BAB III
ANALISIS DAN PERANCANGAN

3.1 Analisis

Sebelum merancang sistem baru, langkah pertama yang harus dilakukan adalah menganalisis sistem yang sudah ada sebelumnya. Tujuan dari analisis ini adalah untuk membandingkan kinerja sistem lama dengan sistem baru yang diusulkan.

3.1.1 Identifikasi Masalah

Identifikasi masalah merupakan langkah awal yang perlu dilakukan untuk menemukan dan memahami berbagai isu atau pokok permasalahan yang muncul dalam suatu konteks atau sistem. Pokok-pokok permasalahan tersebut antara lain:

a. Tingginya mobilitas antar karyawan dan atasan menghambat proses birokrasi penandatanganan yang ada pada perusahaan.
b. Tidak terpusatnya data rekapan dan tidak terkelompoknya dokumen surat menyurat menyebabkan sulitnya dalam mencari dan memilah informasi surat yang telah diterbitkan.
c. Penumpukkan dokumen menyebabkan terlewatnya dokumen surat yang perlu di tanda tangani.

Gambar 3.1 Activity Diagram Proses Tanda tangan dokumen Material Service Requisition

Pada Gambar 3.1 diatas merupakan alur proses penandatanganan dokumen MSR (Material Service Requisition). Dalam proses ini, sales akan membuat dokumen dan juga melakukan penandatanganan awal. Selanjutnya, dokumen akan diajukan kepada masing-masing atasan untuk direview dan ditandatangani. Pada dokumen MSR, diperlukan penandatanganan dari beberapa pihak, termasuk Sales, Sales Manager, Operational Manager, Direktur, dan Suply Chain Management. Hal ini menjadi penghambat proses birokrasi penandatanganan ketika para karyawan dan atasan tidak ada di tempat atau sedang berpergian.

Tabel 3.1 Analisa Sebab Akibat

Permasalahan	Solusi	Manfaat
Mobilitas karyawan dan atasan memperlambat proses birokrasi penandatangananan dokumen surat menyurat	Membuat fitur penandatanganan elektronik	Mempermudah penandatanganan dari berbagai tempat
Sulitnya dalam mencari dan memilah dokumen surat menyurat	Membuat fitur daftar dokumen surat menyurat	Mempermudah pencarian dan pengelompokkan dokumen
Terlewat dan terlupanya permintaan tanda tangan	Membuat fitur reminder berupa notifikasi	Mengingatkan pengguna untuk melakukan penandatanganan

3.1.2 Pemecahan Masalah

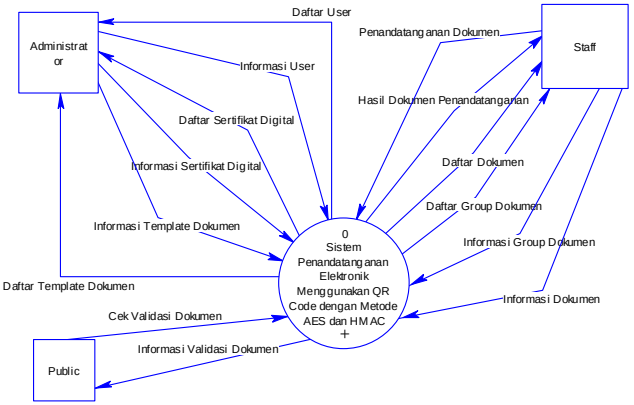
Berdasarkan hasil analisis identifikasi masalah, penulis merancang solusi berupa pengembangan sistem yang dapat mempermudah proses penandatanganan surat menyurat internal. Sistem ini diharapkan mampu memberikan solusi yang efektif guna mengatasi permasalahan yang ada. Data yang akan dikelola dalam sistem informasi ini melibatkan beberapa jenis pengguna, seperti administrator, staff, dan pengguna global/publik.

3.2 Perancangan

3.2.1 Perancangan Sistem

Bagian ini menjelaskan proses dalam perancangan sistem penandatanganan elektronik berbasis web yang dikembangkan untuk PT. Malang Agro Resources. Perancangan sistem ini menggunakan Data Flow Diagram (DFD) sebagai alat untuk memetakan aliran data dan proses yang terjadi dalam sebuah sistem. DFD membantu memvisualisasikan interaksi antara pengguna, sistem, dan entitas eksternal, serta memastikan sistem dapat beroperasi dengan efisien dan efektif. Gambar 3.2 menampilkan Context Diagram dari sistem penandatanganan elektronik berbasis QR Code

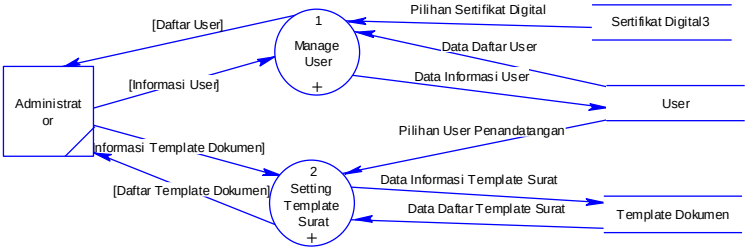
dengan metode AES dan HMAC yang diterapkan di PT. Malang Agro Resources.



Gambar 3.2 Context Diagram Sistem Penandatanganan Elektronik

Selanjutnya merupakan DFD Sistem Penandatanganan Elektronik Menggunakan QR Code dengan Metode AES dan HMAC pada Malang Agro Resources yang diusulkan.

Proses Manage User dan Setting Template Dokumen dijelaskan melalui DFD level 1 pada Gambar 3.3. Pada proses Manage User, administrator memiliki kemampuan untuk menambahkan, mengubah, atau menghapus akun pengguna. Gambar 3.8 menjelaskan detail lebih lanjut mengenai proses ini. Sementara itu, pada proses Setting Template Dokumen, administrator dapat menambahkan, mengedit, atau menghapus konten template surat, termasuk jenis surat dan daftar pengguna yang terlibat dalam proses penandatanganan. Untuk penjelasan lebih rinci, lihat Gambar 3.9.

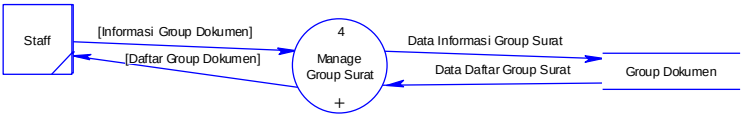


Gambar 3.3 DFD Level 1 Manage User dan Setting Template Dokumen

DFD level 1 untuk proses Manage Certificate oleh admin ditampilkan pada Gambar 3.4. Proses ini memungkinkan admin untuk melakukan penambahan, perubahan, atau penghapusan data sertifikat digital yang nantinya dapat digunakan untuk proses penandatanganan dokumen surat-menyurat. Untuk penjelasan lebih detail, lihat Gambar 3.10.

Gambar 3.4 DFD Level 1 Manage Certificate

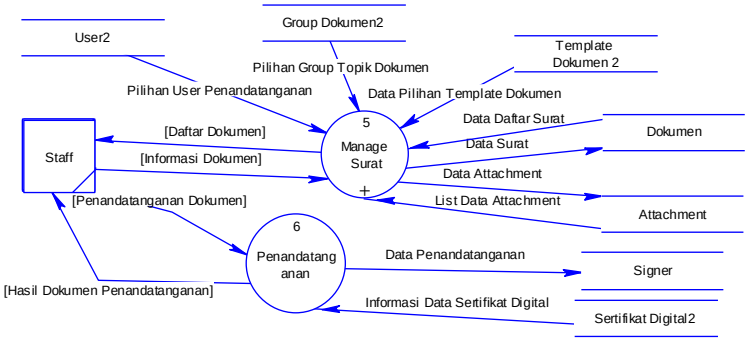
Proses Manage Group Dokumen dijelaskan melalui DFD level 1 pada Gambar 3.5. Proses ini memungkinkan staff untuk menambahkan, mengubah, atau menghapus informasi group dokumen, yang berfungsi sebagai pengelompokan dokumen surat-menyurat untuk perusahaan tertentu. Untuk penjelasan lebih rinci, lihat Gambar 3.11.



Gambar 3.5 DFD Level 1 Manage Group Dokumen

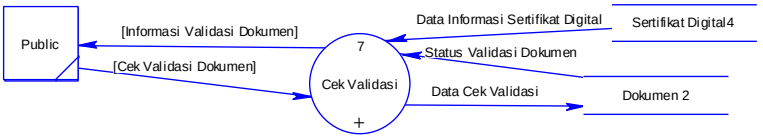
Gambar 3.6 memperlihatkan DFD level 1 Manage Dokumen digunakan untuk membuat permintaan penandatanganan surat dan

mengedit informasi surat. Detail lebih lanjut mengenai proses ini, lihat Gambar 3.12. Sedangkan pada proses Penandatanganan akan menyimpan dan memberi hasil ataupun tanda bahwa telah dilakukan proses tanda tangan.

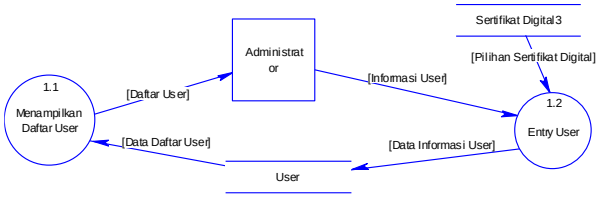


Gambar 3.6 DFD Level 1 Manage Dokumen, dan Penandatanganan

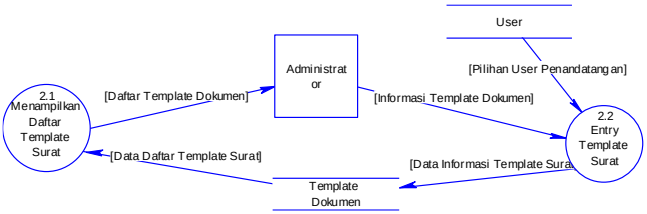
DFD level 1 untuk proses Cek Validasi oleh publik ditampilkan pada Gambar 3.7. Proses ini bertujuan untuk memindai kode QR dan memverifikasi keabsahan tanda tangan yang terdapat pada surat. Untuk penjelasan lebih rinci, lihat Gambar 3.13.



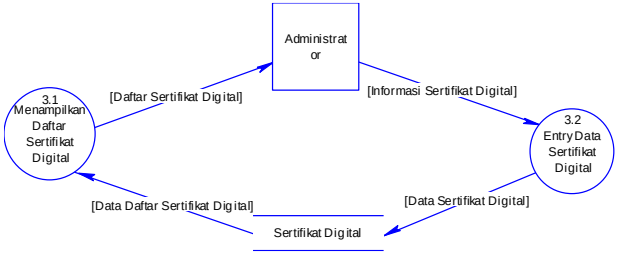
Gambar 3.7 DFD Level 1 Cek Validasi



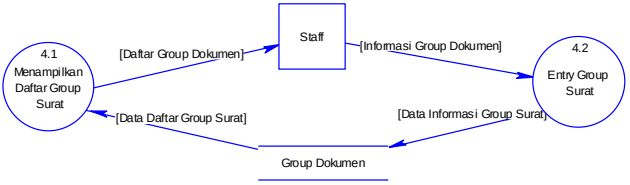
Gambar 3.8 DFD Level 2 Manage User



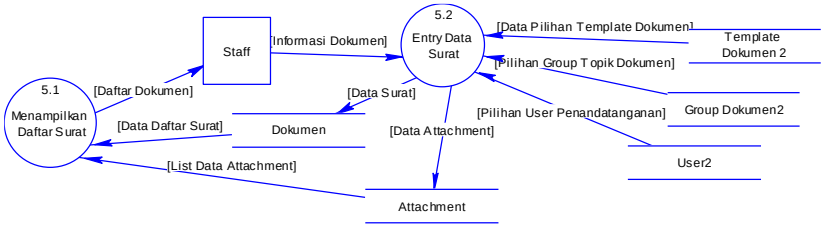
Gambar 3.9 DFD Level 2 Manage User



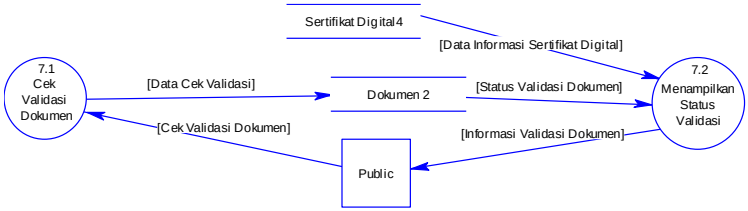
Gambar 3.10 DFD Level 2 Manage Certificate



Gambar 3.11 DFD Level 2 Manage Group Dokumen

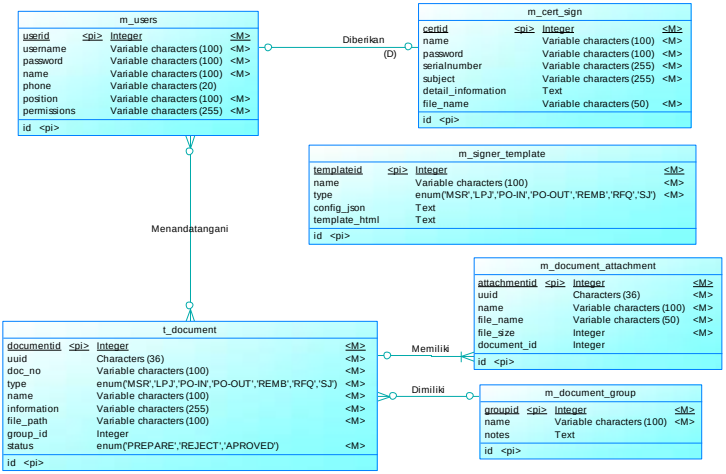


Gambar 3.12 DFD Level 2 Manage Dokumen

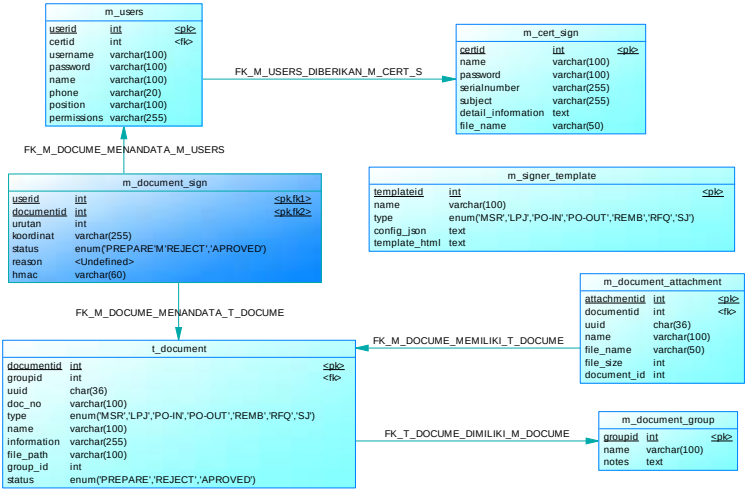


Gambar 3.13 DFD Level 2 Cek Status Validasi

3.2.2 Perancangan Data



Gambar 3.14 Conceptual Data Model (CDM)



Gambar 3.15 Physical Data Model (PDM)

3.2.3 Perancangan User Interface / *Mock-up* aplikasi

Perancangan UI (user interface) merupakan tahap penting dalam pengembangan sistem, karena UI menjadi titik interaksi antara pengguna dan sistem. Pada bagian ini, dirancang mock-up antarmuka pengguna yang menggambarkan alur kerja dan tampilan aplikasi. Rancangan UI ini mencakup halaman-halaman utama yang akan digunakan oleh pengguna, seperti halaman login, manajemen dokumen, penandatanganan dokumen, dan verifikasi dokumen. Perancangan UI dibuat secara konseptual menggunakan tools desain Balsamiq Mockups.

Gambar 3.16 Login User

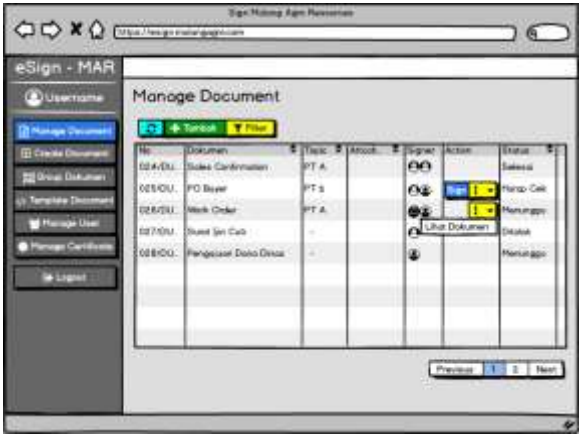
Gambar 3.17 Daftar User serta Modal Data User

Gambar 3.18 Daftar Certificate serta Modal Tambah Certificate

Gambar 3.19 Daftar Template Document serta Data Template

Gambar 3.20 Daftar Group Dokumen serta Modal Data Group Dokumen

Gambar 3.21 Entry Informasi Dokumen Serta Pengaturan Hirarki dan Isi Dokumen

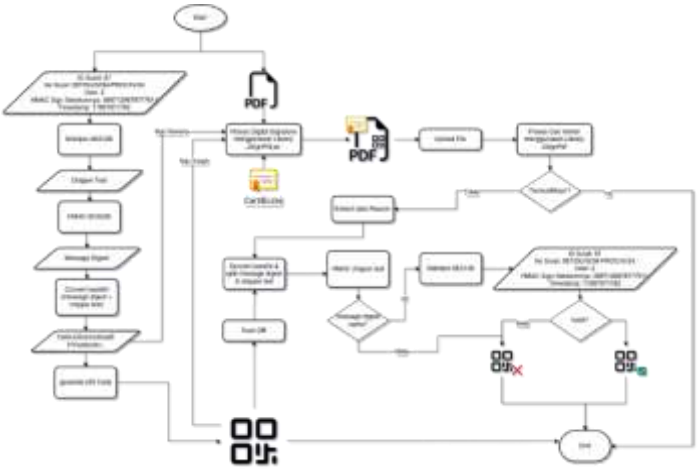


Gambar 3.22 Daftar Dokumen

Gambar 3.23 Penandatanganan Dokumen

Gambar 3.24 Verifikasi Penandatanganan Dokumen

3.2.4 Perancangan Arsitektur



Gambar 3.25 Rancangan Arsitektur Enkripsi dan Dekripsi Informasi Penandatanganan

Pada Gambar 3.25 di atas, merupakan rancangan arsitektur dari proses enkripsi dan dekripsi informasi penandatanganan. Proses ini dimulai dengan pengumpulan informasi penting, seperti ID surat, nomor surat, ID pengguna, timestamp, dan HMAC jika terdapat tanda tangan sebelumnya.

Setelah informasi terkumpul, langkah selanjutnya adalah melakukan proses enkripsi terhadap informasi penandatanganan menggunakan algoritma AES128. Proses ini menghasilkan ciphertext. Pemilihan AES128 didasarkan pada pertimbangan bahwa RSA2048 akan menghasilkan ciphertext yang lebih panjang meskipun berasal dari plaintext yang pendek. Selain itu, RSA2048 beroperasi lebih lambat dibandingkan dengan AES128, sehingga AES128 lebih efisien untuk digunakan dalam konteks ini.

Sebagai langkah pengamanan tambahan, ditambahkan message digest yang dihasilkan dari proses HMAC-SHA256 pada ciphertext. Setelah itu, message digest dan ciphertext akan digabungkan dan diubah menjadi format base64. Data dalam format base64 ini kemudian digunakan untuk pembuatan kode QR sebagai pengganti tanda tangan, serta digunakan sebagai sign reason dalam proses penandatanganan digital menggunakan library JsignPdf, bersamaan dengan sertifikat digital yang disisipkan dalam file dokumen.

Dalam proses verifikasi, kode QR akan dipindai atau file dokumen akan diunggah untuk mengambil informasi yang berisi sign reason pada tanda tangan digital. Khusus pada proses verifikasi yang menggunakan unggahan file dokumen, juga dilakukan pengecekan untuk mengetahui kemungkinan terjadinya modifikasi pada dokumen. Selain itu, proses verifikasi juga melakukan pengecekan terhadap informasi sertifikat digital yang tersimpan dalam sistem untuk memastikan bahwa sertifikat tersebut masih terdaftar atau diakui.

Selanjutnya, informasi yang diperoleh dari kode QR atau sign reason ini berupa teks dalam format base64 yang akan didekode untuk mengembalikan konten berupa message digest dan ciphertext. Ciphertext kemudian akan diproses ulang menggunakan HMAC-SHA256, dan dilakukan pengecekan apakah hasilnya sama dengan message digest yang telah

disertakan dalam format base64. Jika hasilnya sama, proses dilanjutkan dengan melakukan dekripsi menggunakan AES128 untuk mengubah ciphertext kembali menjadi informasi penandatanganan, serta melakukan pengecekan untuk memastikan bahwa informasi yang tertera adalah valid.

Penggunaan lain dari HMAC adalah untuk mengonfirmasi hirarki penandatanganan yang ada terkait dengan penandatanganan sebelumnya. Misalnya, penandatanganan ke-5 terkait dengan penandatanganan ke-4, dan seterusnya hingga penandatanganan ke-1.

Dengan demikian, arsitektur ini tidak hanya menjamin keamanan informasi penandatanganan, tetapi juga memastikan integritas dan keabsahan dari setiap tanda tangan digital yang dihasilkan:

3.3 Rancangan Pengujian

Rancangan pengujian adalah tahap kritis dalam pengembangan sistem guna memastikan bahwa sistem beroperasi sesuai dengan kebutuhan dan spesifikasi yang telah dirancang. Dalam penelitian ini, penggunaan metode Black Box dalam melakukan uji fungsionalitas sistem tanpa melihat struktur internal kode program. Proses pengujiannya dengan menganalisis input yang dimasukkan ke sistem dengan melihat hasil dari output, guna memastikan bahwa sistem memberikan respons yang sesuai dengan harapan.