ISSN 2085-4579

Rancang Bangun Aplikasi Naskah Dinas Elektronik Berbasis Web Menggunakan WDLC

Nur Annisa Kadarwati Febriyani[1], Raden Budiarto Hadiprakoso[2]
[1,2]Rekayasa Kriptografi, Poltek Siber dan Sandi Negara, Bogor, Indonesia
[2]raden.budiarto@poltekssn.ac.id

Diterima 03 September 2020
Disetujui 06 November 2020

***Abstract*—In the modern era of technological development, the application of electronic official script management is a solution to the administrative and communication challenges of agencies during the pandemic, such as today, where administrative work needs to be done from home (work from home). With the condition of a high level of need, the management of official manuscripts in the XYZ organization still uses conventional methods. So, this raises obstructed letter distribution and loss documents problem, and waste of paper use. We propose the Electronic Service Manuscript Management Application to replace the official script management process that previously applied conventional methods to using electronic methods to solve this problem. Besides, we also implement security aspects in the SHA-512 algorithm to fulfill authentication, AES-128 to meet confidentiality, and RSA2048 to meet integrity and non-repudiation. Apart from the security aspect, functionally, the system is built based on the Guidelines for Electronic Service Manuscripts, which are tailored to the organization's needs. The system development uses the Web Development Life Cycle (WDLC) methodology using the Yii2 framework. From the research results, it is concluded that the Electronic Service Manuscript Management Application has been built according to the needs of the organization and can be a security alternative in the official script management process.**

***Index Terms*—digital signature; encryption; official script management; WDLC**

I. PENDAHULUAN

Pengelolaan naskah dinas merupakan komponen yang memegang peranan penting karena menjadi sarana pencapaian tujuan dari organisasi atau instansi [1]. Hal ini dikarenakan naskah dinas adalah alat komunikasi kedinasan yang dibuat oleh pejabat yang berwenang pada instansi pemerintah, perguruan tinggi negeri, BUMN/BUMD untuk menyelenggarakan tugas pemerintahan dan pembangunan [2]. Kondisinya saat ini, instansi pemerintahan memiliki 2 jenis media pengelolaan naskah dinas yakni media konvensional [3] dan media elektronik [4]. Organisasi xyz dalam pengelolaan naskah dinasnya menggunakan media konvensional. Diketahui dari hasil diskusi dengan pihak terkait kondisi persuratan masih menggunakan kertas sebagai media persuratan, pengagendaan yang menggunakan *Microsoft Access*, dan distribusi surat yang masih menggunakan tenaga staf. Hal ini menimbulkan kendala terhambatnya alur penanganan surat karena pimpinan yang tidak berada dikantor, hilangnya dokumen lembar kontrol disposisi, dan pemborosan penggunaan kertas. Permasalahan selanjutnya timbul dari kondisi pandemi saat ini, yang menyebabkan terhambatnya pengelolaan surat, distribusi surat, bahkan pengambilan keputusan terhambat karena pengelolaan naskah dinas yang menggunakan media kertas. Hal ini dapat disimpulkan, bahwa dibutuhkan penyelesaian terhadap permasalahan ini.

Fenomena permasalahan juga terjadi pada organisasi atau perusahaan lain, sehingga mengundang para peneliti untuk mencoba menyelesaikannya. Di antaranya adalah Sukadi dan Veronica [1], Rosyanto [5] , Guntari dan Setiawan [6]. Mereka menyatakan bahwa aplikasi pengelolaan naskah dinas dapat menjadi solusi dalam menyelesaikan permasalahan yang serupa. Selain dari penelitian terkait, pemerintah mengatur mengenai hal yang perlu dipenuhi oleh instansi ketika ingin menerapkan pengelolaan naskah dinas secara elektronik pada Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 Tentang Pedoman Umum Tata Naskah Dinas Elektronik (TNDE) di Lingkungan Instansi Pemerintah. Pedoman Umum TNDE berisikan aturan umum dan acuan [4] dalam mengimplementasikan TNDE. Peraturan ini memuat kebutuhan fungsional dan non fungsional dari sistem TNDE. Kebutuhan tersebut selanjutnya disesuaikan dengan kebutuhan objek penelitian. Berdasarkan kebutuhan yang dimuat pada peraturan ini terdapat salah satu persyaratan yakni legalitas dokumen yang dibuat di dalam sistem yang perlu disesuaikan dengan aturan yang berlaku.

Pemenuhan aspek legalitas naskah dinas, akan dilakukan dengan menerapkan salah satu prinsip yang

dimuat dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE merupakan penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE. Selanjutnya, pada pasal 2 ayat 1 diterangkan bahwa SPBE dilaksanakan dengan berbagai prinsip, yang salah satunya prinsip keamanan. Secara lebih lanjut, prinsip keamanan dimuat dalam pasal 40 ayat 1 yang mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi [7].

Guna memenuhi aspek keamanan yang sesuai dengan SPBE, akan diterapkan Algoritme AES 128 dan RSA 2048. Kedua algoritme ini terbukti dapat diimplementasikan berdasarkan penelitian Siregar, Junaeti, dan Hayatno [8]. Algoritme AES digunakan untuk menunjang aspek kerahasiaan pada dokumen disposisi dan algoritma RSA menunjang aspek keutuhan, keaslian, dan kenirsangkalan. Pemilihan algoritme AES 128 dan RSA 2048 didasarkan pada standar NIST yang menyatakan bahwa algoritme ini dinyatakan aman oleh NIST [9]. Selain AES 128 dan RSA 2048, akan diimplementasikan algoritme SHA 512 yang akan digunakan untuk pengamanan *password*. Dasar pemilihan SHA 512 yakni merupakan algoritme fungsi *hash* yang diakui keamanannya oleh NIST .

Penyelesaian masalah tidak terbatas pada implementasi keamanan dan apa saja kebutuhan aplikasi. Melainkan dibutuhkan suatu *platform* untuk mengimplementasikan aplikasi dan metode pengembangan aplikasi. Menindaklanjuti kebutuhan ini, aplikasi akan dibangun dengan berbasis web dan menerapkan metode WDLC (*Web Development Life Cycle*) untuk pengembangan aplikasi. Pemilihan web didasarkan pada kebutuhan organisasi, anggapan bahwa web saat ini dianggap sebagai *platform* standar untuk melakukan peluncuran berbagai layanan pada web [10]. Selain hal itu, keuntungan dari aplikasi web yakni tersedia secara bebas, dapat diakses melalui perangkat apapun [11] dan dalam penerapannya, karena tidak memerlukan perangkat lunak atau konfigurasi khusus yang perlu dilakukan oleh klien [12]. Selain keuntungan dari web, dasar pemilihan dari web dibandingkan *mobile* dikarenakan terkhusus bidang persuratan dibutuhkan ukuran layar yang cukup besar untuk kemudahan tampilan bagi pengguna, karena jika menggunakan *mobile* tampilan akan cenderung diperkecil yang dapat berisiko merusak tatanan dari surat.

Lebih lanjut, mengenai dasar pemilihan WDLC ialah WDLC merupakan metode pengembangan khusus web yang dikembangkan berdasarkan tahapan dari SDLC(*Software Development Life Cycle*). WDLC menyediakan struktur dasar yang juga mencakup berbagai pedoman untuk memenuhi persyaratan dengan produk akhir [13]. Dengan struktur dasar tersebut membuat WDLC memiliki kelebihan yakni dapat diadopsi untuk aplikasi web yang sederhana dan kompleks [14]. Hal ini dibuktikan dengan terimplementasikannya metode ini dalam beberapa penelitian yakni pada penelitian [15] [16].

Berdasarkan uraian latar belakang permasalahan tersebut, pada penelitian ini akan dilakukan rancang bangun aplikasi pengelolaan naskah dinas elektronik berbasis web yang menerapkan AES-128, RSA 2048, dan SHA 512 untuk memenuhi aspek keamanan sesuai dengan aturan SPBE dan TNDE. Selanjutnya, digunakan metode pengembangan aplikasi yakni WDLC dengan kebutuhan aplikasi menurut pedoman TNDE yang disesuaikan dengan kebutuhan organisasi. Dengan serangkaian implementasi tersebut, penulis berharap aplikasi dapat memenuhi kebutuhan dan menjadi solusi atas permasalahan yang ada.

II. LANDASAN TEORI

A. Aplikasi Pengelolaan Naskah Dinas Elektronik

Aplikasi pengelolaan naskah dinas merupakan aplikasi yang dibangun untuk membantu menyelesaikan permasalahan yang disebabkan digunakannya metode konvensional dalam pengelolaan surat. Solusi ini didapatkan berdasarkan hasil telaah kepustakaan dari beberapa hasil penelitian yakni Guntari dan Setiawan [6] dan Vironica dan Sukadi [1]. Menindaklanjuti dari solusi yang akan diterapkan, dibutuhkan spesifikasi aplikasi pengelolaan naskah dinas elektronik. Spesifikasi aplikasi akan mengacu pada Lampiran Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 tentang Pedoman Tata Naskah Dinas Elektronik (TNDE) di Lingkungan Instansi Pemerintah.

Kebutuhan non fungsional aplikasi dalam Pedoman TNDE memuat beberapa hal yakni keamanan aplikasi, pencatatan *log* aktivitas pengguna, dan fitur penghapusan dan pembatalan. Kebutuhan non fungsional tersebut diimplementasikan secara keseluruhan dalam penelitian. Berkaitan dengan keamanan aplikasi dalam Pedoman TNDE, lingkup keamanan yang disebutkan hanya sebatas pembatasan akses pengguna. Sedangkan keabsahan naskah dinas yang dibuat di dalam aplikasi TNDE perlu disesuaikan dengan peraturan yang berlaku [4]. Berangkat dari kalimat sebelumnya dibutuhkan aturan lanjutan untuk mengatur terkait keamanan dan keabsahan dokumen yang dibuat pada aplikasi yang dalam penelitian ini dokumen yang dibuat pada aplikasi ialah dokumen disposisi. Peraturan Presiden Nomor 95 Tahun 2018 Mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE) akan digunakan sebagai aturan lanjutan untuk memenuhi keamanan dan keabsahan dokumen disposisi pada aplikasi dengan menerapkan prinsip

keamanan SPBE dengan mempertimbangkan prinsip SPBE yang lain pada pasal 2 ayat 1.

B. Algoritme AES-128

NIST (*National Institute of Standards and Technology*) menyatakan algoritme AES merupakan algoritme kriptografi yang terbukti aman yang dapat digunakan untuk melindungi data elektronik [17]. Algoritme AES memiliki tiga macam panjang kunci yakni 128, 192, dan 256 bits [18]. Dengan ketiga ukuran kunci tersebut dinyatakan cukup aman untuk diimplementasikan pada aplikasi pemerintahan dan memadai hingga melampaui tahun 2031 [19]. Berdasarkan penelitian dari Cedric [18] dinyatakan bahwa AES 128 memiliki kecepatan enkripsi dan dekripsi yang lebih cepat dibandingkan dengan AES 256.

C. RSA Digital Signature

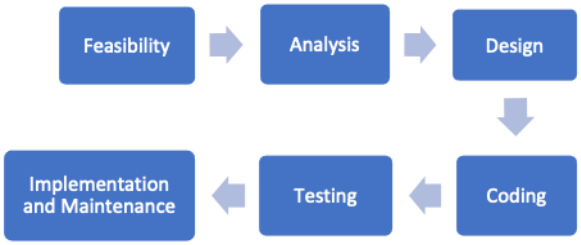
Digital Signature (tanda tangan elektronik) adalah analog elektronik dari tanda tangan tertulis yang dapat digunakan untuk membuktikan kepada penerima atau pihak ketiga bahwa pesan benar-benar ditandatangani oleh pembuatnya (nirsangkal). Terdapat tiga algoritme tanda tangan digital yang direkomendasikan oleh NIST yakni DSA (*Digital Signature Algorithm*), ECDSA (*Elliptic Curve Digital Signature Algorithm*), dan RSA. Algoritme RSA merupakan algoritme dengan kecepatan komputasi yang lebih cepat dari ketiga algoritme tanda tangan elektronik yang direkomendasikan NIST [20]. Hal ini dibuktikan juga dalam beberapa penelitian yakni pada penelitian Ali [21]. Penelitian tersebut juga menyatakan bahwa proses verifikasi dan penandatanganan yang lebih cepat dari ECDSA.

D. SHA-512

Fungsi *hash* merupakan sebuah fungsi yang mengambil jumlah *input* yang berubah-ubah dengan menghasilkan output dengan ukuran tetap [22]. SHA-512 merupakan salah satu jenis algoritme fungsi *hash* yang dinyatakan aman oleh NIST [23]. Karena dinyatakan aman oleh NIST, SHA-512 dapat diimplementasikan sebagai algoritme fungsi *hash* yang digunakan untuk pengamanan *password* yang disimpan pada basis data.

E. Web Development Life Cycle (WDLC)

Web Development Life Cyle (WDLC) merupakan metode pengembangan aplikasi berbasis web yang dibuat berdasarkan adopsi dari SDLC (*Software Development Life Cycle*) [13]. WDLC mendukung pembuatan aplikasi web baik yang sederhana maupun yang rumit, serta dapat disesuaikan dengan metode SDLC yang lain seperti *prototyping* untuk dikembangkan kembali [14]. WDLC memiliki alur proses seperti pada Gambar 1:



Gambar 1. Alur proses WDLC

Berdasarkan gambar di atas WDLC memiliki serangkaian tahapan sebagai berikut:

a) Feasibillity

Merupakan fase pertama dari WDLC adalah perancangan. *Feasibility* sangat penting untuk membangun seluruh situs web. Maka dari itu diperlukan tahapan ini untuk mencapai beberapa hal, yakni tujuan pembuatan situs web, profil pengguna , teknologi web yang akan digunakan, pembagian tugas dan wewenang yang jelas antara pemilik web dan pengembang web, dan konten yang akan ditampilkan pada web.

b) Analysis

Aktivitas ini berisi kegiatan untuk mengumpulkan informasi dari pengguna, dan melakukan analisis terhadap informasi tersebut secara sistematis pada bentuk fungsionalitas dari sistem aplikasi, kebutuhan *input* data dan sumber, *output* data dan kebutuhan tampilan.

c) Design

Pada fase ini akan dilakukan persiapan mengenai rincian desain situs web. Termasuk di dalamnya mengenai pemodelan aplikasi. Desain sistem ini akan di dokumentasi, yang di dalamnya berisi mengenai pemrograman dan pengujian berdasarkan dokumen desain. Tata letak dari situs web merupakan salah satu hal yang penting pada fase ini.

d) Coding

Pada tahapan ini dilakukan pembuatan dan implementasi pemrograman web yang sesuai dengan kebutuhan dan desain yang sudah ditentukan pada tahap *feasibility* dan *analysis.*

e) Testing

Pada fase ini akan dilakukan pengujian sehingga dapat mengetahui dan membandingkan mengenai fungsionalitas dari situs web dengan yang diharapkan saat perancangan. Pada WDLC terdapat beberapa hal yang harus dilakukan uji, yaitu pada halaman web, konten, fungsionalitas, kegunaan, dan kebenaran web.

f) Implementation and Maintenance

Fase ini dilakukan publikasi situs web pada sistem *hosting* untuk melakukan persiapan mengenai peladen dan basis data. Pada fase ini terdapat pemeliharaan pada situs web untuk selalu berisi mengenai informasi terkini.

F. User Acceptance Testing (UAT)

User Acceptance testing (UAT) merupakan jenis pengujian perangkat lunak di mana aplikasi diuji penerimaannya apakah diterima pengguna atau tidak. Maksud dari diterima dalam hal ini adalah sistem sudah sesuai atau memenuhi kebutuhan pengguna [24]. UAT merupakan *acceptance testing* yang menegaskan secara formal apakah sistem memenuhi kebutuhan perusahaan atau tidak [25]. Pemilihan UAT dan panduan pelaksanaan pengujian didasarkan pada penelitian sebelumnya oleh Kesuma [26] dan Arumsari [27] yang menggunakan UAT untuk menjawab perumusan masalah.

III. METODOLOGI

Metodologi yang digunakan dalam membangun aplikasi pengelolaan naskah dinas elektronik adalah WDLC dengan tahapan yang dilakukan yakni *feasibility*, *analysis*, *design*, *coding*, dan *testing*.

A. Feasibility

Pada tahapan ini dilakukan beberapa kegiatan sebagai yakni wawancara dan tinjauan kepustakaan. Wawancara dilakukan terhadap narasumber terkait kondisi persuratan secara mendetail untuk mengetahui kebutuhan dasar dari aplikasi. Penyusunan pertanyaan berdasarkan *output* yang ingin dicapai pada tahapan ini yakni terkait tujuan aplikasi, karakteristik dari pengguna, dan konten aplikasi yang akan ditampilkan. Tinjauan Kepustakaan dilakukan dengan cara mengumpulkan referensi dan mempelajari teori mengenai konsep dasar dari alur persuratan, algoritme AES 128, RSA 2048, WDLC, pemrograman web, Yii2, metode *testing*, dan aturan yang berkaitan dengan penelitian.

B. Analysis

Terdapat dua proses untuk memenuhi kebutuhan aplikasi pengelolaan naskah dinas elektronik di antaranya identifikasi dan penyelesaian kebutuhan fungsional dan non fungsional. Identifikasi dilakukan dengan melakukan wawancara kepada pihak Subbagian Tata Usaha STSN untuk mendapatkan *user requirement* yang akan digunakan sebagai dasar melakukan identifikasi kebutuhan fungsional. Hasil *user requirement* kemudian dilakukan analisis dengan disesuaikan terhadap Pedoman TNDE sebagai acuan, sehingga *output* akhir dari tahapan analisis bisa tercapai kebutuhan fungsional, kebutuhan non fungsional, hasil identifikasi pengguna aplikasi.

C. Design

Tahap ini adalah tahapan dilakukannya pemodelan aplikasi menggunakan diagram yang merepresentasikan desain aplikasi yang akan dikembangkan. Pemodelan ini berupa *data model* dan *process model*. Data model menggunakan ERD (*Entity Relationship Diagram*) dan *process model* menggunakan *use case diagram* untuk menjelaskan bagaimana fitur pada aplikasi . Pembuatan diagram aplikasi menggunakan alat pembuat diagram secara daring melalui situs www.draw.io.

D. Coding

Pada tahapan ini dilakukan pembangunan aplikasi sesuai dengan kebutuhan yang sudah ditentukan pada tahap *feasibility*. Proses *Coding* menggunakan bahasa pemrograman PHP dengan menggunakan *framework* Yii2. Implementasi algoritme AES 128, SHA 512, dan RSA 2048 pada sistem dilakukan juga pada tahapan ini sebagai layanan keamanan terhadap dokumen yang dibentuk di dalam aplikasi.

E. Testing

Tahapan testing dilakukan dengan melakukan serangkaian pengujian yakni pengujian penerimaan aplikasi berupa pengujian aplikasi dan *user acceptance testing*. Pengujian aplikasi menggunakan metode yang dikemukakan oleh Kundu [28] dan UAT dilakukan dengan melakukan penyebaran kuesioner kepada responden pengguna aplikasi.

IV. HASIL DAN PEMBAHASAN

A. Identifikasi Pengguna

Identifikasi pengguna ialah penentuan hak akses yang akan diberikan kepada pengguna dalam proses bisnis yang berjalan. Berdasarkan alur proses bisnis surat masuk dan keluar serta hasil wawancara disimpulkan bahwa aktor yang berperan adalah administrasi umum selaku dan pejabat yang memberikan disposisi.

B. Kebutuhan Fungsional dan Non Fungsional

Aplikasi pengelolaan naskah dinas elektronik dibangun dengan pedoman TNDE dan SPBE yang disesuaikan dan dibatasi dengan kebutuhan organisasi. Berikut adalah kebutuhan fungsional dan non fungsional aplikasi pengelolaan naskah dinas elektronik:

a) Kebutuhan Fungsional

1. Manajemen Pengguna
   - Aplikasi dapat menyediakan fungsi penambahan pengguna
   - Aplikasi dapat menyediakan fungsi edit data pengguna

- Aplikasi dapat menyediakan fungsi pembatasan hak akses pada pengguna

2. Agenda Surat Masuk
   - Aplikasi dapat menyediakan fungsi penambahan surat masuk
   - Aplikasi dapat menyediakan fungsi penambahan disposisi
   - Aplikasi dapat menyediakan fungsi edit surat masuk
3. Manajemen Template
   - Aplikasi dapat menyediakan fungsi manajemen pejabat
   - Aplikasi dapat menyediakan fungsi manajemen tingkat keamanan surat
   - Aplikasi dapat menyediakan fungsi manajemen tingkat kecepatan surat

b) Kebutuhan Non Fungsional

1. Keamanan Aplikasi
   - Aplikasi memiliki fitur untuk mengotentikasi pengguna saat memasuki sistem
   - Aplikasi memiliki fitur tanda tangan digital pada dokumen disposisi
   - Aplikasi memiliki fitur enkripsi disposisi
   - Aplikasi memiliki fitur dekripsi disposisi
2. Pencatatan Log Aktivitas Pengguna
   - Aplikasi menyediakan fitur agenda surat
3. Fitur Penghapusan dan Pembatalan
   - Aplikasi menyediakan fungsi penghapusan akun pengguna
   - Aplikasi menyediakan fungsi penghapusan surat masuk
   - Aplikasi menyediakan fungsi penghapusan disposisi

C. Lingkungan Implementasi

Berikut ini adalah spesifikasi teknologi yang digunakan dalam pengembangan aplikasi pengelolaan naskah dinas elektronik:

a) Spesifikasi Perangkat Keras

1. *Processor* : Intel Core i3-2310M
2. RAM : 8 GB
3. *Hard disk* : 500 GB

b) Spesifikasi Perangkat Lunak

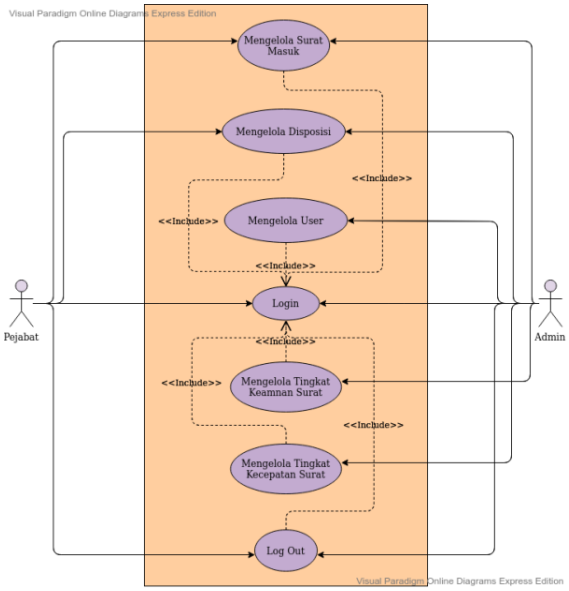
1. PHP *Framework* : Yii2
2. *Code Editor* : Sublime Text 3
3. *Server* : WAMPP

D. Desain Aplikasi

Desain aplikasi pengelolaan naskah dinas elektronik memuat gambaran dari *data model* dan *process model*. Gambaran data ini akan digunakan sebagai landasan pengembangan aplikasi pengelolaan naskah dinas elektronik menggunakan ERD. *Process model* digunakan untuk memberikan gambaran terkait proses apa saja yang terjadi di dalam aplikasi. *Use case diagram* digunakan pada penelitian ini untuk memberi gambaran fitur pada aplikasi dan pembagian hak akses. Gambar 2 menunjukkan *use case diagram* aplikasi pengelolaan naskah dinas elektronik.

E. Hasil Implementasi

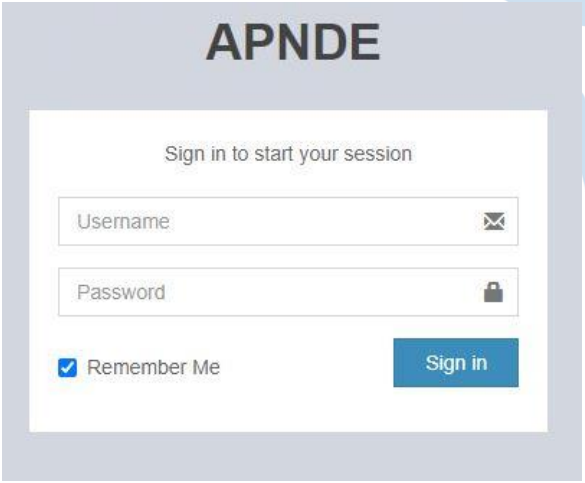
Hasil implementasi dari aplikasi pengelolaan naskah dinas elektronik memiliki dua jenis hak akses berdasarkan hasil identifikasi pengguna yakni pejabat dan administrasi umum. Berdasarkan dari 2 macam hak akses yakni admin dan pejabat, aplikasi pengelolaan naskah dinas elektronik memiliki 3 tiga bagian tampilan, yakni tampilan fitur yang dapat diakses oleh pejabat dan admin, tampilan fitur yang hanya dapat diakses oleh pejabat, dan tampilan fitur yang hanya dapat diakses oleh pengelola atau *admin.* Ketiga fitur utama aplikasi ini ditambahkan dengan satu fitur tambahan utama yakni enkripsi AES. Berikut adalah tiga tampilan fitur aplikasi pengelolaan naskah dinas elektronik:



Gambar 2. *Use Case* diagram aplikasi pengelolaan naskah dinas elektronik

a) Fitur Aplikasi Untuk Aktor Pejabat dan Admin

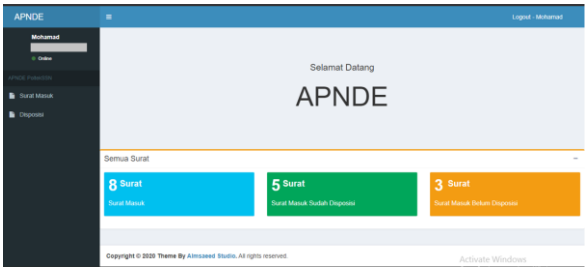
Fitur yang dapat diakses baik pengguna dan admin dalam aplikasi ini adalah fitur *login* dan *logout*. Fitur *login* digunakan untuk melakukan akses aplikasi dan fitur *log out* digunakan untuk mengakhiri sesi dalam aplikasi. Gambar 3 merupakan tampilan halaman *login* pada aplikasi:



Gambar 3. Halaman *login*

b) Fitur Aplikasi Aktor Pejabat

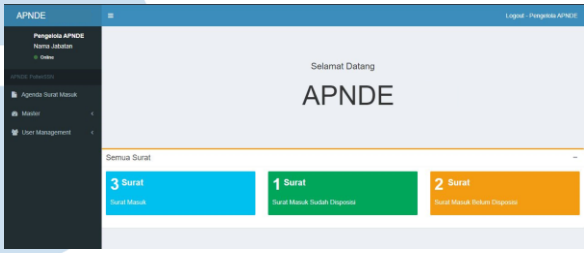
Pejabat dalam lingkup aplikasi mendapatkan akses untuk mengetahui surat yang ditujukan kepada pejabat yang bersangkutan dan memberikan disposisi atas surat yang ditujukan ke pejabat. Berkaitan dengan memberikan disposisi, pejabat dapat melakukan edit, hapus, tanda tangan, dan *download* dari disposisi yang dibuat. Gambar 4 menunjukkan tampilan aplikasi yang diperoleh aktor pejabat:



Gambar 4. Halaman aplikasi aktor pejabat

c) Fitur Aplikasi Aktor Admin

Admin memiliki akses untuk melakukan pengelolaan surat, pengguna, tingkat kecepatan surat, tingkat keamanan, dan melakukan monitor terhadap surat apakah sudah diberi disposisi atau belum oleh pejabat yang bersangkutan. Berikut adalah tampilan aplikasi untuk aktor admin :



Gambar 5. Halaman aplikasi aktor admin

d.) Fitur Enkripsi AES

Enkripsi AES diterapkan pada setiap *file* naskah dinas guna menjaga kerahasiaan dan integritas naskah. Fitur enkripsi ini diimplementasikan dengan menggunakan *library secure encryption*, pada bahasa pemrograman PHP. Enkripsi ini dilakukan setiap ada file naskah dinas yang dikirim keluar, sedangkan kunci disimpan pada basis data.

F. Hasil Pengujian Aplikasi

Hasil pengujian aplikasi pada penelitian ini merupakan hasil pengujian aplikasi menggunakan metode yang dikemukakan oleh Kundu dan hasil UAT. Pengujian aplikasi merupakan hasil pengujian terhadap *functionality*, *usability*, *compability*, *performance*, dan *security* terhadap aplikasi sesuai dengan *test case* yang dikemukakan oleh Kundu. Berikut adalah tabel rangkuman hasil pengujian yang dilakukan:

Tabel 1. Hasil pengujian aplikasi

Jenis Pengujian	Status
Functionality Testing	*Pass*
Usability Testing	*Pass*
Compability Testing	*Pass*
Performance Testing	*Pass*
Security Testing	*Pass*

Berdasarkan dari beberapa hasil pengujian pada tabel diatas berikut adalah penjelasan secara rinci dari masing-masing pengujian yang dilakukan:

a) Functionality Testing

Hasil pengujian *functionality testing* diperolah berdasarkan hasil pengujian terhadap *button*, *link*, dan *form* pada aplikasi, dengan jumlah masing-masing untuk *button*, *link*, dan *form* ialah 25 halaman, 155 *button* dan *link*, dengan metode pengujian yakni memastikan *button*, *link*, dan *form* bekerja dengan baik serta mampu menangani jika terjadi kesalahan *input*. Berdasarkan hasil tersebut diperoleh bahwa aplikasi dapat berjalan sesuai dengan harapan dan dapat menangani *eror* yang terjadi.

b) Usability Testing

Usability testing dilakukan dengan melakukan *navigation testing*. *Navigation testing* mencakup *button* dan *link testing*, sehingga pengujian *link* dan *button* juga disebut dengan *navigation testing*. Hal ini menyebabkan hasil pengujian ini mengacu pada hasil pengujian sebelumnya yakni *functional testing* yang mengacu pada hasil *button* dan *link test* yang sudah dilakukan sebelumnya. Sehingga berdasarkan hasil tersebut *navigation* pada aplikasi pengelolaan naskah dinas elektronik sudah berjalan dengan baik.

c) Compability Testing

Pelaksanaan *compatibility testing* pada aplikasi ini terbatas hanya pada kompatibilitas browser pada satu sistem operasi menggunakan situs www. lambdatest.com dengan cara memasukkan URL aplikasi, kemudian melakukan pemilihan versi *browser* di mana aplikasi akan dilakukan pengujian dan memastikan aplikasi dapat berjalan dengan tampilan yang sesuai. Hasil dari pengujian ini didapatkan bahwa aplikasi kompatibel dengan beberapa *browser* yakni *mozilla firefox*, *chrome*, opera, dan *edge.*

d) Performance Testing

Pengujian ini dilakukan untuk menguji performa aplikasi menggunakan *tools* GTMetrix. Hasil dari pengujian didapatkan. Hasil dari pengujian ini diperoleh *speed* score yakni 81%, Yslow *score* 77%, *fully loaded time* 3,3 s, *total page size* 176 KB, dan terdapat 14 *request*. Hasil tersebut sudah melampaui batas yang ditentukan oleh GT metrix, di mana batas *page speed score* adalah lebih dari 74 %, Yslow juga minimal 74 %, *full loaded time* yang harus kurang dari 7.9 detik, *total page size* yang kurang dari 3.12 MB, dan jumlah *request* yang kurang dari 88. Berdasarkan hal tersebut performa dari aplikasi pengelolaan naskah dinas elektronik dinilai sudah baik karena telah memenuhi batas standar yang ditentukan oleh GTMetrix.

e) Security Testing

Security testing dilakukan bertujuan untuk mengetahui keamanan dari aplikasi pengelolaan naskah dinas elektronik. Terdapat beberapa pengujian keamanan yang dilaksanakan berdasarkan *test case* dari Kundu. Berikut adalah penjelasan hasil pelaksanaan *security testing* yang dilakukan berdasarkan *test case* yang dikemukakan oleh Kundu:

1. Melakukan akses URL halaman internal aplikasi secara langsung pada *browser* tanpa melakukan *login*. Hal tersebut berakibat aplikasi melakukan *redirect* ke halaman utama aplikasi yakni halaman *login* yang menandakan aplikasi telah telah mencegah *user* melakukan akses ke halaman aplikasi tanpa melakukan *login* terlebih dahulu
2. Memasukkan URL lain yang memiliki hak akses berbeda ketika mengakses suatu halaman pada aplikasi. Hal tersebut berdampak pada munculnya notifikasi larangan perintah. Dari hasil tersebut disimpulkan bahwa sistem mencegah *user* untuk melakukan akses terhadap halaman yang bukan diperuntukkan untuk *user* tersebut.
3. Mencoba memasukkan *invalid input* ke semua input *field* aplikasi. Pengujian dilakukan bersamaan dengan *functionality testing* ketika melaksanakan pengujian terhadap *form* pada aplikasi. Hasil pengujian ini yakni aplikasi sudah melakukan *error handling* terhadap *input* yang tidak baik dengan menampilkan notifikasi yang berkaitan dengan kesalahan *input* atau perlunya dilakukan *input* terhadap suatu *field*.
4. Melakukan akses direktori web secara langsung untuk melakukan akses atau pengunduhan konten pada direktori tanpa melakukan *login* atau akses ke dalam halaman aplikasi. Hasil pengujian menunjukkan bahwa muncul notifikasi bahwa perintah yang dilakukan merupakan perintah yang dilarang dilakukan dan disimpulkan direktori aplikasi

tidak dapat di akses secara langsung dan pengujian dinyatakan berhasil.

5. Memastikan penggunaan SSL dengan cara memasukkan URL aplikasi menggunakan HTTP yang seharusnya aplikasi akan langsung melakukan redirect URL menjadi HTTPS. Hasil dari pengujian dinyatakan bahwa aplikasi dapat melakukan directing ke HTTPS ketika melakukan akses aplikasi menggunakan HTTP. Selain hal tersebut, ketika ditinjau pada *address bar* terdapat notifikasi bahwa sertifikat SSL sudah diimplementasikan.
6. Memastikan semua transaksi, *error message*, *security breach attemps* harus tercatat pada *log* di *web server*. Hasil dari pengecekan yang dilakukan adalah terdapat catatan aktivitas aplikasi yang menandakan bahwa seluruh aktivitas yang dilakukan di dalam aplikasi tercatat pada *web server*.

Kesimpulan dari pengujian keamanan yang dilakukan adalah aplikasi pengelolaan naskah dinas elektronik dinilai aman karena memenuhi seluruh *test case* yang dikemukakan oleh Kundu.

Pengujian selanjutnya yakni mengenai penerimaan aplikasi dan kesesuaian aplikasi terhadap kebutuhan pengguna berdasarkan UAT dinyatakan sesuai karena persentase penilaian UAT yakni 95% berdasarkan perhitungan data kuesioner. Hasil ini diperoleh berdasarkan hasil kuesioner yang diberikan pada 5 orang responden yang merupakan perwakilan dari aktor pengguna aplikasi yakni pejabat dan admin dengan jumlah pertanyaan yakni 24 pertanyaan yang guna memastikan kesesuaian aplikasi baik secara fungsional maupun tampilan.

V. SIMPULAN

Berdasarkan hasil pengujian yang dilakukan dalam penelitian ini maka diperoleh kesimpulan sebagai berikut:

1. Aplikasi pengelolaan naskah dinas elektronik. dibangun berdasarkan kebutuhan Organisasi dengan 17 *user requirement* yang diperoleh dari Pedoman TNDE yang disesuaikan dengan kebutuhan organisasi, dengan hasil UAT yang menyatakan bahwa aplikasi telah sesuai dengan kebutuhan organisasi.
2. Aplikasi pengelolaan naskah dinas elektronik dapat memenuhi solusi keamanan terkait pengelolaan naskah dinas elektronik = dengan menjamin kerahasiaan, autentikasi, integritas, dan nir-penyangkalan yang berupa:
   a. Penerapan algoritme AES 128 dalam enkripsi data disposisi dan implementasi HTTPS pada transaksi data yang memenuhi aspek kerahasiaan.
   b. Pembatasan akses ke dalam aplikasi pengelolaan naskah dinas elektronik yang mendukung autentikasi.
   c. Implementasi SHA-512 dan RSA 2048 pada proses penandatanganan dokumen disposisi yang memenuhi aspek integritas dan nir-sangkal.
3. Aplikasi pengelolaan naskah dinas elektronik yang dibangun sudah memenuhi *test case* pengujian keamanan web dari Kundu.

Saran untuk pengembangan aplikasi lebih lanjut adalah dengan menerapkan tanda tangan elektronik menggunakan aplikasi berbasis *mobile*. Hal ini dapat membantu mempermudah petugas untuk menanda tangani naskah dinas kapan pun dan di mana pun.

DAFTAR PUSTAKA

[1] A. Vironica and S. Vincent , "Rancang Bangun Aplikasi Pengelolaan Surat Masuk dan Surat Keluar pada Sekolah Menengah Pertama Negeri 2 Nawangan," *Journal Speed - Sentra Penelitian Engineering dan Edukasi – Volume 5 No 4 - 2013 - ijns.org*, vol. 5, no. 4, pp. 44-51, 2013.

[2] Gunawan, N,K. and Hadiprakoso, R,B. " Comparative Study Between the Integration of ITIL and ISO/IEC 27001 with the Integration of COBIT and ISO/IEC 27001, IOP Conference Series: Materials Science and Engineering" 2020.

[3] MENPANRB, "Peraturan Mentri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 80 Tahun 2012 Tentang Pedoman Tata Naskah Dinas Instansi Pemerintah," 2013.

[4] MENPANRB, "Peraturan Mentri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 Tentang Pedoman Umum Tata Naskah Dinas Elektronik di Lingkungan Instansi Pemerintah," 2011.

[5] A. Rosyanto, "Pembuatan Aplikasi Surat Menyurat Elektronik Berbasis Web di Pemerintah Kota Yogyakarta," 2010.

[6] R. Guntari and R. Setiawan, "RANCANG BANGUN APLIKASI PENGELOLAAN SURAT DI DESA TANJUNG KAMUNING," *Jurnal Algoritma Sekolah Tinggi Teknologi Garut*, vol. 13, no. 1, pp. 269-274, 2016 20.

[7] Pemerintah Republik Indonesia, "Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik," 2018.

[8] H. Siregar, E. Junaeti and T. Hayatno, "Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter," in *IOP Conference Series: Materials Science and Engineering*, 2017.

[9] NIST "Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001.

[10] A. W. Marashdih, Z. F. Zaaba, K. Suwais and N. A. Mohd, "Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting," in *The Fifth Information Systems International Conference 2019*, 2019.

[11] V. Garousi, A. Mesbah, A. Betin-Can and S. Mirshokraie, "A systematic mapping study of web application testing," *Information and Software Technology*, pp. 1374-1396, 2013.

[12] J. Conallen, "Modelling Web Application Architecture with UML," *COMMUNICATIONS OF THE ACM*, vol. 42, no. 10,

pp. 63-70, October 1999.

[13] R. Kamatchi, J. Iyer and S. Singh, "Software Engineering:Web Development Life Cycle," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 3, pp. 1-4, March 2013.

[14] A. Sarkar, "Overview of Web Development Life cycle in Software Engineering," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* , pp. 626-631, 2018.

[15] H. Mstofa and I. Rizqa, "Penerapan Library 2.0 Dengan Metode Web Development Life Cycle (Wdlc) Untuk Dokumentasi Naskah Kuno Nusantara".

[16] R. Kaban and F. Robin, "Pengembangan Sistem Informasi Perpustakaan Dengan Framework CSS Bootsrap dan Web Development Life Cycle," *Jurnal Ilmiah Informatika Volume 2 No.1*, pp. 83-89, 2017.

[17] E. B. Barker, C. W. Barker and A. Lee, "NIST Special Publication 800-21 Guideline for Implementing Cryptography in the Federal Government," National Institute of Standards and Technology, 2005.

[18] T. B. I. Guy-Cedric and S. R, "A Comparative Study on AES 128 BIT AND AES 256 BIT," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 6, no. 4, pp. 30-33, August 2018.

[19] S. Technology, "128-Bit Versus 256-Bit AES Encryption : Practical business reasons why 128-bit solutio provide comprehensive security for every needns," 2008.

[20] A. I. Ali, "COMPARISON AND EVALUATION OF DIGITAL SIGNATURE SCHEMES EMPLOYED IN NDN NETWORK," *International Journal of Embedded systems and Applications(IJESA)*, vol. 5, no. 2, pp. 15-29, June 2015.

[21] Z. Xuan, Z. Du and R. Chen, "Comparison Research on Digital Signature Algorithms in Mobile Web Services," 2009.

[22] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, 1997.

[23] FIPS, FIPS PUB 180-3 Secure Hash Standard (SHS), National Institute of Standards and Technology (NIST), 2008.

[24] A. Dennis, B. H. Wixom and R. M. Roth, System Analysis and Design Fifth Edition, 5th ed., John Willey & Sons, Inc, 2012.

[25] R. Goel and D. N. Gupta, "Survey on Acceptance Testing Technique," *International Journal of Software and Web Sciences (IJSWS)*, pp. 20-23, March-May 2014.

[26] R. C. Kesuma, "Rancang Bangun Aplikasi Secure Disposisi Elektronik dengan Menerapkan Algoritma Blowfish, SHA-512, dan RSA Digital Signature pada Dinas Pengamanan dan Persandian TNI Angkatan Udara," 2018.

[27] D. Arumsari, "Rancang Bangun Aplikasi Disposisi-el Dengan Menerapkan Algoritma AES-256 dan RSA-2048 Pada Perumda Pasar Jaya," 2019.

[28] S. Kundu, "Web Testing : Tool,Challenges and Methods," *IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012*, pp. 481-486, 2012.