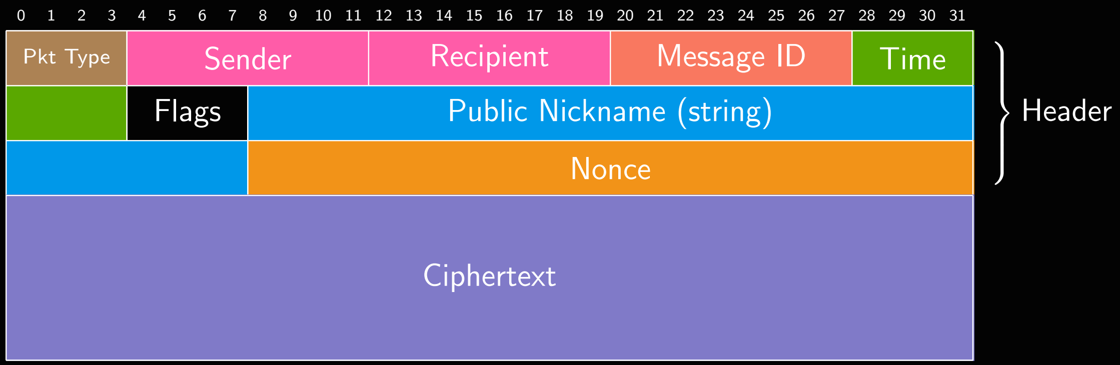
Message Packet (Threema Protocol Layer)



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

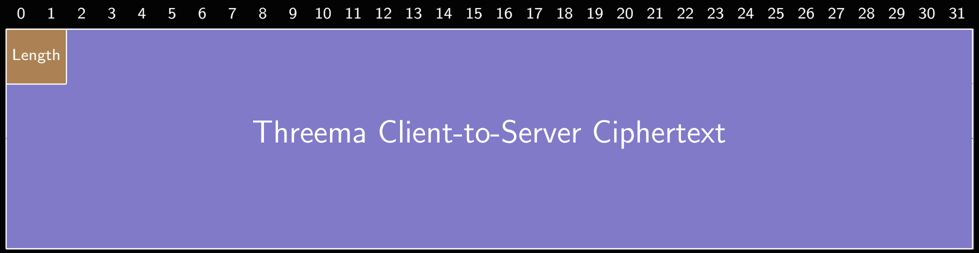
Nonce

Ciphertext

Header

- Only the MSB of *Flags is used*

Message Packet on the Wire

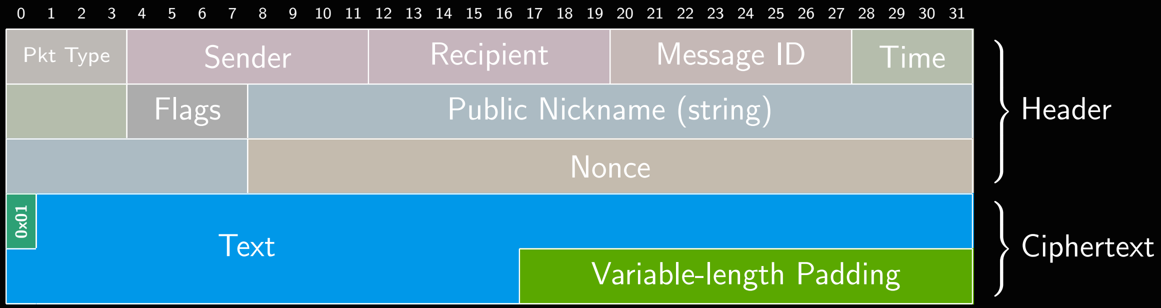


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Length

Threema Client-to-Server Ciphertext

Text Message



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

Header

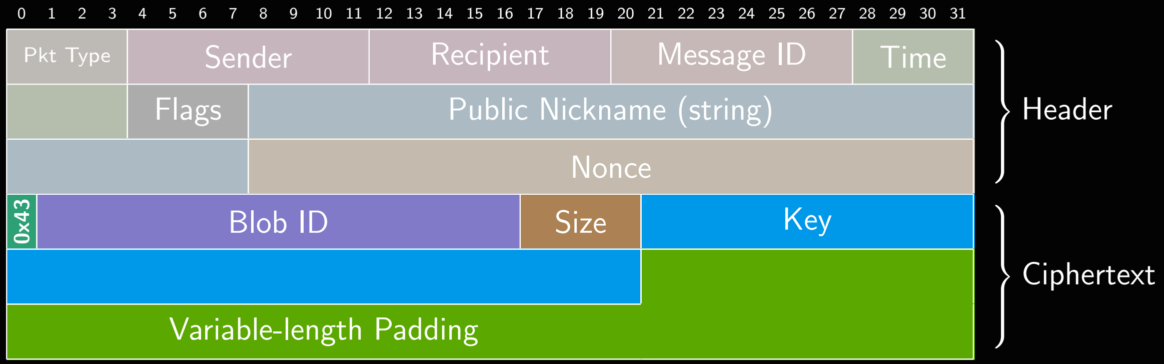
0x01

Text

Variable-length Padding

Ciphertext

Image Message



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

0x43

Blob ID

Size

Key

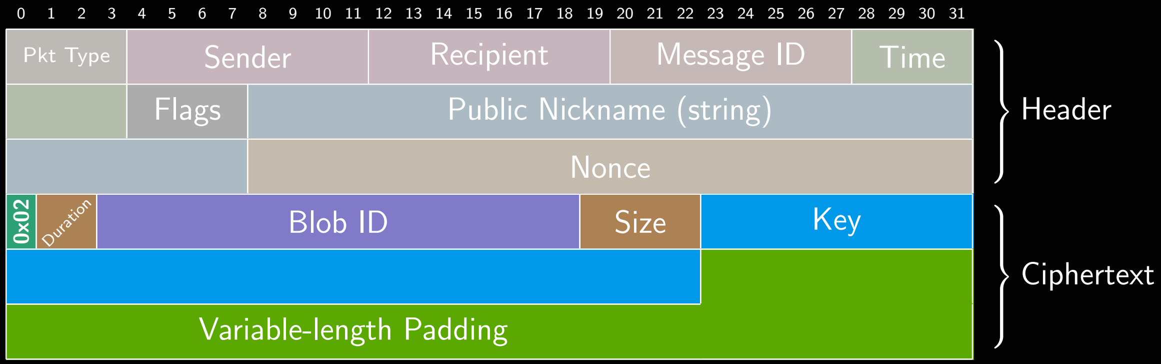
Variable-length Padding

Header

Ciphertext

- 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



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

Header

0x02

Duration

Blob ID

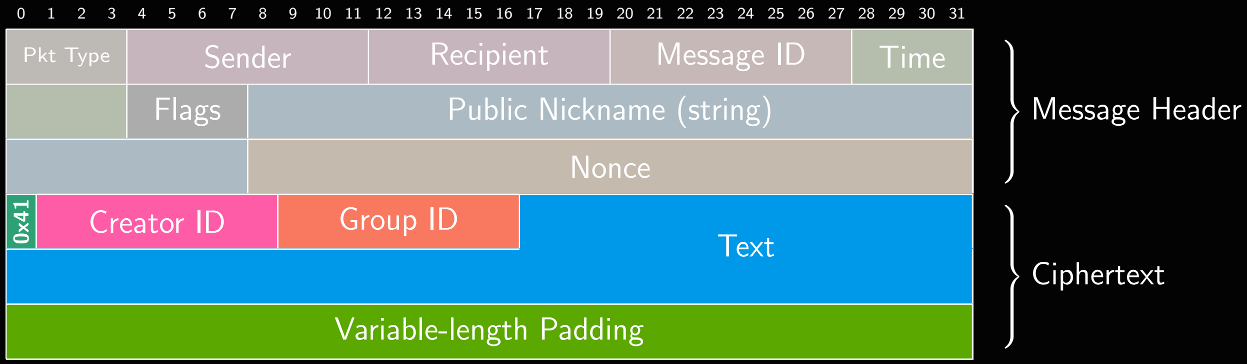
Size

Key

Variable-length Padding

Ciphertext

Group Message Packet



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

0x41

Creator ID

Group ID

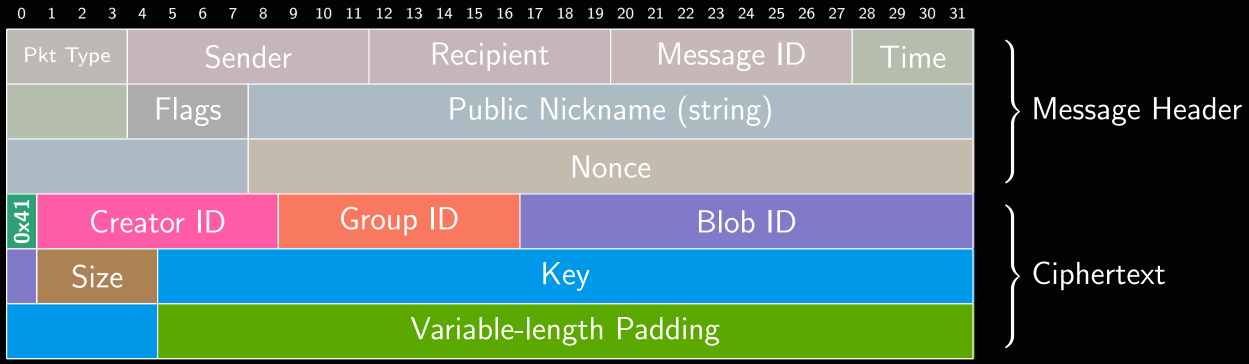
Text

Variable-length Padding

Message Header

Ciphertext

Group Image Message



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

0x41

Creator ID

Group ID

Blob ID

Size

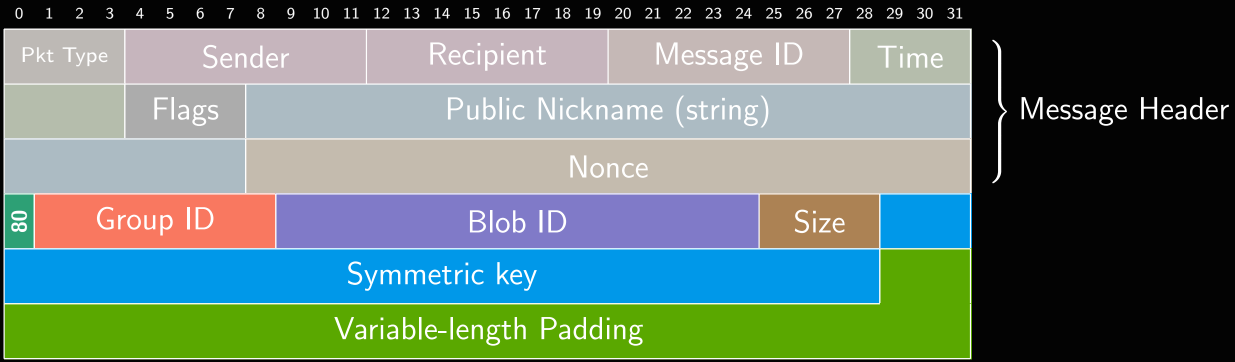
Key

Variable-length Padding

Message Header

Ciphertext

Group Picture Update



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

Message Header

08

Group ID

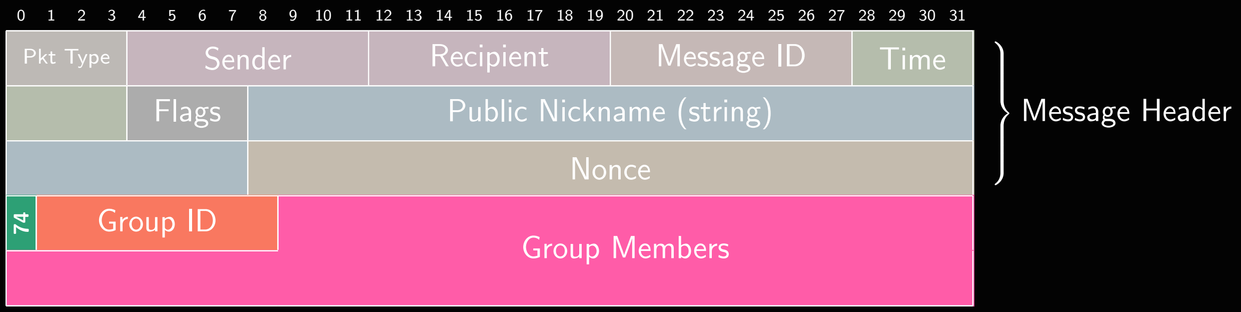
Blob ID

Size

Symmetric key

Variable-length Padding

Create/Update Group (members)



0 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

Pkt Type

Sender

Recipient

Message ID

Time

Flags

Public Nickname (string)

Nonce

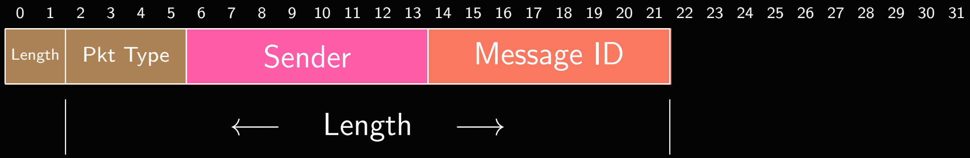
74

Group ID

Group Members

Message Header

Acknowledgement Packet to Server



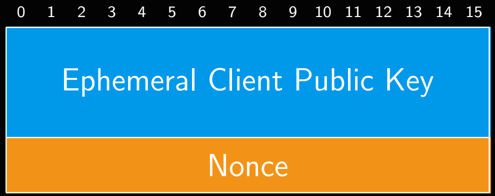
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Length | Pkt Type | Sender | Message ID

⟵ Length ⟶

Client-Server Handshake

Client Hello

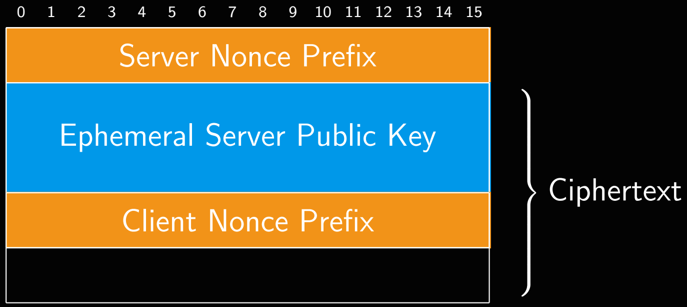


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Ephemeral Client Public Key

Nonce

Server Hello



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

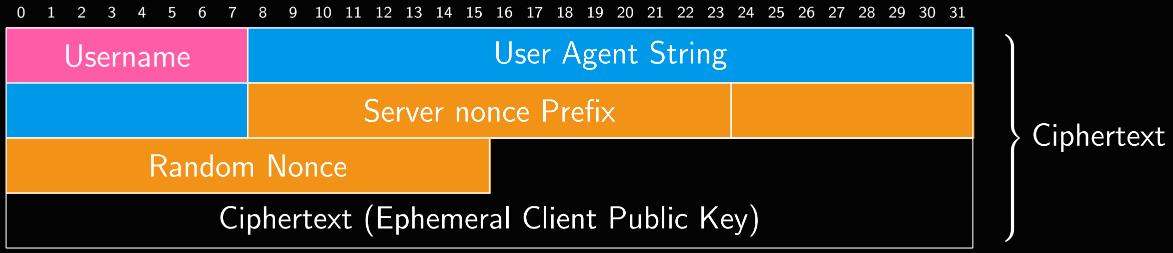
Server Nonce Prefix

Ephemeral Server Public Key

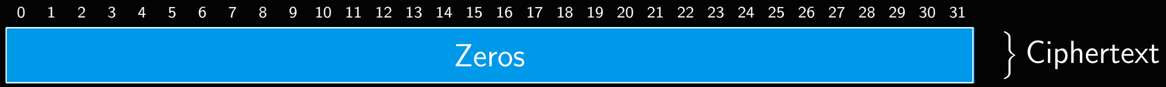
Client Nonce Prefix

Ciphertext

Client Authentication Packet



Server Acknowledgement



PKCS7 Padding

													03	03	03
												04	04	04	04
								08	08	08	08	08	08	08	08
16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
											05	05	05	05	05
										06	06	06	06	06	06