Nama : Eko Nurcahyo

NIM : 20230801169

Business Requirements Document (BRD)

1. Latar Belakang

Perkembangan data digital yang masif meningkatkan risiko keamanan seperti kebocoran data, manipulasi dokumen, dan serangan terhadap kata sandi. Studi Literatur Review (SLR) yang dilakukan mengkaji kinerja, keamanan, dan aplikasi fungsi hash kriptografi modern (SHA-256, SHA-512, SHA-3, dan Blake2). BRD ini menerjemahkan temuan SLR tersebut menjadi kebutuhan bisnis dan sistem yang terstruktur untuk pengembangan dan implementasi solusi keamanan data.

2. Tujuan Bisnis

- Menyediakan solusi keamanan data yang menjamin integritas, autentikasi, dan ketahanan terhadap serangan.
- Memilih dan mengimplementasikan algoritma hash yang optimal berdasarkan trade-off kinerja dan keamanan.
- Mendukung penerapan keamanan password dan integritas dokumen pada sistem informasi organisasi.
- Menjadi dasar pengambilan keputusan teknis untuk pengembangan sistem keamanan ke depan (termasuk IoT/mobile).

3. Ruang Lingkup (Scope)

3.1 In-Scope

- Implementasi fungsi hash: SHA-256, SHA-512, SHA-3, dan Blake2.
- Pengamanan kata sandi (password hashing) dan verifikasi integritas data/dokumen.
- Skema hibrida enkripsi + hashing (mis. AES-256 + SHA3-512) untuk dokumen.
- Evaluasi kinerja (waktu pemrosesan) dan keamanan (avalanche effect, ketahanan brute force).

3.2 Out-of-Scope

- Implementasi kriptografi asimetris secara penuh (RSA/ECC) di luar kebutuhan tanda tangan.
- Pengujian kriptanalisis lanjutan tingkat negara.

4. Pemangku Kepentingan (Stakeholders)

- Business Owner / Manajemen: Menentukan kebijakan keamanan data.

- Tim TI / Developer: Implementasi teknis algoritma hash.
- Tim Keamanan Informasi: Audit dan validasi keamanan.
- Pengguna Sistem: Menggunakan sistem secara aman (login, unggah dokumen).

5. Masalah Bisnis yang Diselesaikan

- Risiko perubahan data tanpa terdeteksi.
- Keamanan password yang lemah terhadap brute force dan rainbow table.
- Ketidakseimbangan antara kebutuhan kecepatan sistem dan keamanan.

6. Kebutuhan Bisnis (Business Requirements)

- Sistem harus mampu memverifikasi integritas data secara konsisten.
- Sistem harus menyediakan mekanisme hashing password yang aman.
- Sistem harus mendukung pilihan algoritma sesuai konteks (kecepatan vs keamanan).
- Sistem harus siap dikembangkan untuk lingkungan resource-constrained (IoT/mobile).

7. Kebutuhan Fungsional (Functional Requirements)

- FR-01: Sistem menghasilkan nilai hash untuk input data menggunakan SHA-256, SHA-512, SHA-3, dan Blake2.
- FR-02: Sistem memverifikasi integritas data dengan membandingkan hash.
- FR-03: Sistem melakukan hashing password dan pencocokan saat autentikasi.
- FR-04: Sistem mendukung kombinasi enkripsi AES-256 dengan hashing (SHA3-512) untuk dokumen.
- FR-05: Sistem menyediakan konfigurasi pemilihan algoritma hash.

8. Kebutuhan Non-Fungsional (Non-Functional Requirements)

- NFR-01 (Keamanan): Hash harus tahan terhadap collision, pre-image, dan brute force.
- NFR-02 (Kinerja): Waktu hashing harus efisien sesuai kebutuhan aplikasi.
- NFR-03 (Skalabilitas): Sistem dapat menangani volume data besar.
- NFR-04 (Reliabilitas): Hasil hashing konsisten dan deterministik.
- NFR-05 (Kompatibilitas): Dapat diintegrasikan dengan sistem dan platform umum.

9. Asumsi dan Batasan

- Sistem berjalan pada lingkungan komputasi standar.
- Algoritma mengikuti standar NIST.
- Implementasi awal belum menguji secara penuh skenario IoT/mobile.

10. Risiko

- Penurunan kinerja jika algoritma berkeamanan tinggi digunakan pada sistem terbatas sumber daya.

- Kesalahan konfigurasi pemilihan algoritma.

11. Kriteria Keberhasilan (Success Metrics)

- Integritas data terjaga (tidak ada perubahan tanpa terdeteksi).
- Autentikasi password aman dan andal.
- Kinerja sistem sesuai SLA.
- Fleksibilitas pemilihan algoritma sesuai kebutuhan.

12. Rencana Pengembangan Lanjutan

- Integrasi teknik salting pada password hashing.
- Optimalisasi implementasi untuk IoT dan mobile.
- Evaluasi algoritma lightweight cryptography.