Business Requirements Document (BRD)
Sistem Manajemen File Berbasis Web dengan Enkripsi RSA

1. RINGKASAN EKSEKUTIF

Dokumen ini menguraikan kebutuhan bisnis untuk pengembangan sistem manajemen file berbasis web yang mengintegrasikan algoritma kriptografi RSA (Rivest-Shamir-Adleman). Tujuannya adalah menciptakan solusi keamanan dokumen digital yang robust, efektif, dan dapat diandalkan untuk melindungi kerahasiaan, integritas, dan autentikasi file selama proses penyimpanan dan transmisi melalui jaringan internet.

2. LATAR BELAKANG MASALAH

2.1 Aset Bernilai Tinggi

Data dan dokumen digital mencakup informasi sensitif seperti dokumen keuangan, data pribadi pengguna, dan informasi rahasia perusahaan yang membutuhkan perlindungan ekstra ketat.

2.2 Peningkatan Ancaman Keamanan Siber

Terdapat lonjakan kasus kebocoran data di Indonesia:

- **Mei 2020:** 91 juta data pengguna Tokopedia bocor dan diperjualbelikan di dark web
- **Mei 2020:** Data Daftar Pemilih Tetap (DPT) Pemilu 2014 bocor di forum peretas
- **2021:** 20 juta data pribadi BPJS Kesehatan bocor dalam bentuk file Excel

2.3 Kelemahan Sistem Konvensional

Sistem manajemen file konvensional memiliki kerentanan terhadap:

- Serangan *data breach* dan *unauthorized access*
- Penyadapan data (*eavesdropping*) selama transmisi
- Manipulasi data (*data tampering*)
- Serangan *man-in-the-middle attack*
- Tidak adanya mekanisme enkripsi yang robust pada proses upload/download file

3. TUJUAN PROYEK

Mengimplementasikan sistem keamanan dokumen digital yang mengintegrasikan:

1. **Algoritma RSA 2048-bit** untuk menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan autentikasi (*authentication*) data
2. **Framework Laravel Filament** sebagai platform modern yang mendukung *best practices* dalam *production environment*
3. **Client-side encryption** dan **server-side decryption** untuk melindungi data selama transmisi melalui jaringan internet

4. KEBUTUHAN FUNGSIONAL (FUNCTIONAL REQUIREMENTS)

4.1 Manajemen Enkripsi & Dekripsi File

FR-01: Sistem harus menggunakan algoritma RSA-OAEP dengan SHA-256 untuk mengenkripsi file pada sisi *client* sebelum diunggah ke server.

FR-02: Sistem harus melakukan dekripsi file pada sisi server menggunakan kunci privat yang terenkripsi dengan AES-256-CBC.

FR-03: Sistem harus mendukung enkripsi dan dekripsi file dengan berbagai format (PDF, DOCX, TXT, PNG, JPG, MP4, ZIP) dan ukuran hingga 100 MB.

4.2 Manajemen Kunci (Key Management)

FR-04: Sistem harus membangkitkan pasangan kunci RSA (publik dan privat) berukuran 2048-bit secara otomatis untuk setiap pengguna baru.

FR-05: Sistem harus menyimpan kunci publik dalam *plaintext* untuk keperluan enkripsi, sementara kunci privat harus dienkripsi dengan AES-256-CBC sebelum disimpan di database (*encryption at rest*).

FR-06: Sistem harus menyediakan mekanisme *key rotation* yang dapat dipicu oleh pengguna atau dijadwalkan secara otomatis.

FR-07: Kunci privat tidak boleh pernah dikirimkan ke sisi *client* untuk menjaga keamanan.

4.3 Manajemen Integritas Data

FR-08: Sistem harus menghitung SHA-256 *hash* dari file original sebelum proses enkripsi untuk memastikan integritas data.

FR-09: Sistem harus memverifikasi *hash* setelah dekripsi untuk mendeteksi upaya manipulasi data (*data tampering*).

FR-10: Jika verifikasi *hash* gagal, sistem harus menolak proses dekripsi dan mencatat kejadian dalam *audit log*.

4.4 Manajemen Akses Pengguna

FR-11: Sistem harus mengimplementasikan *Role-Based Access Control* (RBAC) dengan minimal dua peran: **User** dan **Admin**.

FR-12: User hanya dapat mengakses file miliknya sendiri berdasarkan mekanisme otorisasi berbasis kepemilikan.

FR-13: Admin memiliki hak akses untuk monitoring, troubleshooting, dan manajemen sistem secara keseluruhan.

4.5 Audit Trail & Logging

FR-14: Sistem harus mencatat seluruh aktivitas pengguna dalam *audit log*, mencakup: *upload*, *download*, *delete*, akses kunci, serta *timestamp* dan IP address.

FR-15: Sistem harus mencatat seluruh *security events* seperti *unauthorized access attempts*, kegagalan verifikasi integritas, dan kegagalan autentikasi.

FR-16: Log harus disimpan secara aman dan tidak dapat dimodifikasi oleh pengguna untuk keperluan *forensic analysis*.

5. KEBUTUHAN NON-FUNGSIONAL (NON-FUNCTIONAL REQUIREMENTS)

5.1 Performa (Performance)

NFR-01 (Throughput): Sistem harus mampu mencapai *throughput* minimal **30 MB/s** untuk operasi enkripsi dan **25 MB/s** untuk operasi dekripsi.

NFR-02 (Latency): Waktu rata-rata enkripsi file berukuran 5 MB tidak boleh melebihi **200 milidetik**, dan waktu dekripsi tidak boleh melebihi **250 milidetik**.

NFR-03 (Concurrency): Sistem harus mampu menangani hingga **5 *concurrent users*** dengan waktu respons di bawah **300 milidetik**.

NFR-04 (Tolerance): Sistem harus tetap stabil dan *acceptable* pada beban hingga **10 *concurrent users***, dengan pemahaman bahwa diperlukan optimasi infrastruktur untuk *traffic* lebih tinggi.

5.2 Keamanan (Security)

NFR-05: Sistem harus tahan terhadap serangan *brute force* dengan memanfaatkan ukuran kunci RSA 2048-bit yang secara komputasional sangat sulit ditembus dengan teknologi saat ini.

NFR-06: Sistem harus mencegah **100%** upaya *unauthorized access* berdasarkan mekanisme autentikasi dan otorisasi yang ketat.

NFR-07: Sistem harus mendeteksi **100%** upaya manipulasi data melalui mekanisme verifikasi integritas berbasis SHA-256 *hash*.

NFR-08: Sistem harus tahan terhadap serangan *man-in-the-middle* dengan mengimplementasikan komunikasi berbasis HTTPS/TLS antara *client* dan server.

NFR-09: Sistem harus melindungi kunci privat dengan *encryption at rest* menggunakan AES-256-CBC untuk mencegah akses tidak sah.

5.3 Reliabilitas (Reliability)

NFR-10: Sistem harus mencapai tingkat keberhasilan enkripsi dan dekripsi minimal **98%** dari total operasi.

NFR-11: Target *uptime* sistem adalah minimal **99%**, tidak termasuk periode *maintenance* terjadwal.

NFR-12: Sistem harus memiliki mekanisme *graceful degradation* untuk menangani kesalahan tanpa menyebabkan kegagalan total.

5.4 Infrastruktur (Resource Usage)

NFR-13: Infrastruktur harus disiapkan untuk menangani konsumsi memori yang meningkat secara linear dengan ukuran file (estimasi: 15 MB untuk file 1 MB, 542 MB untuk file 100 MB).

NFR-14: Sistem harus dapat beroperasi pada spesifikasi server minimal: **4 CPU cores**, **8 GB RAM**, dan **100 GB storage**.

NFR-15: Pemanfaatan CPU pada beban 5 *concurrent users* diperkirakan mencapai **65%**, sementara pada 10 *concurrent users* mencapai **89%**.

5.5 Usability (Kemudahan Penggunaan)

NFR-16: Antarmuka sistem harus intuitif dan mengikuti prinsip *user-centered design*, memungkinkan pengguna menyelesaikan proses *upload/download* dalam maksimal **3 langkah**.

NFR-17: Sistem harus memberikan *feedback* yang jelas dan informatif untuk setiap operasi tanpa mengekspos informasi sensitif.

NFR-18: Minimal **80%** pengguna harus menyatakan puas terhadap kemudahan penggunaan sistem berdasarkan *usability testing*.

6. RISIKO DAN BATASAN

6.1 Overhead Performa

Terdapat *trade-off* di mana proses enkripsi RSA dengan *exponent* besar akan menambah beban komputasi pada sistem, membuatnya lebih lambat dibandingkan sistem tanpa enkripsi. Penurunan performa sebesar **10–15%** dianggap wajar untuk aplikasi dengan kebutuhan keamanan tinggi.

6.2 Keterbatasan Ukuran File

Sistem dioptimalkan untuk file berukuran hingga **100 MB**. Untuk file yang lebih besar, disarankan menggunakan pendekatan *hybrid cryptography* (kombinasi RSA dan AES) yang belum diimplementasikan dalam versi ini.

6.3 Kompleksitas Manajemen Kunci

Tantangan implementasi meliputi manajemen kunci enkripsi yang aman, termasuk *key generation*, *key storage*, dan *key rotation*, yang memerlukan pemahaman mendalam tentang praktik kriptografi yang benar.

6.4 Skalabilitas

Sistem dirancang untuk menangani hingga **10 *concurrent users*** tanpa infrastruktur tambahan. Untuk *traffic* lebih tinggi, diperlukan implementasi *load balancing* dan *horizontal scaling*.

6.5 Batasan Testing Keamanan

Pengujian keamanan belum mencakup serangan tingkat lanjut seperti *side-channel attacks* atau *fault injection attacks*, sehingga evaluasi lebih lanjut diperlukan untuk deployment pada lingkungan dengan ancaman keamanan yang sangat tinggi.

7. KESIMPULAN SOLUSI

Solusi ini direkomendasikan karena:

1. **Algoritma RSA** menyediakan mekanisme kriptografi asimetris yang terbukti robust untuk melindungi kerahasiaan dan autentikasi dokumen digital.
2. **Integrasi dengan Laravel Filament** memungkinkan penerapan *best practices* dalam *production environment*, termasuk *role-based access control*, *audit logging*, dan *key management* yang aman.
3. **Client-side encryption** memastikan bahwa file terenkripsi sebelum dikirim ke server, mengurangi risiko penyadapan selama transmisi melalui jaringan internet.
4. **SHA-256 hash verification** memberikan jaminan integritas data dengan mendeteksi 100% upaya manipulasi.
5. **Encryption at rest** untuk kunci privat dengan AES-256-CBC menambah lapisan keamanan ekstra pada manajemen kunci.

Sistem ini memberikan nilai lebih dalam perlindungan data sensitif, kepatuhan terhadap regulasi keamanan informasi (GDPR, HIPAA, PCI-DSS), serta menyediakan *audit trail* yang transparan untuk keperluan *compliance* dan *forensic analysis*.

Tanggal: 22 Januari 2026
Penyusun: Azkiya Zahrul Umam, Raihan Fadhli Ramadhan, Ramadhan Tri Rizky Saputra
Institusi: Universitas Esa Unggul