RANCANG BANGUN SISTEM INFORMASI MANAJEMEN SURAT INTERNAL BERBASIS WEB DENGAN MULTI-FACTOR AUTHENTICATION (MFA) PADA PT. PELABUHAN INDONESIA III (PERSERO)

Rizky Agung Nugroho [1], Muh. Sidqon, S.Si., M.Si [2]
Teknik Informatika, Universitas 17 Agustus 1945 Surabaya
Jl. Semolowaru No.45, Menur Pumpungan, Kec. Sukolilo, Surabaya
[1]rkyagung@gmail.com
[2]mochsidqon@untag-sby.ac.id

Abstract

With the improvement of the digital era, companies are indirectly required to implement Good Corporate Governance (GCG). PT Pelabuhan Indonesia III (Persero) as a state-owned company which is engaged in providing port services has committed since 2011 to implement Good Corporate Governance (GCG) or Good Corporate Governance. In implementing a paper-free environment, PT Pelabuhan Indonesia III (Persero) fully supports government policies, namely reducing paper use and transferring documents to paperless forms. Almost all business processes have implemented this policy, but official messaging services are still using paper. The use of website technology as a medium for management and preparation of official internal letters is a cheap and efficient technology choice because of its relatively easy use and can be accessed on many types of devices. Multi-Factor Authentication is an authentication method. where the system user of a computer is granted access only after successfully presenting two or more evidences for the authentication mechanism. This study focuses on the process of designing and building an internal mail management information system at PT. Pelabuhan Indonesia III (Persero) which is web-based by implementing Multi Factor Authentication (MFA) as the security key for the identity of the signing of the letter.

Keywords*: Good Corporate Governance, MFA, Internal Mail, Digital Signature*

Abstrak

Dengan berkembangngnya era digital, perusahaan secara tidak langsung dituntut untuk menerapkan Good Corporate Governance (GCG). PT Pelabuhan Indonesia III (Persero) sebagai salah satu Perusahaan BUMN (Badan Usaha Milik Negara) yang bergerak dalam bidang penyediaan jasa kepelabuhan telah melakukan komitmen sejak tahun 2011 untuk melakukan Penerapan Good Corporate Governance (GCG) atau Tata Kelola Perusahaan yang baik. Dalam pelaksanaan lingkungan kerja yang terbebas dari kertas, PT Pelabuhan Indonesia III (Persero) mendukung penuh kebijakan pemerintah yaitu pengurangan penggunaan kertas dan peralihan dokumen kedalam bentuk nir kertas. Hampir seluruh proses bisnis sudah menerapkan kebijakan ini, tetapi untuk pelayanan perpesanan resmi masih dilakukan menggunakan kertas. Pemanfaatan teknologi website sebagai media untuk melakukan manajemen dan penyusunan surat internal resmi merpakan pilihan teknologi murah dan efisien karena penggunaannya yang relatif mudah dan dapat diakses di banyak jenis perangkat. Multi-Factor Authentication, atau yang dalam bahasa Indonesia disebut Otentifikasi Multi Faktor adalah metode otentikasi di mana pengguna sistem dari sebuah komputer diberikan akses pada sistem hanya jika berhasil menyajikan dua atau lebih bukti pada mekanisme otentikasi. Penelitian ini befokus pada proses perancangan dan pembangunan sistem informasi pengelolaan surat internal pada PT. Pelabuhan Indonesia III (Persero) yang berbasis web dengan menerapkan Multi Factor Authentication (MFA) sebagai kunci keamanan dari identitas penandatangan surat.

Kata kunci*: Good Corporate Governance, MFA, Surat Internal, Tanda Tangan Digital*

1. PENDAHULUAN

Good Corporate Governance (GCG) atau Tata Kelola Perusahaan yang baik merupakan tuntutan yang harus diterapkan bagi suatu perusahaan pada era digitalisasi. Diterapkannya tata kelola ini sangat penting untuk mengarahkan dan mengelola kegiatan suatu perusahaan. Salah satu aspek yang harus harus dipenuhi oleh perusahaan adalah kejelasan fungsi, struktur, sistem dan pertanggungjawaban organ perusahaan sehingga pengelolaan perusahaan terlaksana secara efektif [1] . PT Pelabuhan Indonesia III (Persero) mendukung penuh kebijakan pemerintah yaitu pengurangan penggunaan kertas dan peralihan dokumen kedalam bentuk nir kertas. Bidang pekerjaan yang sudah menerapkan nir kertas diantaranya adalah pelayanan Kapal, pelayanan Petikemas, pelayanan Non-Petikemas, dan kegiatan layanan kepelabuhanan lainnya, sedangkan untuk pelayanan perpesanan resmi masih dilakukan menggunakan kertas. Sistem perpesanan resmi untuk mengatur surat internal diperlukan sebagai salah satu kiat dalam mengurangi menggunaan kertas.

Dalam hal pemanfaatan media teknologi, penggunaan website memungkinkan pengguna sistem informasi dapat melakukan akses di semua perangkat selama terhubung ke dalam jaringan. Penggunaan aplikasi berbasis web juga dinilai lebih cepat dalam proses pembangunan dibandingkan dengan pembuatan perangkat lunak secara *native* pada perangkat *mobile*. Selain media dalam pemanfaatan teknologi, keamanan juga merupakan pendukung sebuah perangkat lunak dalam memberikan reliabilitas dari suatu sistem informasi. Keamanan juga dijadikan salah satu faktor utama dalam implementasi sebuah sistem informasi. Metode keamanan yang biasa digunakan, *Single-Factor Authentication* saat ini hanya didasarkan pada satu parameter (*properti unimodality*), jika perolehannya dipengaruhi dengan cara apa pun (baik itu gangguan atau gangguan), keakuratan keseluruhan akan menurun, sehingga bukan tugas yang sulit untuk memalsukannya [2]. *Multi Factor Authentication* atau Otentifikasi Multi Faktor adalah salah satu metode keamanan yang memungkinkan pengguna melakukan otentifikasi melalui lebih dari 2 bukti untuk memperoleh akses terhadap sebuah fitur pada sistem informasi. *Multi-Factor Authentication (MFA)* memberikan tingkat keamanan yang lebih tinggi dan memfasilitasi perlindungan berkelanjutan dari perangkat komputasi serta layanan penting lainnya dari akses tidak sah dengan menggunakan lebih dari dua kategori kredensial. Faktor authentikasi yang menyusun MFA harus memenuhi dua atau lebih dari : *something the claimant know, something the claimant has, dan something the claimant is* [3] .

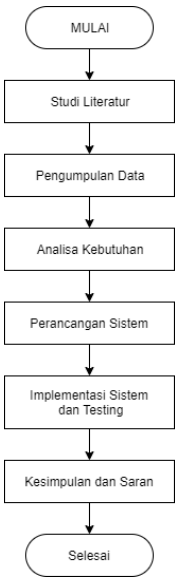
Sejalan dengan wacana Badan Siber dan Sandi Negara (BSSN) pada seminar BsrE Day 2018 dengan tema budaya paperles melalui penerapan digital signature di era *digital office* , demi efisiensi dan efektifitas dalam pemberian layanan, dalam sebuah sistem yang membutuhkan otorisasi diperlukan sebuah tanda tangan digital sebagai pengganti tanda tangan tertulis. Hal ini dapat menjadi percepatan Bangsa Indonesia untuk mencapai *good governance* dengan tetap mengedepankan pengamanan dokumen melalui fitur keamanan sertifikat elektronik yang dapat memberikan jaminan keaslian (*authentication*), keutuhan (*integrity*) dan nir penyangkalan (*non-repudiation*) [4] .

Penelitian akan membahas bagaimana proses perancangan serta pembuatan sistem informasi pengelolaan surat internal online berbasis *web* menggunakan kerangka kerja PHP laravel. Tiap surat yang telah disusun kemudian dilakukan penandatanganan secara digital (*approval*) secara *online* dengan memverifikasi identitas dari penandatangan melalui 4 fakor keamanan,

yaitu *something the claimant know, somehing the claimant has, something the claimant is, dan something the claimant does.* Mempertimbangkan efektifitas , usabilitas dan efisiensi dari tiap faktor keamanan, peneliti akan menggunakan *Personal Identification number* (PIN) sebagai faktor *something the claimant know,* kode *One Time Password* dengan algoritma HMAC yang dikirimkan melalui *email* sebagai faktor *somehing the claimant has,* biometri pengenalan wajah dan membandingkannya dengan dataset yang telah terdaftar sebelumnya sebagai faktor *something the claimant is*, serta *something the claimant does*. Keempat faktor tersebut merupakan faktor yang paling efektif dan efisien untuk diterapkan di lingkungan PT Pelabuhan Indonesia III, dimana setiap pegawai pasti memiliki perangkat pintar (*smartphone*). Surat yang telah selesai ditandatangani dilakukan proses sertifikasi digital menggunakan algoritma RSA agar dapat dibedakan antara dokumen yang telah dimanipulasi dengan dokumen resmi yang diterbitkan oleh sistem.

2. METODE PENELITIAN

Tahapan yang dilakukan pada proses penelitian ini adalah :



Gambar 1 Alur Penelitian

Tabel 1. Spesifikasi peralatan

1. Tahap Studi Literatur
   Studi literatur dilakukan dengan mengumpulkan informasi yang dibutuhkan dari jurnal, buku, dan laporan penelitian. Tahap ini bertujuan untuk memperoleh referensi yang berhubungan dengan topik penelitian.
2. Tahap Pengumpulan Data
   Pengumpulan data dilakukan untuk menunjang penelitian secara keseluruhan, pengamatan terhadap proses penyusunan surat internal yang diterapkan pada PT Pelabuhan Indonesia III (Persero) . Proses ini terdiri dari observasi dan wawancara.
3. Tahap Analisis Kebutuhan
   Pada tahap ini, dilakukan analisa atas kebutuhan baik fungsional maupun non fungsional guna mengetahui kebutuhan pengguna terhadap sistem yang akan dibangun.
4. Perancangan Sistem
   Pada tahap ini, peneliti membuat rancangan dari sistem manajemen surat internal yang akan dibuat berdasarkan analisa kebutuhan yang telah dilakukan sebelumnya. Perancangan tersebut meliputi diagram kasus penggunaan (*use case)*, skenario kasus penggunaan (*use case scenario)*, diagram aktivitas (*activity*)*,* diagram urutan (*sequence*)*,* diagram alur informasi (*information flow*)*,* rancangan basis data, tampilan pengguna.
5. Tahap Implementasi Sistem
   Pada tahap implementasi dan pengujian*,* dipastikan bahwa sistem informasi yang dikembangan bebas dari kesalahan dan sesuai dengan spesifikasi yang telah dirancang, pada hal ini adalah skenario kasus penggunaan (*use case scenario*). Pengujian atau testing juga diperlukan dalam pengimplementasian sebuah rancangan ke dalam sistem sebagai

parameter sistem layak untuk di publikasikan dan digunakan oleh *end user*. Pada penelitian ini, dilakukan skema Pengujian Fungsionalitas Pengujian ini juga disebut dengan *Black Box Testing*.

6. Kesimpulan dan Saran

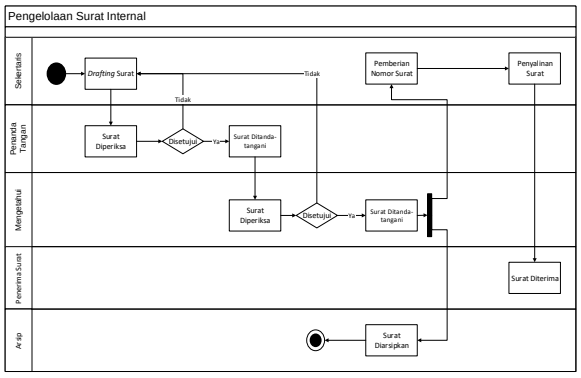
Kesimpulan diperoleh dengan mengacu pada hasil evaluasi, kesimpulan yang diperoleh diharapkan dapat menjawab perumusan masalah yang mejadi landasan dari pengembangan perangkat lunak ini. Sedangkan saran yang diberikan berupa perbaikan peningkatan sistem kedepanya serta saran-saran yang mendukung kesuksesan penggunaan sistem informasi pengolahan surat internal pada PT Pelindo III (Persero).

3. HASIL DAN PEMBAHASAN

Pada penelitian ini, diperoleh hasil terbagi ke dalam perancangan sistem, implementasi sistem, implementasi *multi factor authentication* (MFA) dan pengujian

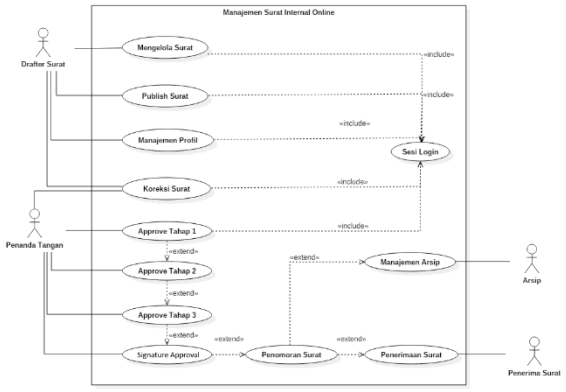
3.1. Perancangan Sistem

Berdasarkan analisa kebutuhan fungsional yang ditentukan, pada butir nomor 2, dapat digambarkan *flowchart* sebagai berikut :



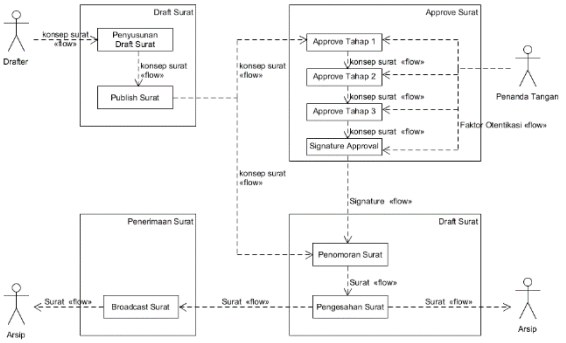
Gambar 2 Flowchart Pelayanan Surat

Berdasarkan hasil analisa kebutuhan dan proses bisnis di atas, dapat dibuat sebuah diagram kasus penggunaan yang akan merepresentasikan sebuah interaksi antara pengguna sistem dengan sistem yang akan dibuat. Gambaran tersebut akan dijelaskan pada diagram dibawah ini:



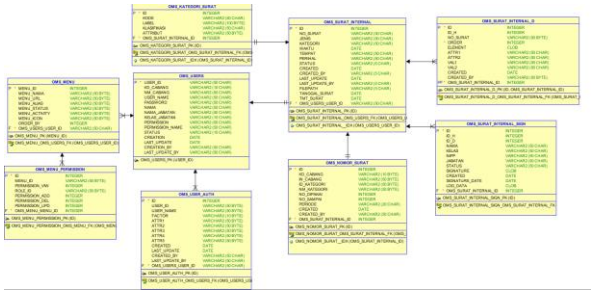
Gambar 3 Diagram *Use Case*

Informasi yang menjadi masukan dan luaran pada tiap tiap use case kemudian disusun menjadi *Information Flow Diagram*



Gambar 4 Information Flow Diagram

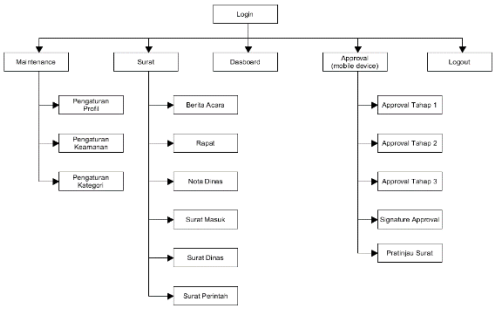
Informasi tersebut kemudian dituangkan ke dalam bentuk entitas data yang tertuang pada ERD



Gambar 5 ERD

Setelah diagram diagram utama yang diperlukan dalam proses analisa kebutuhan

sistem dilakukan, kemudian dilakukan penyusunan dari menu yang direncanakan dari sistem informasi yang akan dibangun. Struktur tersebut tercantum dalam gambar 6

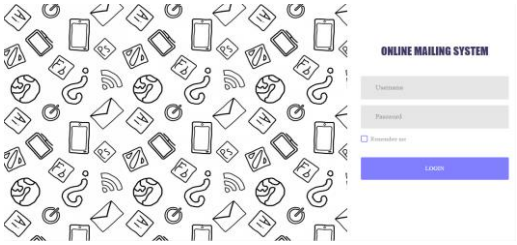


Gambar 6 Struktur Menu

3.2. Implementasi Sistem Informasi

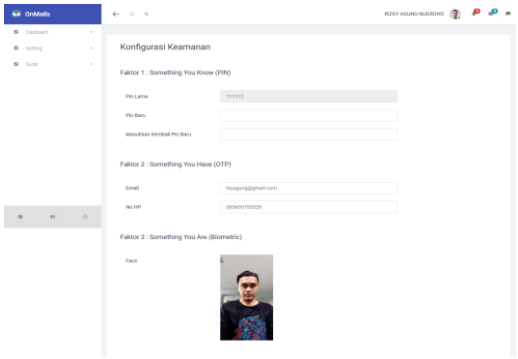
Pada tahap ini,hasil implementasi atas analisa dan rancangan yang telah dibahas pada butir 3.1 sebelumnya yang telah dibentuk menjadi sebuah program Sistem Informasi Manajemen Surat Internal Menggunakan *Multi Factor Authentication* (MFA). Berikut ini akan dijelaskan halaman-halaman hasil dari implementasi.

1. Halaman Login



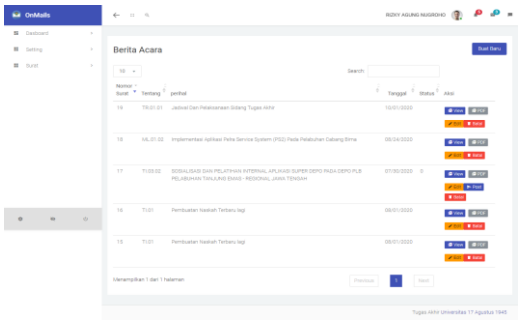
Gambar 7 Halaman Login

2. Halaman Profil & Keamanan



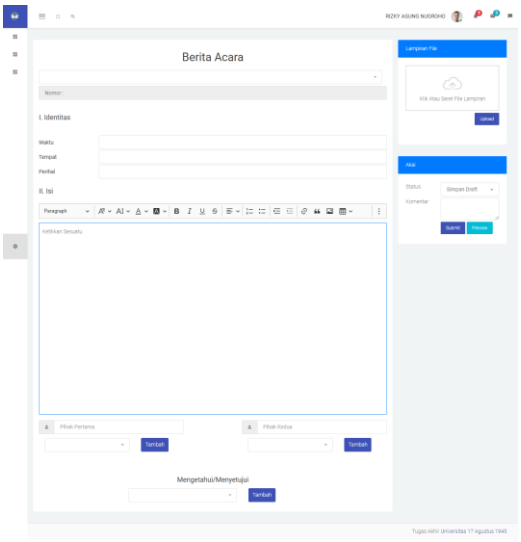
Gambar 8 Halaman Profil

3. Halaman Surat



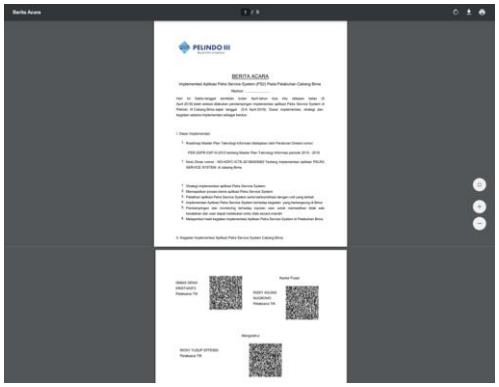
Gambar 9 Halaman Surat

4. Form Surat



Gambar 10 *Form* Surat

5. Cetak Surat



Gambar 11 Cetak Surat

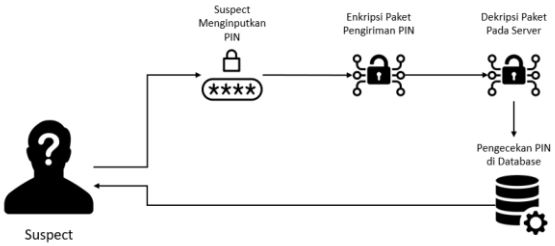
6. Menu *Mobile*

Gambar 12 Halaman *Mobile*

3.3. Implementasi MFA

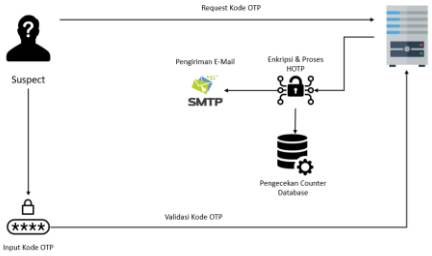
Multi Factior Authentication (MFA) atau authentikasi multi faktor adalah proses klaim suatu identitas dimana dibutuhkan lebih dari 1 faktor keamanan. Suspek pengklaim identitas mencari akses ke sumber daya jaringan atau suatu sistem dari otoritas akses menggunakan kode sandi yang diterima dari otoritas otentikasi. Apabila kode sandi pertama diterima, suspek akan melanjutkan proses otoritas akses dengan faktor kedua dan seterusnya . Tidak ada standar baku berapa jumlah faktor authentikasi yang dapat digunakan dalam memberikan jaminan keamanan suatu identitas. Menurut *Australian Cyber Security Centre* (ACSC), terdapat 3 faktor dalam proses MFA yang dapat digunakan sebagai acuan dalam memberikan faktor keamanan, yaitu *something the claimant knows* (misalnya *Personal Identification Number (PIN), password*) , *something the claimant has* (misalnya token, smartcard, atau *software* sertifikat) dan *something the claimant* is (misal fingerprint, wajah, atau iris). Selain itu, peneliti juga menambahkan faktor *Something The Claimant Does,* untuk memberikan validasi terakhir bagi pengguna sebelum identitas di klaim sebagai tanda tangan digital yang sah. Adapun ke 4 faktor keamanan tersebut di implementasikan dengan teknis :

1. *Something The Claimant Knows*
   Pengguna akan diberikan masukan untuk melakukan *input* pada kolom PIN yang disediakan. Pengguna diwajibkan melakukan input *Personal Identification Number* (PIN) dengan tepat. Kode PIN ini kemudian akan dibuktikan validitas data nya dengan mencocokkan secara simetris data input dengan data yang tersimpan di dalam database. Adapun bagan dari cara kerja *something the claimant knows* pada penelitian ini tercantum pada gambar berikut:



Gambar 13 Proses Verifikasi PIN

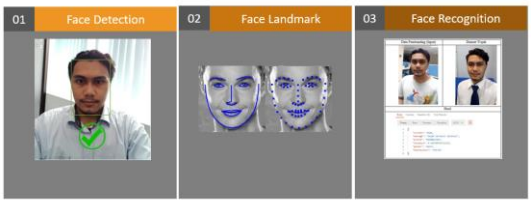
   Pengguna akan melakukan input *Personal Identification Number* (PIN) yang telah diketahui sebelumnya. Reaksi sistem untuk melanjutkan ke tahap 2 akan terpacu apabila input pada tahap ini tidak terdapat kesalahan.
2. *Something The Claimant Has*
   Pada metode *something the claimant has,* Pengguna akan dilibatkan dengan proses validasi menggunakan kunci simetris yang di generate oleh sistem. Kunci ini dikirimkan ke dalam akun *E-Mail* yang telah di daftarkan pada sistem sebelumnya. Prosesnya terdiri dari dua proses utama, yaitu proses generate kunci *One Time Password* (OTP), dan proses validasi kode OTP. Kedua proses ini bergantung pada nomor urut OTP yang akan bertambah tiap user ketika ada permintaan kode OTP. Sehingga kedua kode baik hasil generate dan validate akan identik. Adapun bagan dari cara kerja *something the claimant has* pada penelitian ini tercantum pada gambar berikut:



Gambar 14 Proses Verifikasi OTP

3. *Something The Claimant Is*

Fakor keamanan *Something The Claimant Is* adalah faktor dimana sistem akan memverifikasi biometri dari pengguna. Penelitian ini menggunakan *face-recognition* sebagai biometri yang akan diverifikasi dengan alasan semua device pasti mendukung fitur kamera. Adapun bagan dari cara kerja *something the claimant is* pada penelitian ini tercantum pada gambar berikut:



Gambar 15 Proses Verifikasi Wajah

Tahap awal dalam melakukan verifikasi wajah atau pengenalan wajah, adalah melakukan deteksi wajah dari citra input. Metode SSD (*Single Shot Multibox Detector*) digunakan dalam proses pendeteksian wajah pada fitur keamanan ini. Selanjutnya, sebelum data dari wajah yang sudah dideteksi ini dilakukan pemrosesan pada pendeteksian wajah, sistem akan melakukan pemangkasan pada bagian wajah dan penjajaran sehinga gambar wajah yang telah di pangkas diposisikan pada titik tengah. Selanjutnya, sistem akan mengembalikan 68 titik *landmark* pada wajah dengan metode CNN sederhana. jaringan face recognition services yang berbasis tensorflow dengan arsitektur ResNet-34 akan memproses citra ini untuk memperoleh ekstrasi dari data wajah yang kemudian di terjemahkan ke dalam 128 vektor dari deskriptor wajah.

Untuk melakukan pengenalan wajah (*Face Recognition*), dilakukan perbandingan dua deskriptor wajah. Setelah diperoleh dua deskriptor wajah, kemudian data ini dibandingkan dengan set data deskriptor yang telah di daftarkan sebelumnya dalam bentuk *Euclidean distance*. *Euclidean distance* (jarak Euclidean) disini digunakan untuk menilai apakah wajah yang dibandingkan serupa berdasarkan pada nilai ambang yang telah ditentukan. Untuk menghitung *Euclidean distance* untuk *n-dimensional* vektor adalah sebagai berikut:

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + .. + (p_i - q_i)^2 + .. + (p_n - q_n)^2}$$

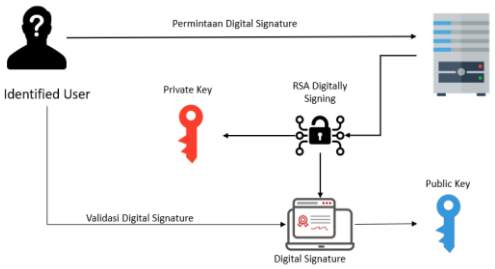
$$d(p,q) = \sqrt{\sum_{i}^{n} (p_i - q_i)^2}$$

Dimana p1 adalah nilai vekor dari deskriptor wajah ke 1 (set data wajah) dan q1 adalah nilai vektor dari deskriptor wajah 2 (masukan wajah yang akan di bandingkan) [5] .

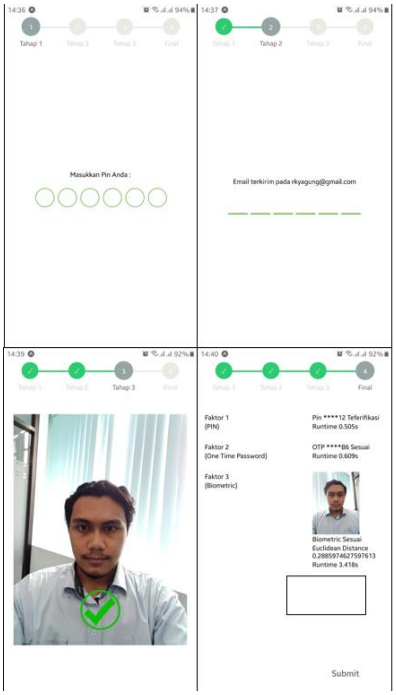
4. *Something The Claimant Does*

Faktor keamanan ini berfokus pada menampilkan 3 faktor sebelumnya yang telah selesai diverifikasi. Pengguna akan melakukan konfirmasi terakhir bahwa ketika telah dlakukan verifikasi pada tahap ini, maka akan terbit *digital signature* yang akan menjadi identitas sah bagi dokumen sebagai pengganti tanda tangan basah. *Digital signature* diproses pada tiap identitas yang menyelesaikan semua faktor keamanan. Proses signature ini dilakukan menggunakan sertifikat yang diperoleh dari *Certificate Authority* (CA). Adapun bagan dari cara kerja something the

claimant is pada penelitian ini tercantum pada gambar berikut:



Gambar 16 Proses *Signature Approval*



Gambar 17 Implementasi MFA

Keseluruhan faktor pada proses keamanan *multi factor authentication* tersebut kemudian di implementasikan pada sistem informasi pengelolaan surat internal ini sesuai dengan yang dijelaskan pada gambar 17.

3.4. Pengujian

Pada tahap pengujian metode yang digunakan penulis untuk melalukan pengujian adalah metode *black box,* pengujian dengan metodi ini berfokus pada fungsionalitas dari sistem yang telah dibangun. Pengujian dilakukan berdasarkan skenario kasus penggunaan dimana dilakukan pencarian kesalahan pada fungsionalitas sistem. Hasil pengujian yang telah dilakukan penulis akan di rangkum sebagai berikut :

Tabel 1 Hasil Pengujian

No	Nama Uji	J	S	G
1	Pengujian Login	4	4	0
2	Pengujian *Draft* Surat	12	12	0
3	Pengujian Manajemen Profil	4	4	0
4	Pengujian Koreksi Surat	12	12	0
5	Pengujian *Approval* Tahap 1	2	2	0
6	Pengujian *Approval* Tahap 2	3	3	0
7	Pengujian *Approval* Tahap 3	3	3	0
8	Pengujian *Signature Approval*	2	2	0
9	Pengujian Penomoran Surat	2	2	0
10	Pengujian Manajemen Arsip	1	1	0

4. SIMPULAN DAN SARAN

Dari uraian pembahasan pada bab-bab sebelumnya akan menghasilkan beberapa kesimpulan sebagi berikut:

1. Telah dilakukan proses perancangan dan pembangunan sistem informasi pengelolaan surat internal berbasis web dengan memanfaatkan fitur keamanan *Multi Factor Authentication* (MFA),
2. Keamanan berlapis pada verifikasi tanda tangan digital dengan memanfaatkan algoritma *Rivest Shamir Adleman* (RSA) pada surat internal yang semula dilakukan secara tradisional guna memberikan keamanan bagi pihak penanda tangan,
3. Dengan diterapkannya sistem ini akan mendukung budaya nir kertas (*paperless*) menggantikan kertas sebagai bukti otentik dokumen, digantikan dengan dokumen digital.

Saran yang diberikan peneliti berdasarkan sistem informasi yang telah dibuat adalah sebagai berikut:

a. Sertifikat yang digunakan dalam proses pembuatan digital signature dapat menggunakan sertifikat yang diperoleh dari *certification authority* BSSN sehingga membuat tanda tangan digital yang tersertifikasi resmi berdasarkan PERMENKOMINFO no 11 Tahun 2018,
b. Sistem dapat dikembangkan lagi menjadi sistem pengelolaan surat internal dan eksternal terintegrasi dengan instansi lain yang akan menggunakan layanan sistem pengelolaan surat yang telah dibuat

DAFTAR PUSTAKA

Jurnal:

[1] J. Emirzon, "*Regulatory Driven* dalam Implementasi Prinsip-Prinsip *Good Corporate Governance* Pada Perusahaan di Indonesia," *J. Manaj. dan Bisnis Sriwij.*, vol. 4, no. 8, pp. 92–114, 2006.

[2] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, 2018, doi: 10.3390/cryptography2010001.

[4] C. Harold F. Tipton and C. Micki Krause, *Informational Security Management Handbook Sixth Edition*, vol. 53, no. 9. 2013.

[5] N. Hazim, S. Sameer, W. Esam, and M. Abdul, "Face Detection and Recognition Using Viola-Jones with PCA-LDA and Square Euclidean Distance," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 371–377, 2016, doi: 10.14569/ijacsa.2016.070550.

Buku Teks:

[3] D. Dasgupta, A. Roy, and A. Nag, *Multi-Factor Authentication More secure approach towards authenticating individuals*. 2017.