

# SecureStream 256 Pro – Podręcznik użytkownika

## Wersja 2.3 (Stable Release)

SecureStream 256 Pro to aplikacja do bezpiecznego szyfrowania i deszyfrowania plików, wykorzystująca AEAD AES-256-GCM (poufność i integralność), Argon2id (KDF), HKDF (wyprowadzanie i domenowanie kluczy) oraz HMAC/KCV (wczesna weryfikacja klucza). Program obsługuje duże pliki dzięki chunkowaniu (rozmiar chunka zapisywany w pliku), tryb ukrywania metadanych, a także bezpieczne I/O z zapisem atomowym. Format v2: nagłówek ENCV2, strumień SGCM2 i stopka SGCM2F (globalna weryfikacja integralności).

## Szybki start

- 1 Uruchom aplikację i wskaż folder z plikami.
- 2 Wybierz metodę uwierzytelniania: hasło lub plik klucza (.key, 32B).
- 3 Opcjonalnie ustaw filtry rozszerzeń, backup oraz ukrywanie metadanych.
- 4 W razie potrzeby dostosuj parametry Argon2id oraz rozmiar chunku.
- 5 Kliknij Szyfruj lub Odszyfruj i obserwuj postęp.

## Hasło a plik klucza (.key)

Hasło – wygodne, elastyczne; siła zależy od jakości hasła.

Zalecane: minimum 12–16 znaków, zróżnicowany zestaw znaków.

Plik klucza (.key, 32 bajty) – najwyższe bezpieczeństwo, niezależne od siły hasła; wymaga bezpiecznego przechowywania kopii klucza najlepiej offline.

## Ukrywanie metadanych

Opcja Ukryj metadane usuwa z nagłówka nazwę i rozszerzenie pliku.

Oryginalne dane nazwa i rozszerzenie są zaszyfrowane w strumieniu i odsłaniają się po deszyfrowaniu. Zwiększa to prywatność, kosztem utrudnionego filtrowania po rozszerzeniach przy szyfrowaniu

## Backup

Włączenie Backup tworzy kopie: przy szyfrowaniu — kopia pliku jawnego w podfolderze backup; przy deszyfrowaniu — kopia pliku .enc. Folder backup jest automatycznie wyłączony z dalszego przetwarzania.

## Prywatność i sieć — brak telemetrii (100% offline)

SecureStream 256 Pro działa w trybie całkowicie offline. Program nie inicjuje połączeń wychodzących i nie gromadzi danych telemetrycznych; wszelkie logi pozostają wyłącznie lokalnie.

## Rozmiar chunku – jak dobrać ustawienia

Chunkowanie określa wielkość porcji danych przetwarzanych w jednym kroku.

Większy chunk zwykle poprawia przepustowość na szybkich nośnikach (SSD/NVMe) i dużych plikach, ale zwiększa chwilowe zużycie pamięci i może pogarszać responsywność systemu na słabszych maszynach. Domyślnie ustawiono 8 MiB jako rozsądny kompromis.

wybrany rozmiar chunku jest zapisywany w pliku; podczas deszyfrowania używana jest wartość z pliku (ustawienie uruchomieniowe jest ignorowane)

Chunk(MiB)	Zastosowanie	Zalety	Uwagi
1–2	Stare HDD, mało RAM, małe pliki, obciążone systemy.	Niskie zużycie RAM, dobra responsywność.	Najniższa przepustowość; więcej operacji I/O
4	Uniwersalne dla mieszanych zbiorów plików.	Balans I/O i RAM	Wolniejsze od 8–16 MiB na SSD
8 (domyślny)	SSD/SATA i większość scenariuszy.	Dobry kompromis wydajność/RAM	Wystarczające dla plików do kilkudziesięciu GB
16	Szybsze SSD/NVMe, większe pliki wideo, archiwa.	Wyższa przepustowość	Nieco większe użycie RAM
32–64	NVMe, bardzo duże pliki, lokalny dysk.	Maksymalizacja throughputu	Może obniżyć responsywność na słabszych CPU/RAM
128–256	Serwery, bardzo szybkie macierze/NVMe	Najwyższa przepustowość	Wysokie użycie RAM; rzadko potrzebne na desktopach

## Parametry KDF (Argon2id)

Argon2id odpowiada za koszt obliczeniowy wyprowadzenia klucza z hasła.

Wyższe wartości zwiększają odporność na ataki słownikowe/kart graficznych, ale wydłużają czas przetwarzania. W SecureStream 256 Pro domyślne ustawienia to  $t=5$ ,  $m=262144$  KiB (256 MiB),  $p=6$ .

Dopuszczalne zakresy:  $t$  1–10,  $m$  32768–1048576 KiB (32 MiB–1GiB),  $p$  1–16.

Parametr	Opis	Domyślne	Zakres	Wpływ/uwagi
$t$ (timecost)	Liczba iteracji; rośnie czas obliczeń	5	1-10	Wyższy=wolniej, bezpieczniej
$m$ (memory KiB)	Pamięć RAM użyta przez KDF	262144	32768–1048576	Wyższy =wolniej, trudniej atakować równolegle
$p$ (parallelism)	Równoległe wątki KDF	6	1-16	Dopasuj do liczby rdzeni; zbyt wysoki „p” może nieprzyspieszyć

## Rekomendacje ustawień Argon2id

Scenariusz	Ustawienia (t/m/p)	Komentarz
Laptop/desktop (typowe)	3 / 131072 / 4	Dobre bezpieczeństwo bez zauważalnego spowolnienia
Wysokie bezpieczeństwo	4–6 / 262144–524288 / 4–8	Zwiększony koszt pamięci i czasu; sprawdź dostępny RAM
Słabszy sprzęt	2 / 65536 / 2–4	Szybciej kosztem mniejszej odporności
Serwer/WS	3–6 / 262144–1048576 / 8–16	Wykorzystaj wielordzeniowość i większą pamięć

## Komunikaty i rozwiązywanie problemów

Komunikaty/objaw	Działanie
Nieprawidłowe hasło/klucz (KCV) dla pliku:	Klucz nie zgadza się z nagłówkiem; sprawdź hasło/plik klucza; upewnij się, że to właściwy plik .key.
Nagłówek uszkodzony – długości name/ext wykraczają poza plik.	Plik .enc jest uszkodzony lub zmodyfikowany; spróbuj z kopią z backupu.
Wysokie użycie RAM	Zmniejsz m (np. do 65536–131072 KiB) lub chunk; zamknij inne aplikacje.

## Parametry i opcje – podsumowanie

Opcje	Opis	Wartość domyślna / Zakres
Tryb uwierzytelniania	Hasło lub 32-bajtowy plik klucza (.key)	Hasło (jeśli brak .key)
Ukryj metadane	Nie zapisuje nazwy/rozszerzenia w nagłówku; dane zapisane wewnątrz strumienia	Wyłączone
Backup	Tworzy kopie: jawne przy szyfrowaniu, .enc przy deszyfrowaniu	Wyłączone
Filtry rozszerzeń	Przetwarzaj tylko wskazane typy (np. .pdf .jpg)	Ręcznie włączane
Chunk (MiB)	Wielkość porcji danych w I/O/AEAD	8 MiB (1–256 MiB)
Argon2id t/m/p	Koszt czasowy, pamięć (KiB), równoległość	5 / 262144 / 6 (t:1–10 m:32768–1048576 p:1–16)

## Rekomendacje bezpieczeństwa dla użytkowników

**Hasła i klucze** – wybieraj silne hasła (minimum 12–16 znaków, zróżnicowane typy znaków) i przechowuj je w menedżerze haseł.

**Pliki kluczy** – nie przechowuj plików .key w tym samym katalogu co zaszyfrowane dane. Trzymaj je na oddzielnym, bezpiecznym nośniku.

**Kopie zapasowe** – regularnie wykonuj kopie zapasowe zaszyfrowanych plików i kluczy. Przechowuj backup w innym, bezpiecznym miejscu.

**Środowisko pracy** – korzystaj z programu wyłącznie na urządzeniach z aktualnym systemem i oprogramowaniem zabezpieczającym (antywirus, firewall).

**Poufność** – nie udostępniaj haseł ani kluczy osobom trzecim. Pamiętaj, że ich kompromitacja oznacza utratę bezpieczeństwa danych

## Informacja prawna

Oprogramowanie SecureStream 256 Pro zostało opracowane z najwyższą starannością i przetestowane zgodnie z założeniami technicznymi opisanymi w niniejszym dokumencie. Autor dokłada wszelkich starań, aby zapewnić poprawność działania i bezpieczeństwo rozwiązania, jednak nie może zagwarantować pełnej bezbłędności w każdym scenariuszu użycia. Użytkownik ponosi odpowiedzialność za sposób wykorzystania programu, w szczególności za stosowanie go zgodnie z przeznaczeniem oraz zasadami bezpieczeństwa opisanymi w dokumentacji.

Aplikacja działa w 100% offline i nie gromadzi telemetry. Wersja portable przeznaczona jest do użytku własnego (bez rozpowszechniania); szczegóły znajdują się w EULA