

LAPORAN TANDA TANGAN DIGITAL

UAS Kriptografi - Implementasi RSA & SHA-256

INFORMASI DOKUMEN

| | |
|---------------|---------------------------|
| Asal Dokumen: | 20260112_204818_ toko.pdf |
| Waktu Proses: | 2026-01-12 20:48:28 |
| Jenis Proses: | Verifikasi Tanda Tangan |
| Algoritma: | RSA-SHA256-PSS |
| Ukuran Kunci: | 2048-bit |

DETAIL TANDA TANGAN

| | |
|-----------------------|--|
| Timestamp: | 2026-01-12T20:48:26.682608 |
| Panjang Tanda Tangan: | 256 bytes |
| Hash Algorithm: | SHA-256 |
| Document Hash: | 459fe429cee4fb8026580cef7a7e0982840adae31aca6f52defe94a5f7976e1d |

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

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

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

Generated by UAS Kriptografi Digital Signature System
Report ID: 20260112_204828