Business Requirements Document (BRD)

I. Executive Summary

Dokumen ini menjabarkan kebutuhan bisnis untuk implementasi sistem keamanan data berbasis algoritma hash modern sebagai respons terhadap meningkatnya ancaman kejahatan siber. Berdasarkan hasil penelitian komparasi algoritma hash, diperlukan migrasi dan algoritma lama (MD5, SHA-1) ke algoritma modern (SHA-512, SHA-3) dengan penerapan Teknik salting untuk mencapai Tingkat keamanan optimal 97,6%

II. Permasalahan Bisnis

1. **Kerentanan Algoritma Lama**
   Algoritma MD5 dan SHA-1 memiliki Tingkat keberhasilan serangan mencapai 35% pada kata sandi kuat, mengamcam keamanan data pengguna
2. **Risiko Rainbow Table Attack**
   Sistem yang tidak menggunakan salting rentan terhadap serangan berbasis table prekomputasi
3. **Penurunan Kepercayaan Pengguna**
   Insiden Kebocoran data dan peretasan kata sandi menurunkan kepercayaan pengguna terhadap sistem informasi digital

III. Tujuan Bisnis

1. **Peningkatan Keamanan**
   Mencapai Tingkat Keamanan sistem hingga 97,6% melalui implementasi algoritma hash modern dengan salting
2. **Optimalisasi Performa**
   Mempertahankan waktu pemrosesan dibawah 515 ms untuk autentikasi berbasis JWT
3. **Standarisasi Keamanan**
   Menerapkan standar keamanan modern yang tahan terhadap serangan kriptanalisis
4. **Perlindungan Data Pengguna**
   Melindungi kredensial dan data sensitive pengguna dari serangan brute force dan rainbow table

IV. Stakeholder

Stakeholder	Peran	Kepentingan
Tim IT Security	Implementator	Menereapkan dan memelihara sistem keamanan
Developer	Pelaksana Teknis	Integrasi algoritma hash pada sistem aplikasi
End Users	Pengguna akhir	Keamanan data dan kredensial pribadi
Management	Decision Maker	Keputusan investasi dan compliance kemanan
Compliance Officer	Pengawas	Memastikan kepatuhan regulasi keamanan data

V. Kebutuhan Fungsional

1. Implementasi Algoritma Hash Modern

- Sistem harus mendukung penggunaan algoritma SHA-512 dan SHA-3
- Algoritma lama seperti MD5 dan SHA-1 harus dihapus dari sistem produksi.
- Sistem harus mampu melakukan migrasi data hash lama ke algoritma hash modern**.**

2. Penerapan Teknik Salting

- Sistem harus menghasilkan nilai salt yang unik untuk setiap password pengguna.
- Nilai salt harus disimpan secara aman bersama dengan hash password.
- Panjang salt minimal 128-bit untuk menjamin tingkat keamanan yang optimal.

3. Autentikasi Berbasis JSON Web Token (JWT)

- Sistem harus mengimplementasikan SHA-512 untuk proses penandatanganan (signing) token JWT.
- Waktu pemrosesan autentikasi maksimal 515 ms per request.
- Sistem harus menyediakan mekanisme token expiration dan token refresh.

4. Monitoring dan Logging

- Sistem harus melakukan logging terhadap seluruh aktivitas autentikasi.
- Sistem harus mampu melakukan deteksi dan pemberian peringatan (alert) terhadap percobaan serangan brute force.
- Tersedia dashboard monitoring untuk memantau performa algoritma hash dan proses autentikasi.

VI. Kebutuhan Non Fungsional

1. Keamanan

- Sistem harus memiliki tingkat ketahanan keamanan minimal 97,6% terhadap ancaman siber.
- Sistem harus tahan terhadap serangan rainbow table.
- Sistem harus memiliki mekanisme perlindungan terhadap collision attacks pada algoritma hash.

2. Performa

- Waktu respons autentikasi maksimal ≤ 515 ms per permintaan.
- Sistem harus mampu menangani lebih dari 100.000 request per hari.
- Implementasi keamanan tidak boleh memberikan dampak signifikan terhadap pengalaman pengguna (user experience).

3. Reliability (Keandalan)

- Sistem harus memiliki tingkat uptime minimal 99,9%.
- Tersedia mekanisme backup dan recovery untuk menjaga integritas data.
- Sistem mendukung failover capability guna memastikan layanan tetap berjalan saat terjadi kegagalan.

4. **Maintainability (Kemudahan Pemeliharaan)**
    - Sistem harus dilengkapi dengan dokumentasi teknis yang lengkap.
    - Arsitektur sistem harus bersifat modular agar mudah dikembangkan.
    - Sistem mendukung jalur peningkatan (upgrade) algoritma hash secara mudah di masa depan.

VII. Metrik Keberhasilan

Metrik	Target	Baseline
Tingkat Keamanan Sistem	97,6%	65% (MD5)
Keberhasilan serangan pada password	≤ 20%	35% (MD5)
Waktu Pemrosesan Autentikasi	≤515 ms	134 ms (MD5)
Insiden Kebocoran data	0 per tahun	Data tidak tersedia

VIII. Roadmap Implementasi

IX. Risiko dan Mitigasi

Risiko 1: Penurunan Performa Sistem

Penggunaan algoritma SHA-512 memiliki waktu komputasi yang lebih tinggi dibandingkan MD5 (±199 ms dibandingkan ±134 ms), yang berpotensi memengaruhi performa sistem.

Mitigasi:

- Optimalisasi infrastruktur sistem
- Penerapan mekanisme caching
- Implementasi load balancing

Risiko 2: Kompleksitas Migrasi Data

Proses migrasi hash password dari algoritma MD5 ke SHA-512 untuk pengguna yang sudah terdaftar berpotensi menimbulkan kompleksitas teknis.

Mitigasi:

- Penerapan migrasi bertahap (*phased migration*)
- Dukungan dual-mode selama masa transisi
- Penerapan proses re-authentication bagi pengguna

Risiko 3: Resistensi Tim Teknis

Adanya kurva pembelajaran (learning curve) bagi tim teknis dalam mengimplementasikan algoritma kriptografi baru.

Mitigasi:

- Penyelenggaraan program pelatihan (training)
- Penyediaan dokumentasi teknis yang lengkap
- Dukungan teknis berkelanjutan

X. Asumsi dan Dependencies

Asumsi

- Infrastruktur server yang digunakan telah mendukung proses komputasi algoritma hash modern.
- Tersedianya anggaran yang memadai untuk melakukan peningkatan dan pengembangan sistem.
- Tim pengembang memiliki pengetahuan dasar mengenai konsep dan implementasi kriptografi.
- Pengguna bersedia melakukan proses re-authentication selama tahap migrasi sistem berlangsung.

Dependensi

- Adanya persetujuan resmi dari pihak manajemen untuk pelaksanaan implementasi sistem.
- Ketersediaan library kriptografi yang andal, seperti hashlib dan cryptography.
- Dilakukannya peningkatan (upgrade) pada basis data untuk mendukung penyimpanan nilai salt.
- Ketersediaan lingkungan pengujian (testing environment) yang memadai.