

# MoQ Secure Objects

End to End Symmetric Encryption and Authentication Scheme

IETF 119  
March 2024

Cullen Jennings  
Suhas Nandakumar

# Goals

This is not a replacement for Common Encryption (cenc) in CMAF, it is an alternative for use with things such as LOC or where “cenc” schemes cannot be used.

Minimize Bandwidth for MoQ Objects (such as audio)

Not new crypto, simply uses HKDF and AEAD Schemes

RFC 5116 defines an API for symmetric encryption such as AES-GCM

Easy integration with Key Establishment schemes (MLS and others)

Easy Integration with container formats (such as LOC)

Transparent to MoQT and Relays

# AEAD Crypto

Prerequisites: A set of keys per track identified by a key ID, and the cipher suite that key uses (could come from MLS)

Object\_key and object\_salt are derived from the FullTrackName, Key, KeyID, cipher suite using HKDF. If the key is changed, it gets a new keyID.

Nonce is formed from concatenation of GroupID and ObjectID xor'd with salt.  
Nonce is unique for this object\_key as GroupID/ObjectID is unique for Track.

The extra authenticated data includes Key ID, Group ID, and Object ID. Relay can not change these.



# Why focus on low bandwidth

Lyria is a 3kbps audio codec. Newer ML codecs are use even less bandwidth.

A 1.9 kbps codec with 50 ms packets would use 12 bytes per packet.

With a 1 byte key ID and 80 bit auth tag, crypto will add 11 bytes.