

# Secure Objects

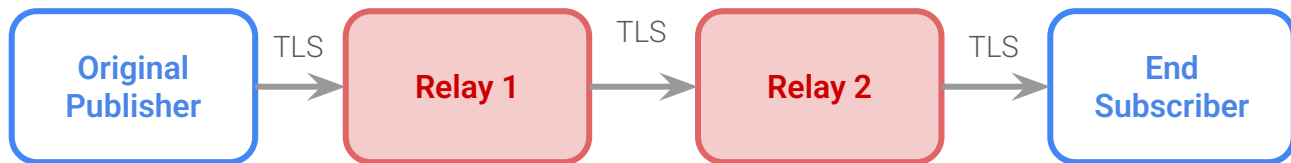
End-to-End Encryption for Media over QUIC  
draft-ietf-moq-secure-objects-00

**IETF 125**

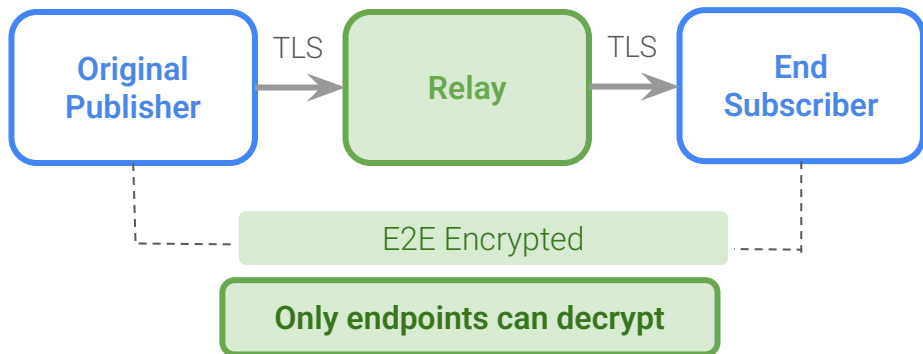
**Authors:** Cullen Jennings, Suhas Nandakumar, Richard Barnes

# What is Secure Objects ?

## THE CHALLENGE: Relays Can Read Your Data



## The Solution: End to End Encryption



## Security Goals

- Relays route, not read - content is encrypted end to end
- Integrity and Authenticity - Subscribers verify content is unmodified
- Selective Protection - Some metadata readable, some encrypted

# Security Protection Levels

---

## HBH ONLY ( Relay can modify)

Track Alias,, Mutable Properties

## E2E AUTHENTICATED (Relay can read, not modify)

Group ID, Object ID, Immutable Properties,  
Track Namespace/Name, KeyID

## E2E ENCRYPTED + AUTHENTICATED

Object Payload, Encrypted Properties

## Relay Visibility Matrix

Field	Read	Modify
Mutable Properties	YES	YES
Immutable Properties	YES	NO
Encrypted Payload	NO	NO

# Issues Closed

---

#	Issue Title
60	Diagram accuracy issues
53	Latency implications
51	Some editorials on draft -03
50	Define how to detect lost/missing objects
48	Define SCOPE for Key ID
47	Invocation limits for AEAD algorithm

#	Issue Title
46	HKDF label for secure objects
45	Improve serialization description
44	Is 'name' the right term
38	MTI/recommended cipher suites table
37	Add note about applications

**Key Additions:** AEAD Limits, deletion detection, Key ID scoping, cipher suite recommendations, editorial clarification

# Open Issues Summary

---

Issue	Topic	Status
#61	Private Ext. Registration	<a href="#">PR Merged</a>
#59	AAD Redundancy	Update KID scope and add clarification
#58	Varint Encoding	Discuss encoding options
#49	Security Properties	Document threat model
LOC#9	Track Property Auth	<b>Add Track Properties handling</b>

# Issue #59: How much AAD is Necessary ?

Several AAD fields appear redundant - can we reduce overhead?

```
SECURE_OBJECT_AAD {  
  Key ID (i),  
  Group ID (i),  
  Object ID (i),  
  Track Namespace (...)  
  Track Name (...),  
  Immutable Props (...)  
}
```

This is wrong, but how we got here is:

- Key ID, Group ID, Object ID was to match the SFrame security design of using KID, CTR for AAD
- Immutable Properties are included to validate they were not modified.
- Track Namespace & Track Name to resist replay across tracks by the relay.

Current draft has some mistakes around scope of KeyID.  
Proposed fix is on the next slide.

# Issue #59: How much AAD is Necessary ?

---

## Proposed Solution

```
SECURE_OBJECT_AAD {  
  Track Name (..),  
  Immutable Props (..)  
  Group ID (i),  
  Object ID (i),  
}
```

- Key ID is in Immutable Properties, Propose, remove duplicate Key ID
- Remove Track Namespace as it is included as input to Key derivation (HKDF)
  - Open issue if we should do or not
- TrackName is not part of input to key derivation (HKDF) and thus it is needed for integrity protection, via the AAD.
  - Stops relay from copying object on one track to another in same namespace

# Issue #58: Varint Encoding Ambiguity

**MOQT allows multiple varints encodings for the same value - breaks AAD construction**

```
// Value: 42 can be encoded
multiple ways

Encoding 1: [0x2A] // 1 byte
Encoding 2: [0x40, 0x2A] // 2 bytes
Encoding 3: [0x80, 0x00, 0x00,
0x2A] // 4 bytes

// All represent 42 - but different
bytes!
```

## Proposed Solution #1: Fixed 64-bit Integers

Pros: Ambiguous, Cons: More bytes on wire

## Proposed Solution #2: Mandatory Minimal Encoding

moq-transport #1517 ( Change SHOULD to MUST: "MUST be encoded using least number of bytes")

Pros: Minimal Overhead

# Issue #49: Security Properties Documentation

---

**Be explicit about what security properties this spec achieves ?**

## **Proposal to add the following details:**

- Define overall threat model - what can compromised relays do?
- Fanout forgery attacks - relay sends different forgeries to different subscribers
- Duplicate key/namespace/track/group/object ID attacks
- Deletion detection limitations
- Group/Object ID range limits

# Issue LOC#9: Track Properties can't be Authenticated/Encrypted

## Track properties appear only in control message - authentication gap

- **Option #1:** Don't provide end to end security for track properties
  - Applications will just add properties that need end to end security as object properties to first object of the group.
- **Option #2:** Provide authentication only for track properties when an object is received.
- **Option #3:** Provide authentication + encryption for track properties when an object is received.
- **Option #4:** Provide a separate End to End Encryption / Protection for track properties in control messages.

# Issue LOC#9: Track Properties can't be Authenticated/Encrypted

## Option #2 Authentication Only

```
SECURE_OBJECT_AAD {  
  Key ID (i),  
  Group ID (i),  
  Object ID (i),  
  Track Namespace (..),  
  Track Name (..),  
  Serialized Imm Object Props (..),  
  Serialized Imm Track Props (..) // NEW!  
}
```

- Publishers include immutable track props in control messages.
- If relay modifies → AAD mismatch on object arrival → DECRYPTION FAILS
- Only detects if control message was tampered when the data object arrives

## Option #3 Encryption + Authn in Objects

```
Encrypted Track Properties {  
  Type (0xB),  
  Length (i),  
  Key-Value-Pair (..) ...  
}
```

### Conveyed inside:

- Encrypted Properties List of objects
- E.g., video codec config, audio params
- Relays CANNOT read these
- very close to option 1

# Encrypted Track Properties (example)

---

## Group X

### First Object

Encrypted Properties List

Media Payload

### Subsequent Objects

Media Payload

First Object of every group must include encrypted track properties

Configuration changes take effect at group boundaries

Late joiners obtain encrypted properties at group boundaries

## Option 4: Private Track Properties in Control Messages

---

```
PRIVATE_PROPERTIES {  
  Nonce (8),  
  Encrypted Properties (..),  
  Authentication Tag (..)  
}  
  
// In PUBLISH/SUBSCRIBE_OK  
messages
```

Define additional mechanism to encrypt track properties end to end in control messages.

Mechanism need to address following:

- Lack of crypto binding
  - Control messages are not bound to objects through AEAD - replay/substitution attacks possible
- Nonce management Complexity
  - Separate nonce space is needed, not tied to Group or Object ID. Request ID is hop by hop and not in responses.
- Requires MoQT Spec updates