LAPORAN TANDA TANGAN DIGITAL

UAS Kriptografi - Implementasi RSA & SHA-256

INFORMASI DOKUMEN

Asal Dokumen:	test_sertifikat_3.pdf
Waktu Proses:	2026-01-12 19:58:05
Jenis Proses:	Verifikasi Tanda Tangan
Algoritma:	RSA-SHA256-PSS
Ukuran Kunci:	2048-bit

DETAIL TANDA TANGAN

Timestamp:	2026-01-12T19:58:04.885348
Panjang Tanda Tangan:	256 bytes
Hash Algorithm:	SHA-256
Document Hash:	28cffe9b4e7372dc66422ffad38b4100ff7398f22bee37acee1660cfaee35df1

HASIL VERIFIKASI

Aspek Keamanan	Status	Keterangan
Autentikasi	VALID	Verifikasi identitas penandatangan
Integritas Data	INTACT	Dokumen tidak berubah setelah ditandatangani
Non-repudiasi	PROVEN	Penandatangan tidak dapat menyangkal tandatangannya
Hash Match	MATCH	Kesesuaian hash dokumen

ANALISIS KEAMANAN

1. **RSA 2048-bit**: Tingkat keamanan tinggi, tahan terhadap serangan brute-force
2. **SHA-256**: Fungsi hash kriptografi yang kuat, resisten collision
3. **PSS Padding**: Meningkatkan keamanan terhadap serangan tertentu
4. **Timestamp**: Mencegah replay attack dengan pencatatan waktu
5. **Digital Signature**: Memberikan autentikasi, integritas, dan non-repudiasi
6. **Hash Verification**: Memastikan dokumen tidak berubah setelah ditandatangani

Kesimpulan: Sistem tanda tangan digital ini **BERHASIL** memverifikasi keaslian dan integritas dokumen.