[LAMBANG KABUPATEN]

PEMERINTAH KABUPATEN ACEH TENGAH
DINAS KOMUNIKASI DAN INFORMATIKA
BIDANG PERSANDIAN DAN KEAMANAN INFORMASI
Jalan Tunas Harapan No. 1 Takengon 24514

INVENTARISASI ASET YANG DIENKRIPSI DAN LAPORAN AWAL PENERAPAN KRIPTOGRAFI UNTUK KEAMANAN DATA

KABUPATEN ACEH TENGAH

TAHUN 2026

Nomor Dokumen	:	.../.../Invent-Kripto/ Diskominfo/2026
Indikator Pemdi	:	I11 — Tingkat Kematangan Penerapan Kriptografi (IKASANDI)
Level yang dibuktikan	:	Level 1 — Initiate
Dasar utama	:	Perbup 1/2025 tentang Penataan Pola Hubungan Komunikasi Sandi; Perbup 2/2025 tentang Penyelenggaraan Persandian; Perbup 48/2025 Arsitektur SPBE
Unit Pengampu	:	Bidang Persandian dan Keamanan Informasi — Diskominfo
Periode data	2025—Semester I 2026	

I. Latar Belakang

Kriptografi merupakan mekanisme utama untuk menjamin kerahasiaan (confidentiality), keutuhan (integrity), keaslian (authenticity), dan/atau nirsangkal (non-repudiation) data yang dikelola Pemerintah Kabupaten Aceh Tengah. Penyelenggaraan persandian untuk pengamanan informasi telah didasari Peraturan Bupati Aceh Tengah Nomor 1 Tahun 2025 tentang Penataan Pola Hubungan Komunikasi Sandi dan Peraturan Bupati Aceh Tengah Nomor 2 Tahun 2025 tentang Penyelenggaraan Persandian di Lingkungan Pemerintah Kabupaten Aceh Tengah.

Sebagai bukti dukung awal (Level 1 — Initiate) pada Indikator 11 Pemerintah Digital (Tingkat Kematangan Penerapan Kriptografi untuk Keamanan Data / IKASANDI), Bidang Persandian dan Keamanan Informasi Dinas Komunikasi dan Informatika melakukan inventarisasi awal terhadap aset yang dienkripsi, meliputi data dalam keadaan transit (in-transit), data saat disimpan (at-rest), dan data saat digunakan/diolah (in-use). Inventarisasi ini juga menyajikan laporan awal penerapan kriptografi sebagai dasar peningkatan pada level berikutnya.

II. Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan UU No. 19 Tahun 2016;
2. Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang (terkait data pribadi);
3. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
4. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
5. Peraturan Presiden Nomor 133 Tahun 2024 tentang Badan Siber dan Sandi Negara;
6. Peraturan BSSN tentang Pedoman Manajemen Keamanan Informasi dan Persandian;
7. Peraturan Menteri PANRB Nomor 8 Tahun 2026 tentang Indikator Pemerintah Digital;
8. Peraturan Bupati Aceh Tengah Nomor 1 Tahun 2025 tentang Penataan Pola Hubungan Komunikasi Sandi di Lingkungan Pemerintah Kabupaten Aceh Tengah;
9. Peraturan Bupati Aceh Tengah Nomor 2 Tahun 2025 tentang Penyelenggaraan Persandian di Lingkungan Pemerintah Kabupaten Aceh Tengah;
10. Peraturan Bupati Aceh Tengah Nomor 48 Tahun 2025 tentang Arsitektur SPBE.

III. Maksud dan Tujuan

Inventarisasi dan laporan awal ini dimaksudkan untuk:

- mendata seluruh aset/data yang saat ini telah dilindungi dengan mekanisme kriptografi;
- memetakan status penerapan enkripsi pada data in-transit, at-rest, dan in-use;
- mengidentifikasi algoritma, modul, kunci, dan sertifikat yang digunakan;

- menjadi dasar/baseline untuk peningkatan penerapan kriptografi pada level berikutnya.

IV. Ruang Lingkup

Inventarisasi mencakup sistem/aplikasi/layanan yang dikelola oleh Dinas Komunikasi dan Informatika serta Perangkat Daerah yang menggunakan infrastruktur SPBE Kabupaten Aceh Tengah, dengan klasifikasi status data:

- In-transit: data yang dikirim melalui jaringan (internet/VPN);
- At-rest: data yang disimpan pada server, basis data, media penyimpanan, atau cadangan (backup);
- In-use: data yang sedang diolah di memori/sistem (sejauh dapat diidentifikasi).

V. Daftar Aset yang Dienkripsi

V.1. Data In-Transit

No	Layanan/ Saluran	Mekanisme	Algoritma/ Protokol	Penyedia/ Modul	Keterangan
1	Website resmi acehtengahkab.go.id	HTTPS/TLS	TLS 1.2/1.3	Let's Encrypt (sertifikat)	Selalu aktif, redirect HTTP→HTTPS
2	Portal OpenData/Satu Data	HTTPS/TLS	TLS 1.2/1.3	Sertifikat SSL	Selalu aktif
3	Layanan e-Office	HTTPS/TLS	TLS 1.2	Sertifikat internal/CA	Akses internal+eksternal
4	Webmail dinas (@acehtengahkab.go.id)	HTTPS/TLS + STARTTLS	TLS 1.2/1.3, STARTTLS	Mail server + CA	Enkripsi koneksi email
5	Akses jarak jauh (VPN)	IPsec/OpenVPN	AES-256, RSA-2048	VPN gateway	Untuk petugas/operator
6	Integrasi/API antar aplikasi	HTTPS + token	TLS 1.2, JWT/API key	API gateway sederhana	Sebagian layanan prioritas
7	Layanan perizinan (DPMPTSP online)	HTTPS/TLS	TLS 1.2/1.3	Sertifikat SSL	Layanan publik
8	Administrasi kependudukan (sinkronisasi)	HTTPS/VPN	TLS 1.2 + IPsec	VPN ke pusat	Saluran terenkripsi
9	Akses jaringan Wi-Fi pejabat	WPA2-Enterprise	AES	RADIUS internal	Jaringan internal

V.2. Data At-Rest

No	Lokasi/Jenis Data	Mekanisme	Algoritma/ Modul	Penyedia	Keterangan
1	Database e-Office	Enkripsi berkas/tablespace	AES-256 (database native)	DBMS	Backup terenkripsi
2	Database e-Absensi	Enkripsi data sensitif	AES-256	Aplikasi/DBMS	Data biometrik wajah & NIK
3	Database kependudukan	Enkripsi	LUKS AES-256	Diskominfo	Akses terbatas

	(salinan/cache)	disk/partisi			
4	Database webmail/email	Enkripsi penyimpanan mailbox	TLS at-rest + password hash (bcrypt)	Mail server	Termasuk arsip
5	Storage dokumen/file server	Enkripsi volume	BitLocker/LUKS	Server penyimpanan	Folder terbatas
6	Backup data harian/mingguan	Enkripsi berkas backup	AES-256 (terkompres terenkripsi)	Tools backup	Disimpan di storage terpisah
7	Sertifikat & kunci TTE	Penyimpanan kunci privat	Hardware token (USB/BSrE)	BSrE/BSSN	Untuk pejabat
8	Kredensial admin/rahasia aplikasi	Penyimpanan terenkripsi	AES-256 / vault sederhana	Berkas konfigurasi terbatas	Akses hanya admin

V.3. Data In-Use

No	Mekanisme	Penerapan Saat Ini	Keterangan
1	Enkripsi memori proses	Belum diterapkan (direncanakan)	Saat ini proteksi in-use mengandalkan kontrol akses
2	Pengelolaan kunci (key management)	Penyimpanan kunci sederhana, terpisah dari data	Pengembangan KMS terpusat direncanakan pada Level 2/3
3	Masking data sensitif saat tampil	Diterapkan pada sebagian aplikasi (NIK, nomor HP)	Sebagian layanan publik
4	Penghapusan aman (secure deletion)	Dilakukan manual untuk media yang akan diganti	Akan distandarkan melalui SOP

VI. Daftar Sertifikat dan Kunci Kriptografi

No	Jenis	Pemilik/ Pengguna	Penerbit	Masa Berlaku	Status
1	Sertifikat SSL/TLS website	acehtengahkab.go.id	Let's Encrypt	1 tahun (auto-renew)	Aktif
2	Sertifikat SSL/TLS OpenData	data.acehtengahkab.go.id	Let's Encrypt	1 tahun	Aktif
3	Sertifikat SSL/TLS e-Office	eoffice.acehtengahkab.go.id	Internal CA	2 tahun	Aktif
4	Sertifikat Tanda Tangan Elektronik	Pejabat Penandatangan	BSrE (BSSN)	Sesuai kebijakan BSrE	Aktif/sebagian
5	Sertifikat VPN	Gateway VPN	Internal CA	1—2 tahun	Aktif
6	Kunci enkripsi backup	Diskominfo	Generate internal	Rotasi tahunan	Aktif
7	Sertifikat email	Mail server	Internal CA/self-signed	1 tahun	Aktif

VII. Standar dan Algoritma yang Digunakan

No	Kebutuhan	Algoritma/Standar	Tingkat Penerapan
1	Enkripsi simetris (data)	AES-256	Digunakan untuk storage, backup, VPN

2	Enkripsi transit	TLS 1.2/1.3, HTTPS, STARTTLS	Wajib pada layanan publik
3	Hashing kata sandi	bcrypt / SHA-256 dengan salt	Diterapkan pada sebagian besar aplikasi
4	Integritas data	HMAC-SHA256 (sebagian integrasi)	Diterapkan terbatas
5	Tanda tangan elektronik	Sertifikat BSrE	Diterapkan untuk pejabat
6	Pertukaran kunci	RSA-2048, ECDHE pada TLS	Diterapkan
7	Standar acuan	Permenkominfo/ Peraturan BSSN; NIST sebagai acuan	Sebagian besar telah mengikuti standar nasional

VIII. Ringkasan Penerapan Awal

No	Kategori Persandian	Jumlah Aset Teridentifikasi	Sudah Dienkripsi	Belum/Sebagian
1	Layanan publik (website/portal)	6	6	0
2	Aplikasi internal (e-office, e-absensi, email)	3	3	0
3	Database server	5	5 (at-rest)	0
4	Media penyimpanan/backup	3	3	0
5	Saluran integrasi/API	5	3	2
6	VPN/akses jarak jauh	1	1	0
7	Kredensial/ rahasia aplikasi	5	4	1
8	Perangkat akhir (laptop/PC)	~ 300	25 (hardware/ BitLocker)	275
	TOTAL	~ 328	50	278 (mayoritas perangkat akhir)

Sebagian besar layanan publik dan server utama telah menerapkan enkripsi in-transit dan at-rest. Namun, enkripsi pada perangkat akhir, penerapan manajemen kunci terpusat, dan masking/proteksi data in-use masih perlu ditingkatkan pada tahap selanjutnya.

IX. Temuan Awal dan Kesenjangan

- Seluruh layanan publik utama telah menggunakan HTTPS/TLS;
- Database dan backup penting sudah dienkripsi at-rest dengan AES-256;
- Tanda Tangan Elektronik (TTE) berbasis sertifikat BSrE telah digunakan pejabat;
- Enkripsi pada perangkat akhir (laptop/PC) masih terbatas (±25 dari ~300 unit);
- Belum ada manajemen kunci (KMS) terpusat dan rotasi kunci yang terjadwal;

- Penggunaan kriptografi untuk integritas data (HMAC) dan email signing baru diterapkan terbatas;
- Audit/validasi konfigurasi kriptografi belum dilakukan secara menyeluruh.

X. Rencana Tindak Lanjut

No	Kegiatan	Target Waktu	Penanggung Jawab
1	Memperluas enkripsi perangkat akhir (BitLocker/LUKS) untuk seluruh laptop pegawai	2026—2027	Bidang Persandian
2	Membangun/ menetapkan manajemen kunci (KMS) terpusat	2027	Bidang Persandian
3	Menyusun SOP/kebijakan penggunaan kriptografi, algoritma, dan rotasi kunci	Triwulan III—IV 2026	Bidang Persandian & Bagian Hukum
4	Menonaktifkan protokol lemah (SSLv3/TLS 1.0/1.1) dan algoritma usang	Triwulan III 2026	Bidang APTIKA
5	Mengaktifkan TTE untuk seluruh pejabat/operator yang berwenang	2026—2027	Diskominfo & BKPSDM
6	Uji konfigurasi/TLS configuration review	Semester II 2026	Bidang Persandian
7	Penerapan HMAC/penandatanganan pada integrasi API prioritas	2027	Bidang APTIKA & Persandian

XI. Penutup

Demikian inventarisasi aset yang dienkripsi dan laporan awal penerapan kriptografi untuk keamanan data di Kabupaten Aceh Tengah disusun. Dokumen ini merupakan baseline penerapan pada Level 1 — Initiate dan menjadi dasar peningkatan tata kelola persandian menuju Level 2 (Emerging) dan Level 3 (Established) sesuai target Indeks IKASANDI.

Takengon, ... 2026

Kepala Bidang Persandian dan

Keamanan Informasi,

(.....)

NIP. .....

Menyetujui,

Kepala Dinas Komunikasi dan Informatika,

(.....)

NIP. .....