

MoQ Secure Objects

IETF MOQ Interim
Boulder
Feb 9 to 10

Cullen Jennings

V2

Open Issue 54: add a private header extension for pad to N byte boundary

This can improve privacy. By padding all traffic up to some predefined sizes (often powers of 2) it makes is harder to fingerprint the what application created the traffic or what data it is sending.

Proposal: Define a private header extension that allows padding to byte boundary. This is easy to add now or later.

Issue #44 :- “Name” might not be right term for Full Object ID

PR #55 renames Object Name to Full Object ID ,

Where “Full Object ID” is combination of Full Track Name,
Group ID and Object ID

Issue #50 Define how to detect deleted objects.

Malicious relays could remove objects and groups. Some applications may wish to detect that. Some may not or may be able to detect based on internal structure of the data in the object outside the scope of this spec. However, this spec does provide a mechanism application can use to detect deletion by relay.

Typically applications increment groupid and objectid monotonically. Detecting loss in such case is straightforward.

For applications that use groupid and objectid that can have gaps, its mandated to include Group ID and Object ID gap extensions as Immutable extensions. If object gap extension is missing in a secure object, it is assumed to be 1. Similarly, for group gap extension.

For applications that need to detect lost object, mandatory to signal end of subgroups, groups, and tracks using object status.

Example:

Group 5:

Sub-group 1: 1, 3(gap=2), 5(gap=2,end of subgroup)

Sub-group 2: 2(gap=2), 4 (gap=2,end of subgroup)

If relay deleted 3, this would be detected on receiving 5.
Since the data used to detect the gap was AEAD protected,
the relay cannot edit the gap in object 5 without detection.

Issue #37 Notes for applications using this

Proposal:

- MUST NOT ever encrypt two objects in the same track with different data. Note: this is not allowed by MoQT.
- Applications that use secure object MUST define what cipher suites are Mandatory To Implement

#38 Do we want to add a table of MTI, recommended, not recommended cipher suites for Sec Object

Proposal:

IANA registry that lists cipher suites as one of:

Y - has IETF Consensus and requires Standard Action

N - Not evaluated

D - Discouraged

#45 Improve description of serialization process of the plain text data

Proposal is to fix the section references and clarify the serialization process

#48 : Define SCOPE for Key ID #48

Lifetime and scope of KeyID is determined by the application.

The application assigns each track a set of (Key ID, track_base_key) tuples, where each track_base_key is known only to authorized original publishers and end subscribers for a given track. How these per-track **secrets and their lifetime** are established is outside the scope of this specification

#47 Invocation limits for AEAD algorithm

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/11/>

Normative reference to aead-limits draft and say publish MUST switch to a new key before exceeding limits as defined in Section 6.2.1 and 7.4 of that draft

#53 Latency implications

Add to usage consideration, secure object need all the data for an object before it can check any of the data is valid. This can cause latency if the application design for object puts too much data in a single object. For example, if 6 seconds of video were put into a single object, none of that video could be used until all 6 seconds were received.

#46 Have HKDF label represent secure objects rather than MOQ in general

Proposal: Include Secure Objects in the Key Label

```
moq_key_label = "MOQ Secure Objects 1.0 Secret key " +  
serialized_full_track_name + cipher_suite + key_id
```

Issue #51 :- Editorial Changes

PR #52 fixes all the suggestions