

LAMPIRAN TEKNIS BUKTI KONFIGURASI KRIPTOGRAFI

SERTIFIKAT DIGITAL · TLS · ENKRIPSI DISK · VPN

Nomor Dokumen	:	.../.../Bukti-Kripto/ Diskominfo/2026
Induk Laporan	:	Inventarisasi Aset yang Dienkripsi & Laporan Awal Kriptografi
Indikator	:	I11 — Penerapan Kriptografi untuk Keamanan Data (IKASANDI), Level 1
Periode data	:	Semester I Tahun 2026
Dasar	:	Perbup 1/2025; Perbup 2/2025; Perbup 48/2025

1. Bukti Konfigurasi TLS/HTTPS Layanan Web

Tangkapan layar berikut membuktikan bahwa layanan web Pemerintah Kabupaten Aceh Tengah telah menggunakan koneksi terenkripsi HTTPS/TLS:

[LAYAR SCREENSHOT]

Gambar 1.1 — Sertifikat TLS Website acehtengahkab.go.id

<https://www.acehtengahkab.go.id> (kunci gembira hijau, TLS 1.3)

[TAMPILAN LAYAR]

Sertifikat yang diterbitkan oleh otoritas sertifikat terpercaya (Let's Encrypt/CA). Protokol aktif: TLS 1.2/1.3. Tidak menggunakan SSLv3/TLS 1.0/1.1.

[LAYAR SCREENSHOT]

Gambar 1.2 — Sertifikat Portal OpenData (data.acehtengahkab.go.id)

https://data.acehtengahkab.go.id (TLS aktif)

[TAMPILAN LAYAR]

Sertifikat wildcard/untuk subdomain data dengan redirect HTTP→HTTPS.

[LAYAR SCREENSHOT]

Gambar 1.3 — Hasil SSL/TLS Configuration Test (SSL Labs/immuniweb)

Contoh: ssllabs.com/sslttest (skor A/A-) — dilekatkan jika tersedia

[TAMPILAN LAYAR]

Laporan hasil uji konfigurasi TLS yang menunjukkan protokol, cipher suite, dan skor keamanan.

2. Bukti Enkripsi Email (STARTTLS/TLS)

Screenshot konfigurasi server email menunjukkan koneksi terenkripsi pada pengiriman (SMTP STARTTLS) dan penerimaan (IMAPS/POP3S):

[LAYAR SCREENSHOT]

Gambar 2.1 — Konfigurasi SMTP outgoing (port 587 STARTTLS) dan IMAPS (993 SSL/TLS)

mail.acehtengahkab.go.id

[TAMPILAN LAYAR]

Setting klien email pegawai mewajibkan koneksi terenkripsi.

[LAYAR SCREENSHOT]

Gambar 2.2 — Webmail diakses melalui HTTPS

<https://mail.acehtengahkab.go.id>

[TAMPILAN LAYAR]

Halaman login webmail dengan indikator gembok/HTTPS.

3. Bukti Konfigurasi VPN (IPsec/OpenVPN)

[LAYAR SCREENSHOT]

Gambar 3.1 — Pengaturan/konfigurasi VPN Gateway

VPN gateway pemkab (IPsec site-to-site atau OpenVPN remote access)

[TAMPILAN LAYAR]

Cipher yang digunakan: AES-256-CBC/GCM; autentikasi RSA-2048/SHA-256; PSK/sertifikat.

[LAYAR SCREENSHOT]

Gambar 3.2 — Daftar koneksi VPN aktif/log

Dashboard VPN — status terowongan

[TAMPILAN LAYAR]

Membuktikan saluran VPN digunakan untuk akses administratif dan sinkronisasi data.

4. Bukti Enkripsi Disk/Volume dan Backup

[LAYAR SCREENSHOT]

Gambar 4.1 — Enkripsi partisi data dengan LUKS/BitLocker

Server database e-Office/absensi/kependudukan

[TAMPILAN LAYAR]

Output perintah cryptsetup/BitLocker status yang menunjukkan volume terenkripsi AES-256.

[LAYAR SCREENSHOT]

Gambar 4.2 — Enkripsi file backup

Folder backup harian/mingguan

[TAMPILAN LAYAR]

File backup dalam bentuk arsip terenkripsi (.gpg/.age/terenkripsi) dengan ekstensi/indikator terkunci.

[LAYAR SCREENSHOT]

Gambar 4.3 — Enkripsi laptop kerja (BitLocker)

Laptop pejabat/admin (sebagian perangkat)

[TAMPILAN LAYAR]

Status BitLocker "On" pada perangkat Windows.

5. Bukti pada Aplikasi (password hash, TTE)

[LAYAR SCREENSHOT]

Gambar 5.1 — Halaman login e-Office/e-Absensi via HTTPS

<https://eoffice.acehtengahkab.go.id>

[TAMPILAN LAYAR]

Aplikasi internal diakses melalui HTTPS; password disimpan dalam bentuk hash (bcrypt/SHA-256+salt).

[LAYAR SCREENSHOT]

Gambar 5.2 — Tanda Tangan Elektronik (TTE) pada naskah dinas

Modul TTE e-Office (BSrE)

[TAMPILAN LAYAR]

Bukti naskah ditandatangani secara elektronik dengan sertifikat dari BSrE/BSSN (visual dan info sertifikat).

[LAYAR SCREENSHOT]

Gambar 5.3 — Sertifikat TTE Pejabat

Akun BSrE

[TAMPILAN LAYAR]

Daftar sertifikat digital TTE yang dimiliki pejabat penandatangan.

6. Rekap Daftar Sertifikat & Masa Berlaku

No	Layanan/ Sertifikat	Penerbit	Protokol/ Algoritma	Masa Berlaku	Status
1	acehtengahkab. go.id	Let's Encrypt	TLS 1.3, RSA 2048/ECC	90 hari (auto- renew)	Aktif
2	data.acehtenga hkab.go.id	Let's Encrypt	TLS 1.2/1.3	90 hari	Aktif
3	eoffice.acehteng ahkab.go.id	Internal CA	TLS 1.2	1—2 tahun	Aktif
4	mail.acehtenga hkab.go.id	Internal CA	STARTTLS/ IMAPS	1 tahun	Aktif
5	VPN gateway	Internal CA/PSK	AES-256,	1—2 tahun	Aktif

			RSA-2048		
6	Sertifikat TTE Pejabat	BSrE (BSSN)	PKS#7/ RSA-2048	Sesuai kebijakan	Aktif/sebagian
7	Sertifikat penandatanganan kode/dokumen	BSrE/Internal	RSA-2048	1 tahun	Aktif

7. Penutup

Lampiran teknis ini menjadi bagian tidak terpisahkan dari Laporan Awal Penerapan Kriptografi Kabupaten Aceh Tengah. Seluruh bukti konfigurasi pada lampiran ini diverifikasi oleh Bidang Persandian dan Keamanan Informasi Dinas Komunikasi dan Informatika dan disimpan sebagai arsip elektronik. Pada Level 1 ini, bukti konfigurasi sudah tersedia untuk seluruh layanan publik dan server utama, sementara penguatan lebih lanjut (manajemen kunci terpusat, enkripsi perangkat akhir menyeluruh, dan audit konfigurasi) direncanakan pada level berikutnya.

Takengon, 2026

Kepala Bidang Persandian & Keamanan Informasi,

(.....)

NIP.