proses putaran terakhir yang meliputi:
  a. SubBytes
  b. ShiftRows
  c. AddRoundKey

Algoritma AES yang digunakan pada penelitian ini yaitu dengan panjang kunci 256 *bit*, dengan panjang kunci 256 *bits* maka terdapat sejumlah 2^{256} = 1,16 x 10^{77} kemungkinan kunci.

E. QR Code

Quick Response (*QR*) *Code* merupakan penyempurnaan dari *barcode id* yang dapat menyimpan lebih banyak informasi. *QR code* pertama kali digunakan pada industri otomotif di Jepang yang kemudian menjadi sangat popular karena keterbacaannya sangat cepat dan kapasitas penyimpanan lebih besar dibandingkan dengan kode UPC standar. *QR code* memiliki ukuran terkecil 21x21 modul dan ukuran terbesar 177x177 modul. *QR code* mempunyai 4 level koreksi kesalahan, yaitu: L, M, Q, H. Untuk kapasitas *QR Code* bergantung rgantung pada versi dan tingkat koreksi kesalahan, serta jenis data yang dapat dikodekan oleh *QR Code* ada 3, yaitu: *numeric*, *alphanumeric*, dan *byte*[18].

III. TINJAUAN PUSTAKA

Pemanfaatan tanda tangan digital untuk meningkatkan aspek keamanan terhadap suatu dokumen, khususnya dokumen penting seperti: ijazah, transkrip, sertifikat keterampilan/ keahlian, sertifikat badan usaha, surat perizinan dan lainnya dipandang perlu. Terdapat beberapa penelitian terdahulu yang mendukung dalam penelitian mengenai pemanfaatan tanda tangan digital ini.

Menurut Maykin dan Pramote dalam penelitiannya yang berjudul *Paper-based Document Authentication using Digital Signature and QR Code*, beberapa dokumen berbasis kertas seperti: dokumen akta kelahiran, sim, dan paspor yang masih belum dapat digantikan secara efisen dengan dokumen berbasis elektronik, sehingga masih dapat dengan mudah terjadinya penipuan. Dengan implementasi tanda tangan digital dan *QR Code* pada dokumen berbasis kertas, maka akan timbul integritas antara pesan teks pada dokumen dengan pembuat dokumen[19].

Menurut Aji dalam penelitiannya yang berjudul Pengembangan Aplikasi Pengaman Dokumen Digital Memanfaatkan Algoritma *Advanced Encryption Standard*, RSA *Digital Signature* dan *Invisible Watermarking*, kemudahan dalam mendistribusikan dokumen melalui media komunikasi elektronik menimbulkan suatu kerentanan berupa penduplikasian dan publikasi dokumen tanpa seizin dari pemilik dokumen tersebut. Walaupun digitalisasi dokumen merupakan suatu kebutuhan, perlu dipikirkan juga apsek keamanannya. Kriptografi menjadi salah satu solusi untuk mengamankan dokumen digital, memanfaatkan algoritma AES untuk melindungi saat proses distribusi dokumen dan algoritma RSA *Digital Signature* untuk menjamin otentikasi pengirim dan penerima dokumen yang memberikan layanan *non-repudiation*[17].

Ankit dan Pavithr dalam penelitiannya yang berjudul *Degree Certificate Authentication using QR Code and Smartphone*, membuat sistem yang menghasilkan sertifikat gelar yang dapat diverifikasi menggunakan *QR Code* melalui aplikasi *smartphone*. *QR Code* berisikan tanda tangan digital dari otoritas institusi pendidikan. Sistem ini dibuat untuk mencegah pembuatan sertifikat gelar palus di institusi pendidikan[18].

Abdul dan Abdul dalam penelitiannya yang berjudul Tanda Tangan Digital Menggunakan *QR* Code dengan Metode *Advanced Encryption Standard*, membuat sistem yang menerapkan tanda tangan digital pada dokumen pengambilan barang. Tanda tangan digital berfungsi sebagai otentikasi tanda tangan pimpinan dan juga verifikasi dokumen pengambilan barang yang sah. Pada penelitian ini didapatkan akurasi klasifikasi *QR Code* menggunakan *naïve bayes classifier* sebesar 90% dengan *precision* positif sebesar 80% dan *precision* negatif sebesar 100%[20].

Menurut Yusuf, Erwin, dan Dewa dalam penelitian yang berjudul Implementasi Algoritma Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital, tanda tangan digital dapat digunakan untuk pembuktian secara matematis bahwa data tidak mengalami modifikasi secara ilegal[21].

Selanjutnya Fitri, Yoga, Dede, dan Imas dalam penelitian yang berjudul Implementasi Skema *QR-Code* dan *Digital Signature* menggunakan Kombinasi Algoritma RSA dan AES untuk Penggunaan Data Sertifikat Elektronik, mengimplementasikan tanda tangan digital pada *file* sertifikat elektronik untuk kegiatan webinar dan kursus *online*. Tanda tangan digital pada *file* sertifikat elektronik ini memanfaatkan fungsi *hashing* SHA-3 dan super enkripsi kombinasi antara RSA dengan AES 128 mode operasi CBC. Tanda tangan digital disisipkan pada *file* sertifikat elektronik dengan skema *QR Code*. Penelitian ini mendapatkan waktu enkripsi dan dekripsi dibawah 0,1 mili detik, nilai entropi sebesar 4,96, dan juga nilai *avalanche effect* sebesar 40,61% membuktikan perubahan kode *chipertext* sudah sangat acak[22].

IV. ANALISIS DAN RANCANGAN SISTEM

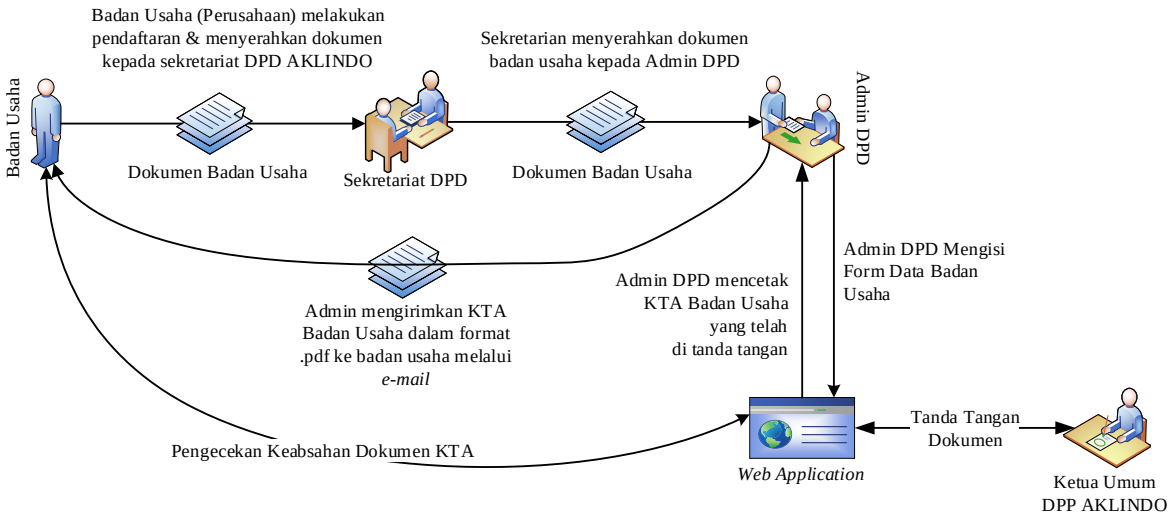
Aplikasi sistem informasi asosiasi AKLINDO harus dapat menghasilkan KTA yang dilengkapi tanda tangan digital dengan menerapkan metode AES dan SHA-2. Pada penelitian ini, data yang digunakan adalah data badan usaha anggota AKLINDO Provinsi Jawa Barat. Data ini adalah data informasi umum mengenai badan usaha.

Pada tahap perancangan aplikasi sistem informasi asosiasi AKLINDO dimulai dari pembuatan *flowchart* proses bisnis, hak akses pengguna (*user*), perancangan *use case diagram*, perancangan *user interface*, *flowchart* enkripsi dan dekripsi dan basis data (*database*). Dalam penggunaannya, aplikasi sistem informasi asosiasi AKLINDO setiap pengguna memiliki hak akses yang berbeda-beda.

A. Flowchart Proses Bisnis

Gambar 6 menunjukan alur dari proses bisnis yang ada pada Asosiasi AKLINDO Provinsi Jawa Barat.

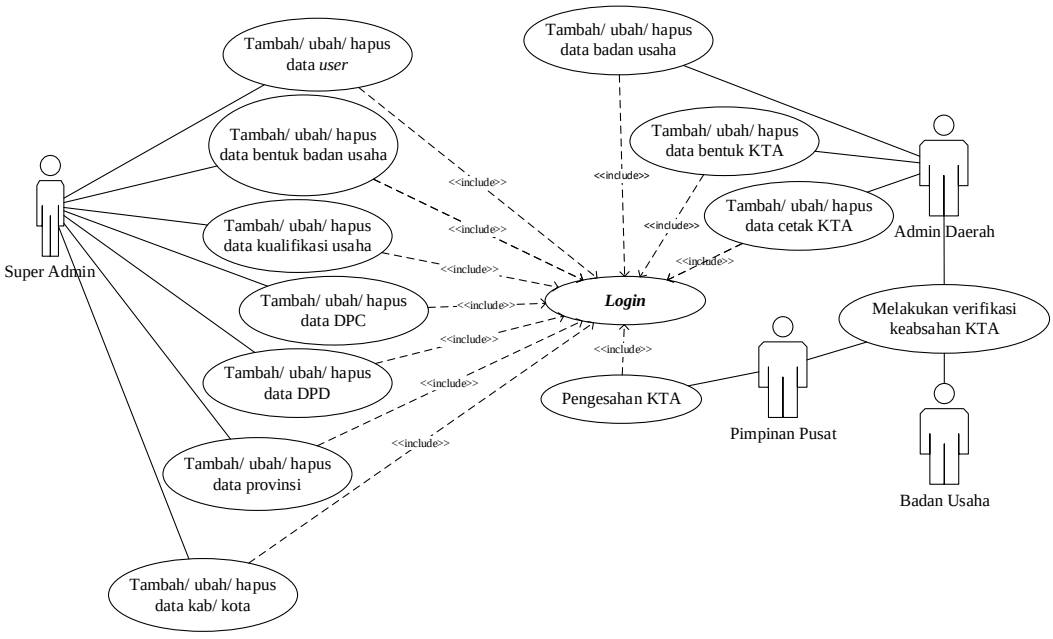
p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 6. *Flowchart* Proses Bisnis

B. Use Case Diagram

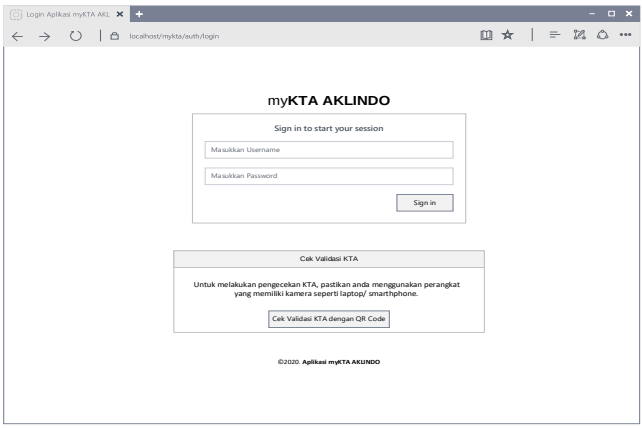
Pada aplikasi sistem informasi asosiasi AKLINDO, setiap pengguna (*user*) memiliki hak aksesnya tersendiri, hal ini digambarkan pada Gambar 7 *Use Case Diagram*. Admin pusat (superadmin) memiliki hak akses, seperti: tambah/ ubah/ hapus data pengguna (*user*), data bentuk badan usaha, data kualifikasi badan usaha, data DPC, data DPD, data provinsi, dan data kab/ kota. Untuk admin daerah (admin) memiliki hak akses, seperti: tambah/ ubah/ hapus data badan usaha, data bentuk KTA, data cetak KTA, dan verifikasi keabsahan KTA. Untuk pimpinan pusat memiliki hak akses, seperti: pengesahan KTA dan verifikasi keabsahan KTA. Sedangkan untuk pengguna badan usaha hanya memiliki hak akses untuk verifikasi keabsahan KTA.



Gambar 7. *Use Case Diagram* Super Admin, Admin Daerah, Pimpinan Pusat, dan Badan Usaha

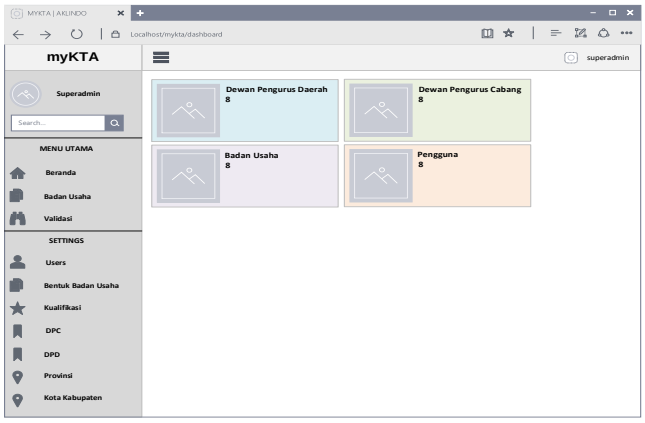
C. Rancangan User Interface

Berikut ini beberapa perancangan *user interface* pada aplikasi sistem informasi asosiasi yang telah dibangun seperti Gambar 8 menggambarkan halaman *login* yang akan digunakan oleh setiap *user*.



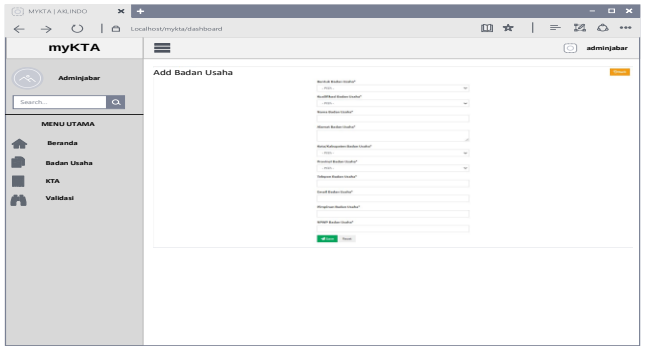
Gambar 8. *Use Interface Login*

Untuk Gambar 9 menggambarkan halaman *dashboard* ketika melakukan *login* sebagai superadmin, terdapat beberapa perbedaan hak akses pada masing-masing aku *user*.



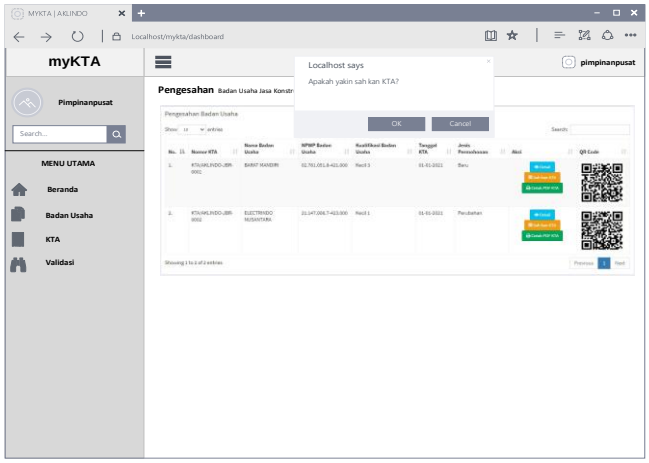
Gambar 9. *Use Interface Dashboard* Superadmin

Untuk Gambar 10 menggambarkan halaman tambah data badan usaha ketika *user* melakukan *login* sebagai admin.



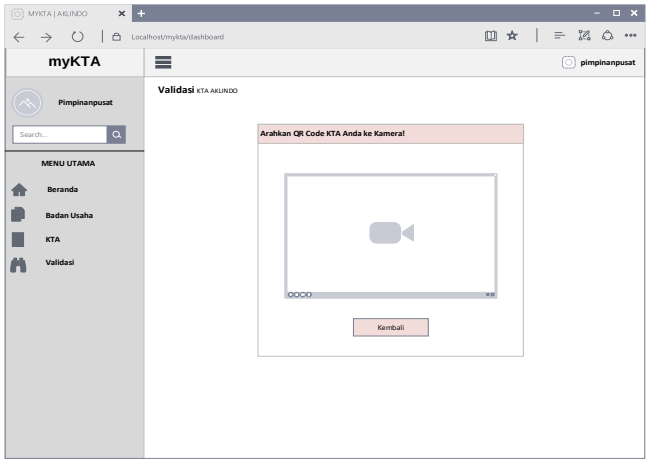
Gambar 10. *Use Interface* Tambah Badan Usaha

Pada Gambar 11 menggambarkan halaman menu pengesahan KTA yang hanya dapat di akses ketika *user* melakukan *login* sebagai pimpinanpusat.



Gambar 11. *Use Interface* Menu Pengesahan KTA

Pada Gambar 12 menggambarkan halaman untuk validasi KTA.

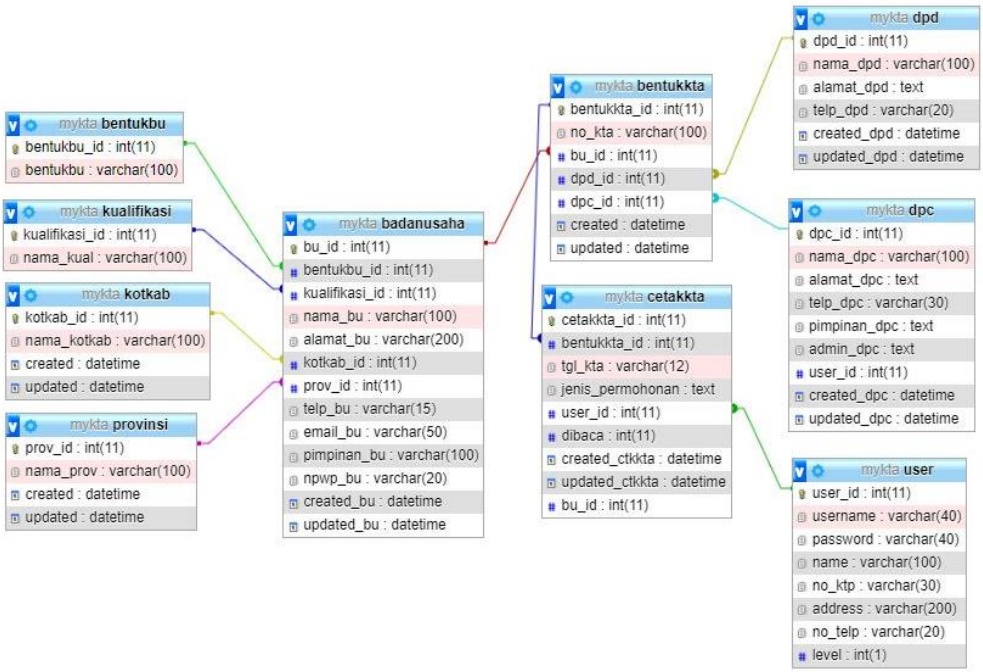


Gambar 12. *Use Interface* Validasi KTA

D. Perancangan Basis Data

Sistem informasi asosiasi AKLINDO ini menggunakan data dari asosiasi AKLINDO Provinsi Jawa Barat. Gambar 13 menunjukan hubungan antar tabel pada 1 (satu) *database* sistem informasi asosiasi AKLINDO, yang terdiri dari tabel *user*, tabel dpc, tabel dpd, tabel bentuk kta, tabel cetakkta, tabel badanusaha, tabel bentukbu, tabel kualifikasi, tabel kotkab, dan tabel provinsi.

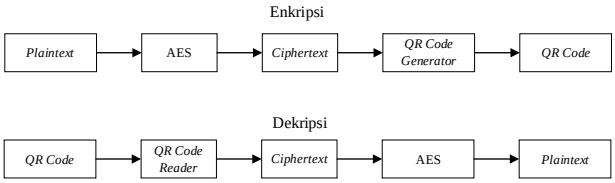
p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 13. Relasi Antara *Table Database*

E. Perancangan Tanda Tangan Digital

Dalam perancangan tanda tangan digital terdapat 2 (dua) proses utama, yaitu proses *sign* dan proses *verify*. Pertama pada proses *sign*, data akan melalui proses *hashing* menggunakan fungsi *hash* SHA-256, lalu akan mendapatkan nilai *hash* dari data. Selanjutnya *message digest* dari data masuk pada proses enkripsi menggunakan kunci privat dari algoritma AES. Pada proses enkripsi dengan AES ini akan dihasilkan kode tanda tangan digital, lalu dikonverikan menjadi *QR Code* melalui *QR Code generator*. Gambar *QR Code* yang dihasilkan lalu disisipkan pada dokumen KTA. Untuk proses *verify* dimana adalah kebalikan dari proses *sign*, maka *QR Code* akan terlebih dahulu dibaca menggunakan *QR Code reader*, lalu kode tanda tangan digital tersebut melewati proses dekripsi dengan AES, maka akan menghasilkan *message digest*.

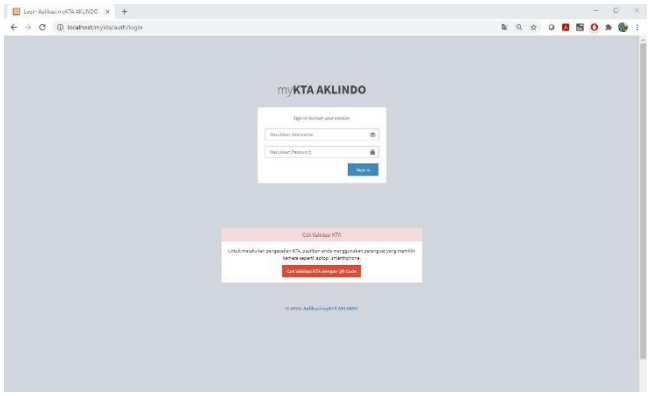


Gambar 14. Proses Enkripsi dan Dekripsi

V. HASIL PENELITIAN DAN EVALUASI

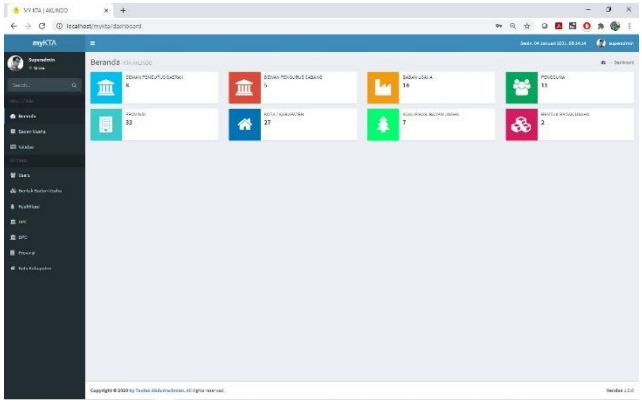
A. Hasil Implementasi Perancangan

Hasil dari perancangan sistem informasi asosiasi AKLINDO yang dibahas pada bab sebelumnya, menghasilkan sebuah sistem informasi asosiasi sebagai berikut: Gambar 15 menunjukan halaman *form login* yang digunakan oleh setiap *user*.



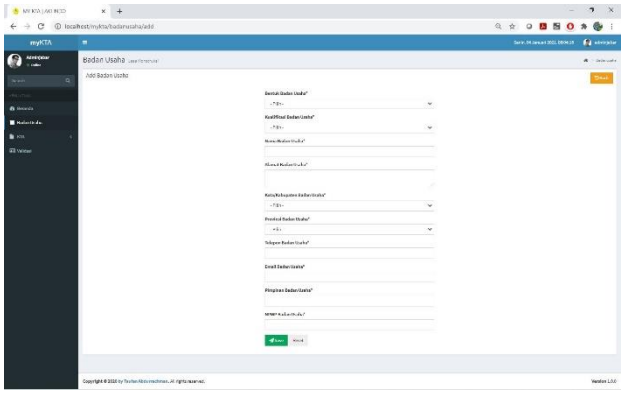
Gambar 15. Halaman *Form Login*

Selanjutnya pada Gambar 16 menunjukan halaman *dashboard* superadmin selaku admin pusat yang memiliki hak akses yaitu dapat melakukan aktivitas, penambahan, perubahan, dan penghapusan data, seperti: data *users*, data bentuk badan usaha, data kualifikasi, data DPC, data DPD, data provinsi, data kabupaten/ kota, cek validasi KTA dan melihat data badan usaha



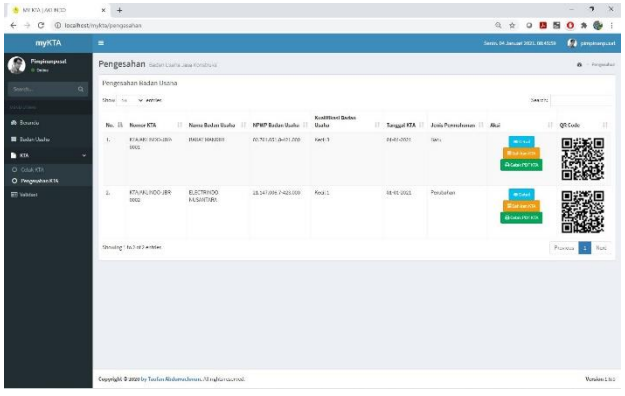
Gambar 16. Halaman *Dashboard* Superadmin

elanjutnya pada Gambar 17 menunjukan halaman tambah data badan usaha. *User* dengan status admin daerah (admin) dapat mengelola data yaitu menambah, mengubah, dan menghapus data, seperti: data badan usaha, data bentukkta, dan data cetakkta.



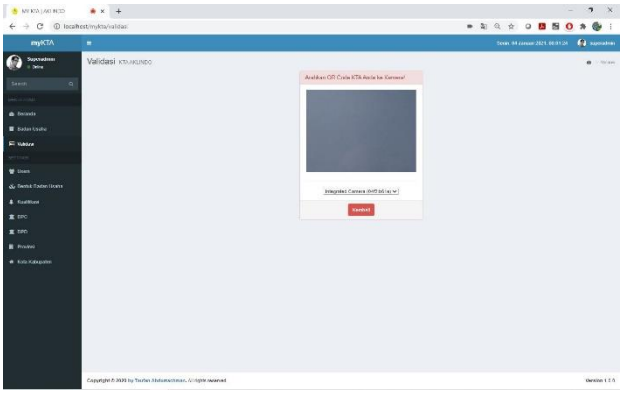
Gambar 17. Halaman Tambah Data Badan Usaha

Selanjutnya ketika *user* melakukan *login* sebagai pimpinan pusat, *user* dapat melakukan pengesahan KTA, melihat data pengesahan KTA dan melihat detail data KTA yang akan disahkan melalui halaman pengesahan KTA yang dapat dilihat pada Gambar 18.



Gambar 18. Halaman Data Pengesahan KTA

Selanjutnya, untuk melakukan pengecekan validitas KTA dapat memanfaatkan *QR Code* sebagai representasi dari suatu tanda tangan yang disematkan pada setiap KTA. Gambar 19 menunjukan halaman untuk melakukan pengecekan validitas KTA.



Gambar 19. Halaman Validasi KTA

B. Pengujian dan Pembahasan

Pada tahap pengujian aplikasi sistem informasi asosiasi AKLINDO ini, pengujian menggunakan metode *black box testing* secara lokal untuk menguji kesesuaian antara masukkan dan keluaran dari sistem, pengujian terhadap sistem yang telah dibangun hanya dilakukan terhadap fungsionalitas dari sistem tersebut. Hasil dari pengujian menggunakan metode *black box* dapat dilihat pada Tabel II, dari hasil pengujian dapat disimpulkan bahwa sistem informasi asosiasi AKLINDO dapat berjalan dengan baik. Keluaran dari setiap skenario pengujian untuk setiap fungsionalitas telah menghasilkan keluaran yang sesuai dengan yang diharapkan.

TABEL II
PENGUJIAN FUNGSIONALITAS SISTEM

No	Uji Fungsionalitas	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan	
				Berhasil	Gagal
1	*Login*	*Login* dengan *username* dan *password* superadmin	Masuk ke halaman *dashboard* superadmin	V	
		Login dengan *username* dan *password* admin	Masuk ke halaman *dashboard* admin	V	
		Login dengan *username* dan *password*	Masuk ke halaman *dashboard* pimpinanpusat	V	

No	Uji Fungsionalitas	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan	
				Berhasil	Gagal
		pimpinanpusat			
2	*User*	Tambah *user*	Masuk ke halaman tambah *user* dan data *user* tersimpan ke dalam *database*	V	
		Hapus *user*	Masuk ke halaman data *user* dan data *user* terhapus dari *database*	V	
3	Kualifikasi	Tambah kualifikasi	Masuk ke halaman tambah kualifikasi dan data kualifikasi tersimpan ke dalam *database*	V	
		Hapus kualifikasi	Masuk ke halaman data kualifikasi dan data kualifikasi terhapus dari *database*	V	
4	Badan Usaha	Tambah badan usaha	Masuk ke halaman tambah badan usaha dan data badan usaha tersimpan ke dalam *database*	V	
		Ubah badan usaha	Masuk ke halaman ubah badan usaha dan data badan usaha terbaru tersimpan ke dalam *database*	V	
		Hapus badan usaha	Masuk ke halaman data badan usaha dan data badan usaha terhapus dari *database*	V	
		Detail badan usaha	Masuk ke halaman detail badan usaha	V	
5	Cetak KTA	Tambah cetak KTA	Masuk ke halaman tambah cetak kta dan data cetak kta tersimpan ke dalam *database*	V	
		Ubah cetak KTA	Masuk ke halaman ubah cetak kta dan data cetak kta terbaru tersimpan ke dalam *database*	V	
		Hapus cetak KTA	Masuk ke halaman data cetak kta dan data cetak kta terhapus dari *database*	V	
		Export pdf KTA	Dokumen digital KTA siap diunduh	V	
6	Pengesahan	Pengesahan KTA	Masuk ke halaman pengesahan KTA dan *QR Code* terbentuk	V	
		Detail KTA	Masuk ke halaman detail KTA	V	
7	Verifikasi	Verifikasi KTA	Masuk ke halaman verifikasi dan mengakses *webcam*/ kamera	V	

Pengujian selanjutnya yaitu pengujian enkripsi dan melihat *response time* yang diperlukan oleh sistem untuk melakukan proses enkripsi dan menghasilkan *QR Code*. *Test Case* yang digunakan pada pengujian ini dapat dilihat pada Tabel III.

TABEL III
TEST CASE PENGUJIAN ENKRIPSI DAN RESPONSE TIME

Plaintext	diisi dengan nomor KTA AKLINDO yang telah ditentukan untuk setiap badan usaha sebagai *input* pengujian
Key	namakuloaklindo2008
Metode	SHA256 dan AES 256 CBC

TABEL IV
PENGUJIAN ENKRIPSI DAN *RESPONSE TIME*

Uji Kasus	*Input* Pengujian	Hasil Enkripsi	*Response Time* (*μs*)	Hasil *QR Code*
1	KTA/AKLINDO-JBR-0001	ZMc8DtMNZx3vgXiVgkZkBs0adX6wdZXgkESDeR5EU4Y=	0,0000178	
2	KTA/AKLINDO-JBR-0002	ZMc8DtMNZx3vgXiVgkZkBgCguq0iDAlQ1kWbdAkQ/f4=	0,0000219	
3	KTA/AKLINDO-JBR-0003	ZMc8DtMNZx3vgXiVgkZkBs73/rBoqLoJZ96QM5PSiDI=	0,0000169	
4	KTA/AKLINDO-JBR-0004	ZMc8DtMNZx3vgXiVgkZkBk6JmUiluNdgiN+CUAZ1zl4=	0,0000171	
5	KTA/AKLINDO-JBR-0005	ZMc8DtMNZx3vgXiVgkZkBgXSIpcCElcZAelS2jw6n2M=	0,0000181	
6	KTA/AKLINDO-JBR-0006	ZMc8DtMNZx3vgXiVgkZkBkplth8i58gW+h8/Aqic3vc=	0,0000190	

Pada Tabel IV dapat dilihat hasil pengujian *response time* dan hasil pembentukan *QR Code* dengan menggunakan *test case* yang telah ditentukan.

Pada Tabel IV dapat dilihat bahwa ketika dilakukan pengujian secara lokal didapatkan *response time* kurang dari 0,00003*μs* dan *input* pengujian dapat di enkripsi dengan baik menggunakan metode SHA-2 dan AES 256.

Selanjutnya melakukan pengujian *avalanche effect* yang dapat digunakan sebagai parameter pengujian untuk menganalisis tingkat keamanan pada algoritma kriptografi kunci simetris dan fungsi *hash*. Perubahan pada *plaintext* maupun pada *key* walaupun hanya 1 bit, akan menghasilkan perubahan yang signifikan pada hasil dari *chipertext*. Rumus untuk menghitung nilai *avalanche effect* menggunakan persamaan berikut ini[23]:.

$$avalanche\ effect = \frac{jumlah\ perubahan\ bit}{jumlah\ seluruh\ bit\ awal}\ x\ 100\%$$

Avalanche effect yang bertujuan untuk membandingkan seberapa besar perubahan yang terjadi ketika *plaintext* berubah, sehingga dapat menilai tingkat efektifitas dari penerapan tanda tangan digital ini.

- Pengujian 1, melakukan perubahan 3 (tiga) karakter pada *key*, yaitu mengubah setiap karakter ‘a’ menjadi ‘@’. Hasil perubahan dan nilai *avalanche effect* dapat dilihat pada Tabel V.

TABEL V
TEST CASE DAN HASIL PENGUJIAN *AVALANCHE EFFECT* 1

Plaintext awal	KTA/AKLINDO-JBR-0001
Key	namakuloaklindo2008
Hasil enkripsi *plaintext awal*	ZMc8DtMNZx3vgXiVgkZkBs0adX6wd ZXgkESDeR5EU4Y=
Perubahan *key*	n@m@kulo@klindo2008
Hasil perubahan enkripsi *plaintext*	v3syOKgemp5OAfJpSKf4SfyOLGbiHZl OismzvU4z7yQ=
Perubahan bit	137bit
Avalanche effect	38,92%

- Pengujian 2, melakukan perubahan 2 (dua) karakter pada *plaintext*, yaitu mengubah setiap karakter 'A' menjadi 'a'. Hasil perubahan dan nilai *avalanche effect* dapat dilihat pada Tabel VI.

TABEL VI
TEST CASE DAN HASIL PENGUJIAN *AVALANCHE EFFECT* 2

Plaintext awal	KTA/AKLINDO-JBR-0001
Key	namakuloaklindo2008
Hasil enkripsi *plaintext awal*	ZMc8DtMNZx3vgXiVgkZkBs0adX6wd ZXgkESDeR5EU4Y=
Perubahan *plaintext*	KTa/aKLIND0-JBR-0001
Hasil perubahan enkripsi *plaintext*	Ijumn9iatHUrLTOv+INR/W6ODvoE/2ep Xj3az6sL9q0=
Perubahan bit	138bit
Avalanche effect	39,2%

- Pengujian 3, melakukan perubahan 2 (dua) karakter pada *key*, yaitu mengubah setiap karakter 'k' menjadi 'X'. Hasil perubahan dan nilai *avalanche effect* dapat dilihat pada Tabel VII.

TABEL VII
TEST CASE DAN HASIL PENGUJIAN *AVALANCHE EFFECT* 3

Plaintext awal	KTA/AKLINDO-JBR-0001
Key	namakuloaklindo2008
Hasil enkripsi *plaintext awal*	ZMc8DtMNZx3vgXiVgkZkBs0adX6wd ZXgkESDeR5EU4Y=
Perubahan *key*	namaXuloaXlindo2008
Hasil perubahan enkripsi *plaintext*	7eRCh+tTRMCkhY3bJIvEU5HUAzOkV OtwVzgNrOalQCk=
Perubahan bit	145bit
Avalanche effect	41,19%

- Pengujian 4, melakukan perubahan 4 (empat) karakter pada *key*, yaitu mengubah setiap karakter 'a' menjadi 'A' dan setiap karakter 'k' menjadi 'X'. Hasil perubahan dan nilai *avalanche effect* dapat dilihat pada Tabel VIII.

TABEL VIII
TEST CASE DAN HASIL PENGUJIAN *AVALANCHE EFFECT* 4

Plaintext awal	KTA/AKLINDO-JBR-0001
Key	namakuloaklindo2008
Hasil enkripsi *plaintext awal*	ZMc8DtMNZx3vgXiVgkZkBs0adX6wd ZXgkESDeR5EU4Y=
Perubahan *key*	nAmAXuloAXlindo2008
Hasil perubahan enkripsi *plaintext*	SyLfNVgJkd4lp31CmeFP48GTR/U9Qm 6/5thyERS7+jc=
Perubahan bit	157bit
Avalanche effect	44,6%

Berdasarkan pengujian *avalanche effect* yang telah dilakukan, maka didapat nilai rata-rata *avalanche effect* sebesar 40,97%. Dari nilai rata-rata *avalanche effect* yang didapat, besarnya perubahan yang terjadi pada *plaintext* dan *key* berpengaruh terhadap hasil *chipertext* dari proses enkripsi, maka algoritma AES cukup efektif digunakan tanda tangan digital pada KTA AKLINDO.

VI. SIMPULAN

Berdasarkan pembahasan mengenai hasil implementasi, pengujian dan evaluasi yang telah dilakukan pada aplikasi sistem informasi asosiasi AKLINDO, maka disimpulkan bahwa prototipe aplikasi sistem informasi asosiasi AKLINDO dapat berjalan dengan baik. Metode keamanan padat KTA menggunakan metode AES dan SHA-2 dapat diimplementasikan dengan baik pada sistem dan telah dapat menghasilkan KTA yang dilengkapi dengan *QR Code* sebagai representasi dari tanda tangan digital. *Response time* dari sistem untuk melakukan 1 (satu) proses enkripsi memerlukan rata-rata waktu kurang dari 0,00003μs dan nilai rata-rata *avalanche effect* sebesar 40,97% yang menunjukan seberapa acak perubahan yang terjadi pada *chipertext*.

Saran untuk penelitian kedepannya terkait dengan penggunaan tanda tangan digital pada kartu tanda anggota asosiasi yang bergerak dalam bidang jasa konstruksi, yaitu: dapat melakukan penelitian lebih lanjut untuk menetukan algoritma kriptografi lain yang cocok untuk diterapkan pada sistem informasi asosiasi sebagai metode keamanan data pada KTA. Selin itu dapat ditemukan kombinasi algoritama kriptografi yang lebih baik untuk proses enkripsi dan dekripsi data, sehingga keamanan data anggota asosiasi jasa konstruksi lebih terjamin. Dan diharapkan pada pengembangan aplikasi sistem informasi asosiasi jasa konstruksi kedepannya perlu dilakukan penyesuaian, studi lebih lanjut, dan penambahan fitur-fitur lainnya

UCAPAN TERIMA KASIH

Terima kasih kepada Dewan Pengurus Daerah Asosiasi Kontraktor Ketenagalistrikan Indonesia Provinsi Jawa Barat yang telah memberikan kesempatan untuk melaksanakan dan menyediakan data pada penelitian Tesis ini.

DAFTAR PUSTAKA

[1] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Jakarta, 2008.

[2] Pemerintah Republik Indonesia, *Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Jakarta, 2012.

[3] Pemerintah Indonesia, *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Jakarta, 2016.

[4] Pemerintah Republik Indonesia, *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Jakarta, 2019.

[5] Pemerintah Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik*. Jakarta, 2018.

[6] Pemerintah Republik Indonesia, *Peraturan Pemerintah Republik Indonesia Nomor 24 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik*. Jakarta, 2018.

[7] Menteri Pekerjaan Umum dan Perumahan Rakyat, "Surat Edaran Nomor 06/SE/M/2019 Tentang Sertifikat Badan Usaha, Sertifikat Keahlian, dan Sertifikat Keterampilan Dalam Bentuk Elektronik," Jakarta, 2019.

[8] Lembaga Pengembangan Jasa Konstruksi, "1241-UM/LPJKN/IX/2020 tentang Pengembangan Sistem Informasi Terintegrasi pada Masing-Masing Asosiasi dengan SIKI LPJK," 2020.

[9] A. Irawan, A. Hasna, and R. Pahlevi, "Sistem Informasi Perdagangan Pada PT Yoltran Sari Menggunakan Php Berbasis Web," *Positif*, vol. 1, no. 2, pp. 8–15, 2016.

[10] I. C. Sari, "Optimasi Pemodelan Enkripsi Data dengan Menggunakan Algoritma Kriptografi RSA sebagai Keamanan Data E-Mail," M. Kom. tesis, Universitas Sumatera Utara, 2020.

[11] N. W. Nasution, "Analisis Kinerja Rprime RSA dan Multi-Factor RSA Dalam Mengamankan Pesan," M. Kom. tesis, Universitas Sumatera Utara, 2019.

[12] A. Hadi, "Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Menggunakan Digital Signature dengan Algoritma Kurva Eliptik," M. Si. tesis, Universitas Diponegoro, 2011.

[13] E. C. Prabowo and I. Afrianto, "Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital," *Komputa J. Ilm. Komput. dan Inform.*, vol. 6, no. 2, pp. 83–90, 2017, doi: 10.34010/komputa.v6i2.2481.

[14] H. Agung and Ferry, "Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 34–45, 2016.

[15] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 182, 2020, doi: 10.30865/jurikom.v7i1.1960.

[16] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 2, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.

[17] A. S. Sukarno, "Pengembangan Aplikasi Pengamanan Dokumen Digital Memanfaatkan Algoritma Advance Encryption Standard, RSA Digital Signature dan Invisible Watermarking," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013*, 2013, pp. 1–8, ISSN:1907-5022.

[18] A. Singhal and R. S. Pavithr, "Degree Certificate Authentication using QR Code and Smartphone," *Int. J. Comput. Appl.*, vol. 120, no. 16, pp. 38–43, 2015, doi: 10.5120/21315-4303.

[19] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," in *4TH International Conference on Computer Engineering and Technology*, 2012, vol. 40, no. January, pp. 94–98.

[20] A. G. P. Suratma and A. Azis, "Tanda Tangan Digital Menggunakan Qr Code Dengan Metode Advanced Encryption Standard," *Techno*, vol. 18, no. 1, pp. 59–68, 2017.

[21] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.

[22] F. Nuraeni, Y. H. Agustin, D. Kurniadi, and I. D. Ariyanti, "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik," in *Seminar Nasional Teknologi Informasi, Komunikasi dan Industri (SNTIKI) 12*, 2020, pp. 43–52.

[23] Sugiyanto and R. K. Hapsari, "Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," *J. Ultim.*, vol. 8, no. 2, pp. 131–138, 2016, doi: 10.31937/ti.v8i2.528.