

SecureStream 256 Pro — Karta techniczna

Wersja dokumentu: 2.3 • Data: 29.09.2025

Wersja oprogramowania: 2.3 • Format pliku: ENCV2 / SGCM2 / SGCM2F / EMETA2

Autor: Paweł Pawlikowski • Źródło: www.securestream256pro.com • Kontakt: support@securestream256pro.com

Zestaw kryptograficzny (skrót)

Algorytm danych: AES-256-GCM, tag 128-bit.

KDF (hasło): Argon2id; domyślnie t=5, m=256 MiB, p=6; sól 16 B.

Plik-klucz (tryb alternatywny): 32 B (wymagane dokładnie 32 bajty).

HKDF — rozdzielenie kluczy i etykiety

HKDF_INFO_AEAD = "SecureStream256Pro AEAD key" — klucz bazowy AEAD.

HKDF_INFO_KCV = "SecureStream256Pro KCV key" — klucz do wczesnej weryfikacji (KCV).

HKDF_INFO_FILEKEY = "SecureStream256Pro master from filekey" — master z pliku-klucza.

HKDF_INFO_FILEMAC = "SecureStream256Pro file-mac key" — globalny MAC pliku.

Per-file AEAD: sól HKDF = BLAKE2s(32) z header_bytes || nonce_prefix; info="SecureStream256Pro AEAD per-file".

KCV (Key Check Value)

Wczesna weryfikacja klucza (natychmiastowe zakończenie przy błędnym hasle/kluczu).

Długość KCV = 32 bajty.

Strumień i AAD

Nonce GCM: 12 B = 8 B prefix + 4 B licznik; unikalny dla każdego chunka.

AAD (wspólne + per chunk):

AAD_common = header_bytes || "SGCM2" || chunk_bytes || nonce_prefix

AAD = AAD_common || chunk_index

Nagłówek / Stopka

Nagłówek ENCV2: zawiera MAGIC, tryb (hasło/plik-klucz + flaga metadanych), KDF=Argon2id, długości name/ext, t/m/p, salt, KCV; całe header_bytes stanowią AAD.

Stopka SGCM2F: total_chunks (uint32), total_plain (uint64), BLAKE2s(32) po wszystkich ciphertextach, HMAC-SHA256 (przycięty do 32 B) nad AAD_common || total_chunks || total_plain || digest. Stopka weryfikowana przed atomowym zapisem.

Metadane i prywatność

Tryb „Ukryj metadane”: nazwa/rozszerzenie mogą być ukryte w EMETA2 (wewnętrzny blok META, max 65 535 B).

Prywatność: aplikacja działa w pełni offline; brak telemetrii. Logi lokalne i bez danych wrażliwych.

Filtrowanie: pomijane są symplinki, junctiony i katalogi systemowe tmp_secure i backup.

Wejście/wyjście i spójność zapisu

Zapis atomowy: tymczasowy plik → fsync → os.replace → fsync(dir) po pozytywnej weryfikacji stopki.

Katalog TMP: ukryty, czyszczony przy starcie programu.

Backup (opcjonalny): wykonywany zgodnie z konfiguracją; błędy kopii nie przerywają szyfrowania.

Unicode: pełna obsługa znaków (emoji, złożone skrypty).

Limity i zachowanie (Windows / ogólne)

Rozmiar chunku: do 256 MiB (MAX_CHUNK_BYTES).

Maks. liczba chunków: $2^{32} - 1$.

Maks. plaintext: 2 TiB (twardy limit egzekwowany w pre-skane i strumieniu).

Ścieżki Windows: pełna ścieżka \approx 240 znaków; nazwy skracane i numerowane przy kolizjach.

Bezpieczne nadpisywanie: brak (świadoma decyzja; brak gwarancji skuteczności na SSD/flash).

Suma kontrolna (integralność wydania)

SHA-256 (plik binarny)

5E8D965F89BF4FF04483DCDD704D247486F8CE8FF91AAB3DDCF5DEDF676160A8 SecureStream 256 Pro PL.exe

„Jak zweryfikować”: PowerShell: **(Get-FileHash -Algorithm SHA256 'ścieżka\SecureStream 256 Pro.exe').Hash**