PROJECT AKHIR KEAMANAN INTEGRITAS DATA

Security Service: Digital Signature & Enkripsi

Nagatan Alief Putra Silahen (24031554086)
Muslim Fazlur Rohman (24031554154)

Muhammad Ramadhan Albaary Putra (24031554161)
Kafka Praya Firmansyah (24031554182)

Universitas Negeri Surabaya

Latar Belakang

Pengembangan layanan API berbasis **FastAPI** yang berfungsi sebagai *Trusted Authority Server* untuk sistem Punk Records.menangani keamanan komunikasi digital melalui penyimpanan public key dan verifikasi digital signature

Fokus utama adalah menangani aspek keamanan komunikasi digital dengan mekanisme penyimpanan **Public Key** dan verifikasi **Digital Signature**.

Rumusan Masalah

- Bagaimana membangun Trusted Authority yang efektif mengelola Public Key pengguna?
- Bagaimana mekanisme Digital Signature menjamin bahwa pesan tidak dimodifikasi selama transmisi?
- Mengapa enkripsi AES dan Secure Session (JWT) diperlukan untuk melindungi akses layanan?

Metode

FastAPI

Framework modern untuk membangun API dengan performa tinggi dan dokumentasi otomatis.

AES-256

Standar enkripsi simetris untuk menjaga kerahasiaan pesan antar pengguna secara efisien.

JWT

JSON Web Token untuk mengelola Secure Session dan autentikasi stateless.

Landasan Teori

Kriptografi Kunci Publik & Digital Signature

Kriptografi Kunci Publik

Mekanisme Kunci

Metode yang menggunakan sepasang kunci yang saling berkaitan secara matematis:

- **Public Key:** Dibagikan bebas untuk verifikasi dan enkripsi.
- **Private Key:** Rahasia pribadi untuk tanda tangan dan dekripsi.

Digital Signature

Tanda tangan digital dibuat dengan menghitung nilai **hash** dari isi dokumen, kemudian menandatanganinya menggunakan **Private Key**.

Sistem ini menjamin:

- Autentikasi Pengirim
- Integritas Data
- Non-repudiation

Arsitektur Implementasi

api.py

Logika server: Verifikasi signature, relay pesan terenkripsi, dan fitur Sign PDF.

main.py

Entry point aplikasi yang mengaktifkan server web Uvicorn pada jaringan lokal.

client.py

Sisi pengguna: Pembuatan pasangan kunci RSA dan penandatanganan pesan lokal.

Endpoint Layanan Utama

Endpoint	Fungsi Utama	Keamanan
/login	Autentikasi User & Generate Token	JWT Session
/store	Registrasi Public Key User	Secure Upload
/relay	Pengiriman Pesan Antar User	AES-256 Encrypted
/sign-pdf	Tanda Tangan Digital Dokumen	RSA Signing

Alur Kerja Sistem

1. Login

Dapatkan JWT untuk akses secure session.

2. Store Key

Upload Public Key klien ke Trusted Server.

3. Relay

Kirim pesan aman dengan enkripsi AES.

4. Decryption

Melakukan dekripsi untuk melihat pesan dalam bentuk plain teks

5. Sign PDF

Validasi dokumen PDF secara kriptografis.

Kesimpulan

Layanan API yang dikembangkan berhasil berfungsi sebagai trusted authority server dengan kemampuan menyimpan public key dan memverifikasi digital signature untuk menjamin keaslian serta integritas pesan. Sistem juga menerapkan relay pesan aman menggunakan AES 256-bit dan secure session (JWT) sehingga kerahasiaan data dan kontrol akses dapat terjaga. Selain itu, fitur tanda tangan digital dokumen PDF berjalan dengan baik dan memastikan keaslian dokumen, sehingga seluruh sistem telah memenuhi aspek penilaian tugas dan tujuan keamanan yang ditetapkan.

Terima Kasih

Ada Pertanyaan?

Proyek Akhir Keamanan & Integritas Data - Sains Data UNESA 2025