



Tugas Akhir-2 2022/2023
Institut Teknologi Del
Fakultas Informatika dan Teknik Elektro

Perbaikan Yang Perlu Dilakukan Berdasarkan Sidang Tugas Akhir-2

Berdasarkan hasil masukan/saran dari PANITIA SIDANG TA-2 pada SIDANG yang sudah dilakukan oleh kelompok TASI-2122-202 yang beranggotakan:

No.	Nama Mahasiswa	NIM
1.	Yudika Purba	12S18013

1. Rangkuman perbaikan dari feedback SIDANG TA-2 (KETUA PENGUJI)

Masukan, Usulan, dan Saran Perbaikan Berdasarkan SIDANG	Status Perbaikan (Tuliskan bab/hal yang diubah serta jelaskan perbaikan yang dilakukan)
Memperbaiki format dokumen sesuai dengan masukan pada dokumen hardcopy yang telah diberikan (numbering, tabel gambar, etc	Pada dokumen telah diperbaiki format penulisan yang menggunakan numbering, daftar tabel, daftar isi, tabel gambar. margin, keterangan pada gambar dan memperhatikan typo pada dokumen.
Memperbaiki Use Case Scenario masih salah, tidak ada scenario.	Pada dokumen yang sebelumnya ditulis use case scenario dan use case scenario telah diperbaiki dan sudah terdapat skenario pada setiap tabel. dapat dilihat pada subbab bab 4.4.2
Memperbaiki BPMN, akan lebih baik jika gambar BPMN disatukan pada signing dan verification	Untuk BPMN signing dan verification yang sebelumnya masing masing terpisah telah disatukan menjadi satu BPMN yang ditulis pada subbab 4.4.3.
ERD (Entity Relational Diagram) masih salah	ERD telah diperbaiki dengan penggunaan notasi seperti entitas, atribut, relasi dan dengan garis penghubung pada sub bab 4.4.4
Untuk ERD, CDM, PDM tidak berada pada tahapan yang sama.	Untuk perbaikan ERD, CDM, PDM masih dituliskan pada dokumen dengan subbab berurutan, dimulai dari ERD yang menjelaskan hubungan antara data yang ada, dan dilanjutkan CDM PDM.
Pada bab Analisis, harus menambahkan analisis mengenai, certificates, Hashing, Encrypt dan Decrypt	Pada bab analisis sebelumnya tidak dituliskan analisis terkait certificates, hashing process, encrypt dan decrypt. Telah ditambahkan subbab untuk analisis certificates, hashing process, encrypt dan decrypt.
Memperbaiki Testing	Pada Testing yang telah dilakukan user sudah berjalan dengan baik, dan pengujian setiap unit system telah diperbaiki pada subbab 7.1. Adapun pengujian terdiri dari register, login, signing document, dan verification document
Menambahkan perancangan pada proses Embedding, Hashing, Encrypt, Decrypt.	Perancangan proses embedding certificate, hashing, encrypt dan decrypt sebelumnya tidak dituliskan pada dokumen, dan hanya menuliskan design signing dan verification. Sehingga perancangan untuk embedding, hashing, encrypt dan decrypt telah ditambahkan pada bagian subbab 4.3.



Tugas Akhir-2 2022/2023
Institut Teknologi Del
Fakultas Informatika dan Teknik Elektro

Masukan, Usulan, dan Saran Perbaikan Berdasarkan SIDANG	Status Perbaikan (Tuliskan bab/hal yang diubah serta jelaskan perbaikan yang dilakukan)
Penjelasan serta Tahapan SDLC yang belum tepat	Tahapan SDLC yang digunakan pada pengembangan system adalah waterfall yang merupakan metode pengembangan yang dilakukan tahap per tahap, pada penelitian ini dimulai dengan tahapan analysis, design, implementation, testing, dan maintenance. Pada tahapan dijelaskan bahwa peneliti melakukan diskusi pembangunan system kepada pihak kampus /WR, kemudian merancang design system, dilanjutkan dengan dibangun sebuah system hingga melakukan testing kepada pihak kampus, dan diakhiri dengan maintenance.

2. Rangkuman perbaikan dari feedback SIDANG TA-2 (ANGGOTA PENGUJI)

Masukan, Usulan, dan Saran Perbaikan Berdasarkan SIDANG	Status Perbaikan (Tuliskan bab/hal yang diubah serta jelaskan perbaikan yang dilakukan)
Menyamakan kesimpulan dengan pertanyaan penelitian	Pertanyaan penelitian ditulis pada dokumen adalah mengembangkan system yang efektif untuk signing and verification with digital signature dengan harapan sistem dapat direalisasikan di IT Del dan telah memperbaharui kesimpulan yaitu system signing and verification yang efektif telah berhasil dikembangkan.
Pada latar belakang penggunaan certificate perlu diberikan penjelasan	Penggunaan certificates pada penelitian ini sebelumnya tidak dijelaskan pada bagian latar belakang. Sehingga untuk perbaikan telah ditambahkan penjelasan terkait penggunaan certificate tersebut ke bagian latar belakang dokumen penelitian.
Penjelasan kode program pada file generagenerate.php barisan ke 16 terkait penggunaan MD 5 <code>\$message_digest = md5(\$data);</code>	Penjelasan barisan kode program tersebut adalah, bahwa <code>\$message_digest</code> adalah variable yang menyimpan nilai pesan yang telah dihasilkan setelah menjalankan fungsi md5 pada <code>\$data</code> .
Penjelasan kode program untuk menghasilkan key pair	<code>\$keyPair = openssl_pkey_new(\$conf);</code> Kode program yang berfungsi untuk melakukan generate RSA key pair yaitu private key dan public key menggunakan fungsi <code>openssl_pkey_new()</code> . Keys yang dihasilkan berdasarkan konfigurasi yang telah ditentukan pada barisan kode program sebelumnya.
Penjelasan fungsi kode program bin2hex	Penjelasan <code>\$data</code> adalah variable yang berisi data biner yang dikonversi menjadi heksadesimal. Kode program <code>bin2hex</code> berfungsi untuk mengambil data argument berupa data biner dan mengembalikan representasi heksadesimal dari data dalam bentuk string. Konversi dilakukan byte-wise atau proses byte per byte.



Tugas Akhir-2 2022/2023
Institut Teknologi Del
Fakultas Informatika dan Teknik Elektro

3. Hal-hal yang terkait penulisan dokumen (PEMBIMBING)


Masukan, Usulan, dan Saran Perbaikan Berdasarkan SIDANG	Status Perbaikan (Tuliskan bab/hal yang diubah serta jelaskan perbaikan yang dilakukan)
Pada dokumen abstract masih salah. Perbaiki Abstract	Pada bagian abstract telah diperbaiki dengan menambahkan penggunaan algoritma RSA pada abstract sebelumnya tidak ada.
Format dan Margin untuk daftar isi, daftar gambar, daftar tabel diperhatikan	Pada penulisan dokumen penelitian untuk bagian format penulisannya dan pengaturan margin sudah disesuaikan pada dokumen di bagian daftar isi, daftar gambar, daftar tabel dokumen
Restrukturisasi Bab Analisis. Sesuai masukan dari ketua penguji	Pada bab analisis restrukturisasi telah diubah menjadi sub bab analisis tahapan penelitian, analisis penelitian terdahulu, analisis digital signature, analisis certificates, hashing, encrypt dan decrypt.

Laguboti, 14 Juli 2023


Ketua Sidang,

Mario E. S. Simaremare, S.Kom., M.Sc.
NIDN: 0128058805


Ketua Penguji,


Parmonangan R. Togatorop, S.Kom., M.T.I
NIDN: 0110029201

Anggota Penguji,


Samuel I.G. Situmeang, S.T.I., M.S.
NIDN: 0130058501

Mahasiswa


Yudika Purba
NIM. 12518013