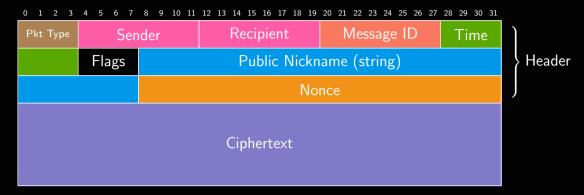
Message Packet (Threema Protocol Layer)



• Only the MSB of Flags is used

Message Packet on the Wire

O 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Length

Threema Client-to-Server Ciphertext

Text Message

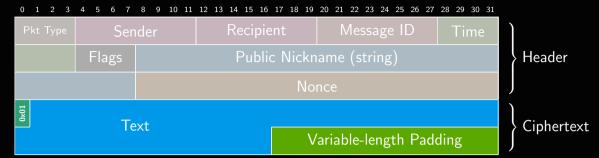
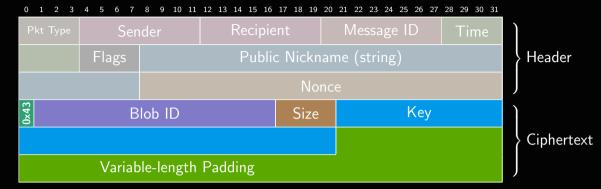
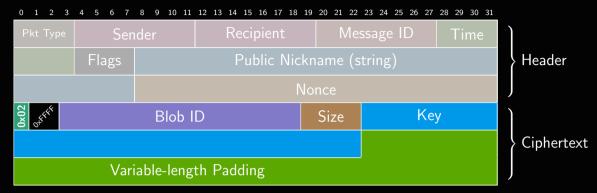


Image Message

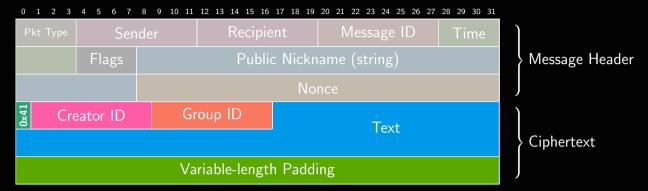


- Blob is symmetrically encrypted using Key and uploaded to asset server.
- Image captions are stored inside the image's EXIF data. These data leak upon creating such an image while the "save media to gallery" option is enabled.

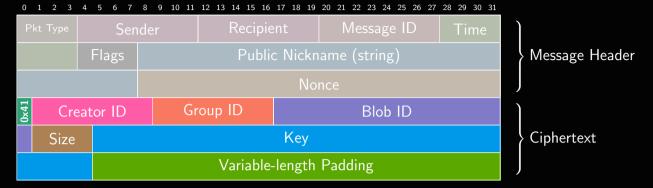
Audio Message



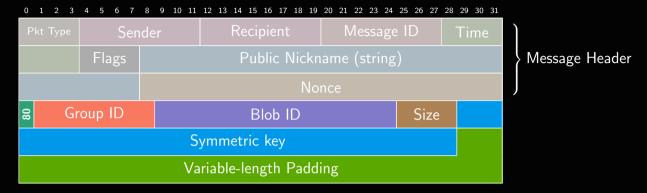
Group Message Packet



Group Image Message



Group Picture Update



Create/Update Group (members)



Acknowledgement Packet to Server

Client-Server Handshake

Client Hello

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Ephemeral Client Public Key

Nonce

Server Hello

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Server Nonce Prefix

Ephemeral Server Public Key

Client Nonce Prefix

Ciphertext

Client Authentication Packet

9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31



Ciphertext

Server Acknowledgement

10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Zeros

Ciphertext