

SecureStream 256 Pro — Datasheet

Document Version: 1.0 • Date: 29.08.2025 • Software Version: 1.0 • File Format: ENCV1

Author: Paweł Pawlikowski • Source: www.securestream256pro.com • Contact: support@securestream256pro.com

Cryptographic Suite (Summary)

Data Algorithm: AES-256-GCM (confidentiality + integrity), 128-bit tag.

KDF (password): Argon2id (default: m = 128 MiB, t = 3, p = 1; salt 16 B).

Key file: 32 B (alternative mode).

HKDF (key file / domain labels):

HKDF_INFO_AEAD = "SecureStream256Pro AEAD v1"

HKDF_INFO_KCV = "SecureStream256Pro KCV v1"

HKDF_INFO_FILEKEY = "SecureStream256Pro FILEKEY v1"

KCV: early key verification before decryption begins.

Nonce: unique per file (96-bit, GCM).

Header: [magic/version], salt, KDF parameters, nonce, optional metadata.

Metadata and Privacy

"Hide metadata" mode (optional): the name/extension of the original file can be hidden in the ciphertext (EMETA).

Privacy: the application operates 100% offline; no telemetry. Logs remain local.

Input/Output and Write Consistency

Atomic write: temporary file in the target directory → fsync → atomic os.replace.

Temporary directory: short name (e.g., tmp), excluded from scanning.

Backup (optional): possible creation of a plaintext source copy; use consciously.

Unicode: full character support (emoji, complex scripts); symlinks/junctions skipped.

Limits and Behavior on Windows Systems

MAX_PATH: on systems without "long paths" the full path ≈ 260 characters, single name ≈ 255 characters.

Safe fallback: in extreme cases (legacy systems, very long paths) the application does not abort — it leaves a plaintext copy next to the .enc file and prompts to shorten the path; the .enc ciphertext remains valid.

Execution Parameters (Summary)

Chunk size: configurable (e.g., 1–256 MiB; adjust based on RAM/IO).

Requirements (minimum): Windows 10/11 x64; recommended ≥ 8 GB RAM with default KDF 128 MiB.

Secure overwriting: not implemented (deliberate decision; on SSD/flash it does not provide a guaranteed effect).

Release Integrity

SHA-256 (binary file):

39F59FF3EDEBB2A5D23C898959E8356DCEF00977D925D5A1FEEF0D2DAAD383C7 SecureStream 256 Pro EN.exe

„How to Verify”: PowerShell: **(Get-FileHash -Algorithm SHA256 'path\SecureStream 256 Pro EN.exe').Hash**