

# Slajd 1 - Szyfrowanie deskryptorów

## Notatka do powiedzenia - bez czytania treści ze slajdu

Każdy deskryptor ma tylko 16 bajtów, dlatego zabezpieczamy go przy użyciu AES-256-GCM. Sam deskryptor jest szyfrowany, natomiast nagłówek pozostaje jawny, aby odbiorca mógł odczytać numer sekwencyjny, epokę klucza i typ wiadomości.

Jawny nagłówek nie oznacza jednak, że można go dowolnie zmienić. Jest on przekazywany do AES-GCM jako AAD, czyli dane uwierzytelniane, ale nieszyfrowane. Zmiana numeru sekwencyjnego lub innego pola spowoduje błąd tagu i odrzucenie rekordu.

Nonce ma 96 bitów i nie musi być przesyłany. Tworzymy go z 32-bitowej wartości salt oraz 64-bitowego numeru sekwencyjnego. Najważniejsza zasada jest taka, że dla jednego klucza ta sama wartość nonce nie może pojawić się ponownie.

**Najważniejsze zdanie:** Nagłówek jest widoczny, lecz chroniony; deskryptor pozostaje poufny.

**Przejdźcie do kolejnego slajdu:** „Przy częstych deskryptorach problemem staje się jednak narzut generowany przez osobny tag dla każdej wartości.”

## Slajd 2 - Grupowanie deskryptorów

### Notatka do powiedzenia - bez czytania treści ze slajdu

Pojedynczy deskryptor ma 16 bajtów, a pełny tag GCM również ma 16 bajtów. Szyfrowanie każdej wartości osobno oznacza więc duży narzut w stosunku do ilości właściwych danych.

Rozwiązaniem jest grupowanie kilku deskryptorów w jeden rekord. Wtedy wiele wartości korzysta ze wspólnego nagłówka i jednego tagu. Zmniejszamy liczbę operacji kryptograficznych oraz lepiej wykorzystujemy pasmo.

Stosujemy dwa tryby. Wiadomości krytyczne wysyłamy pojedynczo, aby uzyskać minimalne opóźnienie. Telemetrię możemy grupować po 8-32 deskryptory albo wysyłać po upływie 1-5 milisekund, zależnie od tego, co nastąpi wcześniej.

**Najważniejsze zdanie:** Większa grupa oznacza mniejszy narzut, ale wymaga krótkiego oczekiwania na zebranie danych.

**Przejdźcie do kolejnego slajdu:** „Ta sama zasada agregacji może zostać zastosowana do pakietów strumienia MPEG-TS.”

## Slajd 3 - Szyfrowanie strumienia .ts

### Notatka do powiedzenia - bez czytania treści ze slajdu

Pakiet MPEG-TS ma stałą długość 188 bajtów. Szyfrowanie każdego pakietu osobno byłoby nieefektywne, ponieważ do każdego 188 bajtów należałoby dodać nagłówek rekordu i 16-bajtowy tag GCM.

Dlatego pakiety są agregowane w niezależne rekordy. W wybranym wariantcie jeden rekord zawiera 16 pakietów TS, czyli 3008 bajtów danych. Do tego dochodzi 24-bajtowy nagłówek oraz 16-bajtowy tag, co daje łącznie 40 bajtów narzutu i rekord o rozmiarze 3048 bajtów.

Nagłówek zawiera między innymi epokę klucza, numer rekordu, identyfikator strumienia i długość payloadu. Jest chroniony jako AAD, a właściwe pakiety TS są szyfrowane. Każdy rekord jest niezależny, więc utrata jednego bloku nie uniemożliwia odszyfrowania kolejnych.

**Najważniejsze zdanie:** Dla 16 pakietów narzut kryptograficzny wynosi tylko około 1,33%.

**Przejdźcie do kolejnego slajdu:** „Liczba pakietów w rekordzie jest kompromisem pomiędzy narzutem a opóźnieniem.”

## Slajd 4 - Porównanie wariantów grupowania TS

### Notatka do powiedzenia - bez czytania treści ze slajdu

Narzut jednego rekordu jest stały i wynosi 40 bajtów. Im więcej pakietów umieścimy w rekordzie, tym mniejszy jest więc jego udział procentowy.

Dla 4 pakietów narzut wynosi 5,32 procent, ale rekord powstaje już po około 5,5 milisekundy. Dla 32 pakietów narzut spada do 0,66 procent, lecz czas oczekiwania rośnie do około 44 milisekund.

Wariant 16-pakietowy jest rozsądnym kompromisem: daje 1,33 procent narzutu i około 22 milisekundy czasu zbierania przy średnim bitrate 1,087 megabita na sekundę. Ten czas oznacza oczekiwanie na zgromadzenie danych, a nie czas wykonywania AES-GCM - samo szyfrowanie takiego bloku jest znacznie krótsze.

Ostateczna liczba pakietów może być dobierana dynamicznie. Dla komunikacji wymagającej bardzo małego opóźnienia wybieramy mniejsze grupy, a dla transmisji nastawionej na efektywność - większe.

**Najważniejsze zdanie:** Rekomendowany punkt startowy: 16 pakietów TS na jeden rekord AES-GCM.