

SecureStream 256 Pro — Karta techniczna

Wersja dokumentu: 1.0 • Data: 27.08.2025 • Wersja oprogramowania: 1.0 • Format pliku: ENCV1

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

Zestaw kryptograficzny (skrót)

Algorytm danych: AES-256-GCM (poufność + integralność), tag 128-bit.

KDF (hasło): Argon2id (domyślnie: m = 128 MiB, t = 3, p = 1; sól 16 B).

Plik-klucz: 32 B (tryb alternatywny).

HKDF (plik-klucz / etykiety domenowe):

HKDF_INFO_AEAD = "SecureStream256Pro AEAD v1"

HKDF_INFO_KCV = "SecureStream256Pro KCV v1"

HKDF_INFO_FILEKEY = "SecureStream256Pro FILEKEY v1"

KCV: wczesna weryfikacja klucza przed rozpoczęciem deszyfracji.

Nonce: unikalny per plik (96-bit, GCM).

Nagłówek: [magic/wersja], sól, parametry KDF, nonce, opcjonalne metadane.

Metadane i prywatność

Tryb „Hide metadata” (opcjonalnie): nazwa/rozszerzenie oryginalnego pliku mogą być ukryte w szyfrogramie (EMETA).

Prywatność: aplikacja działa w 100% offline; brak telemetrii. Logi pozostają lokalnie.

Wejście/wyjście i spójność zapisu

Zapis atomowy: tymczasowy plik w katalogu docelowym → fsync → atomowy os.replace.

Katalog tymczasowy: krótka nazwa (np. tmp), wykluczony ze skanowania.

Backup (opcjonalny): możliwe utworzenie jawnej kopii źródła; stosować świadomie.

Unicode: pełna obsługa znaków (emoji, złożone skrypty); pomijanie symlinków/junctionów.

Limity i zachowanie w systemie Windows

MAX_PATH: na systemach bez „long paths” pełna ścieżka ≈ 260 znaków, pojedyncza nazwa ≈ 255 znaków.

Bezpieczny fallback: w skrajnych przypadkach (stare systemy, bardzo długie ścieżki) aplikacja nie przerywa pracy – pozostawia jawną kopię obok pliku .enc i prosi o skrócenie ścieżki; szyfrogram .enc pozostaje prawidłowy.

Parametry wykonawcze (skrót)

Rozmiar bloku (chunk): konfigurowalny (np. 1–256 MiB; dobór wg RAM/IO).

Wymagania (min): Windows 10/11 x64; zalecane ≥ 8 GB RAM przy domyślnym KDF 128 MiB.

Bezpieczne nadpisywanie: brak (świadoma decyzja; na SSD/flash nie przynosi gwarantowanego efektu)

Integralność wydania

SHA-256 (plik binarny):

BADD4D62886744BBA46ABEACA6C4F931E0ED7167D23EF4C790A1F8E09DB3B031 SecureStream 256 Pro.exe

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