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			

Header

Ciphertext
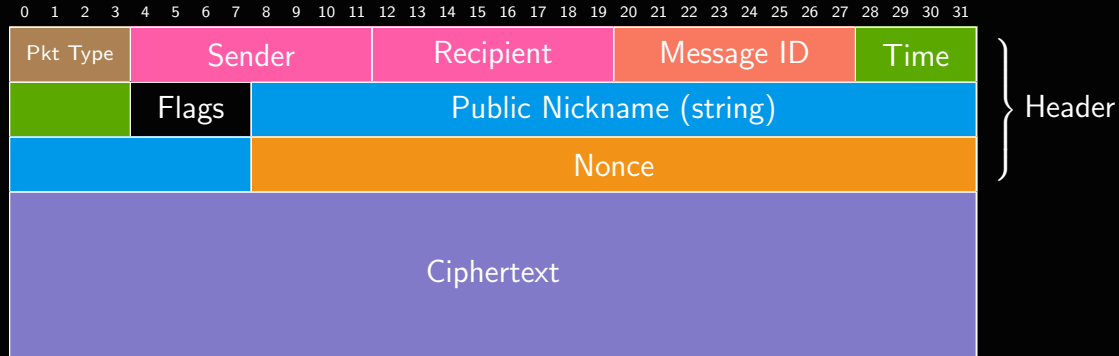
- Only the MSB of *Flags is used*

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

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

⎫
⎬ Header
⎭
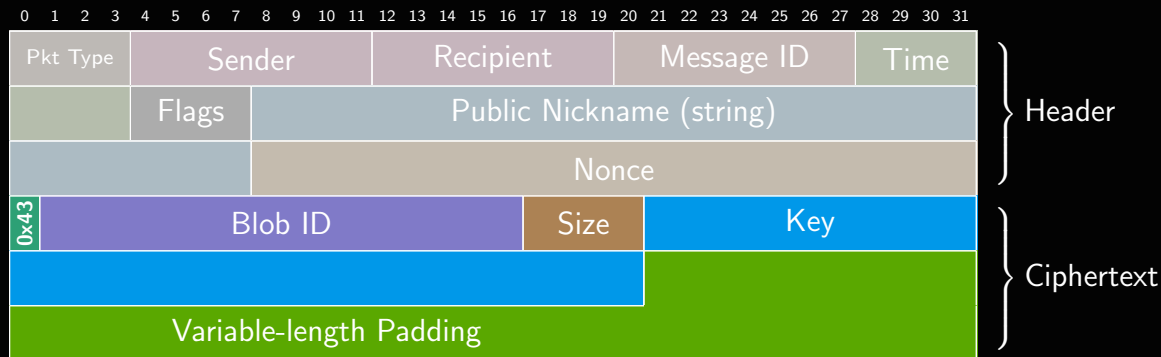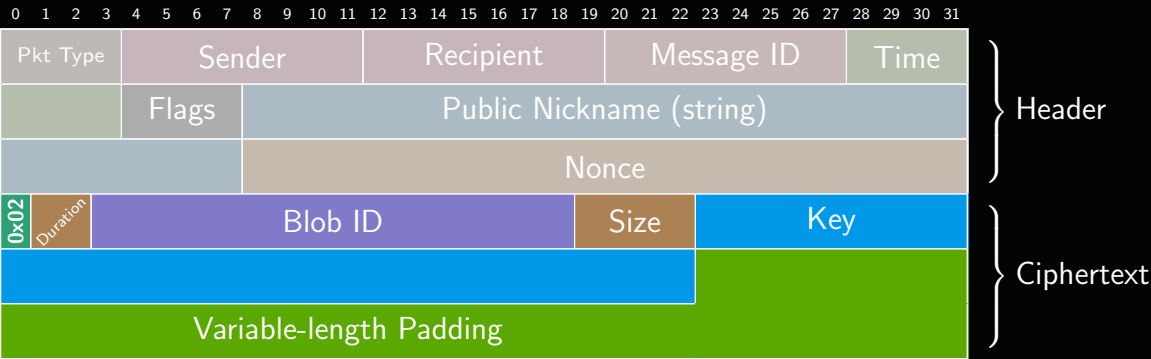
0x43 | Blob ID | Size | Key
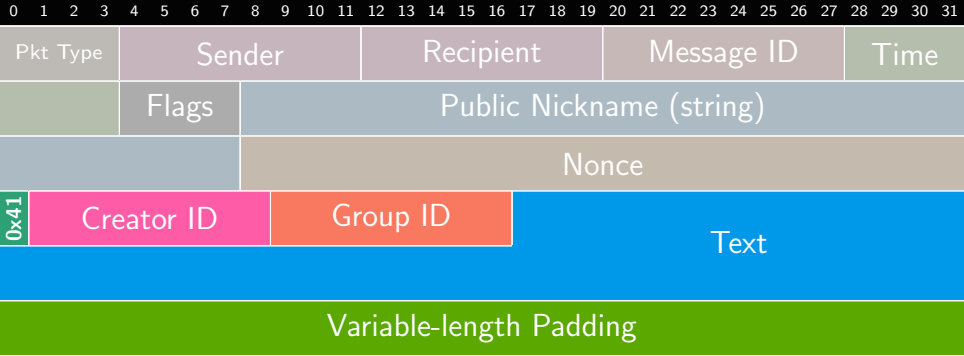Variable-length Padding

⎫
⎬ Ciphertext
⎭
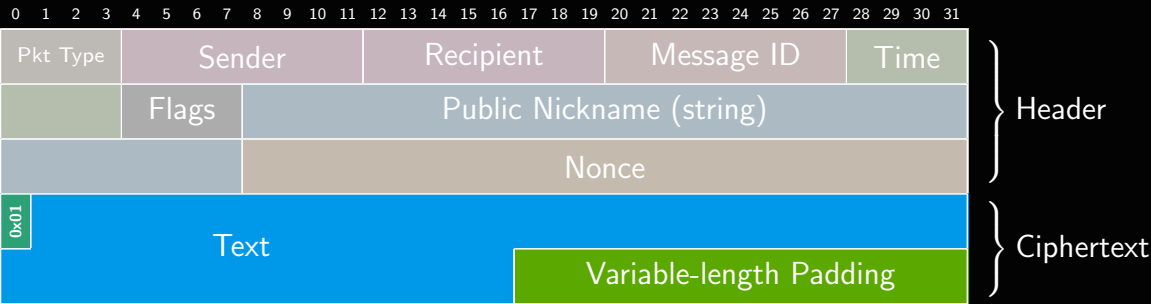
- Blob is symmetrically encrypted using *Key* and uploaded to asset server.

- 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.
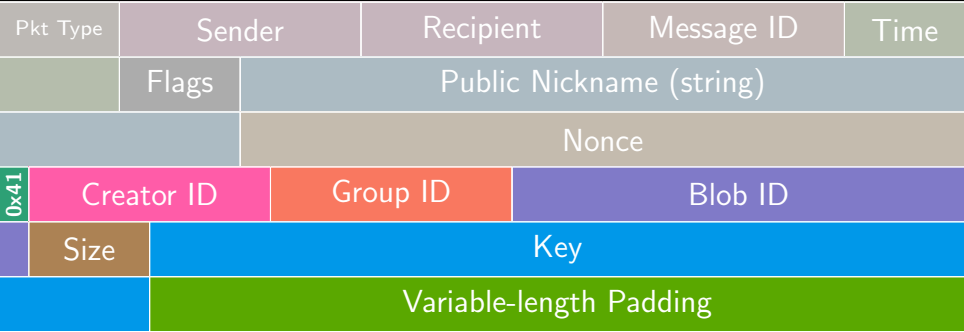
Audio Message

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
			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 — Message Header

0x41 | Creator ID | Group ID | Text — Ciphertext

Variable-length Padding

Group Image Message

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)			⎬ Message Header
		Nonce			⎭
80	Group ID	Blob ID		Size	
Symmetric key					
Variable-length Padding					
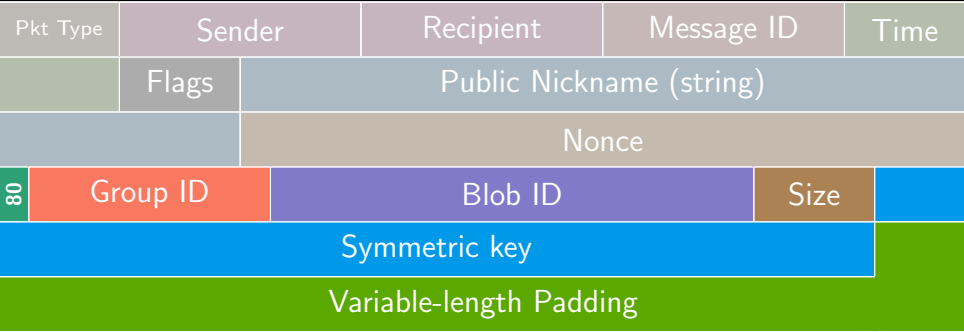
Create/Update Group (members)

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)			⎬ Message Header
		Nonce			⎭
74	Group ID	Group Members			

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

$\longleftarrow$ Length $\longrightarrow$
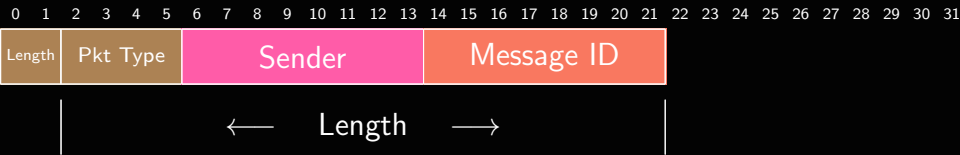
Client-Server Handshake

Client Hello

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

Ephemeral Client Public Key

Client Nonce Prefix

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
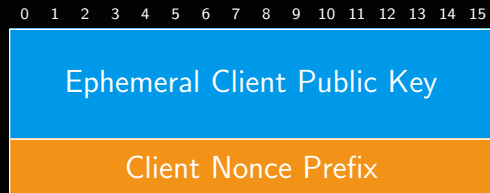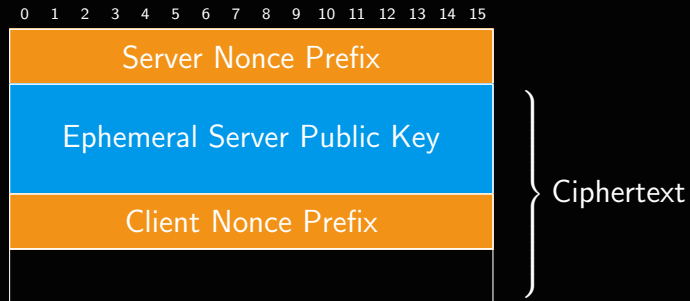
Client Authentication Packet

```
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
```

Threema ID	User Agent String
	Server nonce Prefix	
Random Nonce	
Ciphertext (Ephemeral Client Public Key)	

Ciphertext
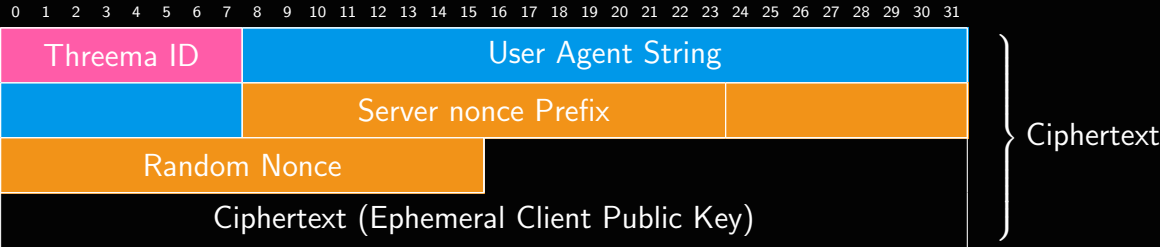
Server Acknowledgement

```
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
```

Zeros

Ciphertext
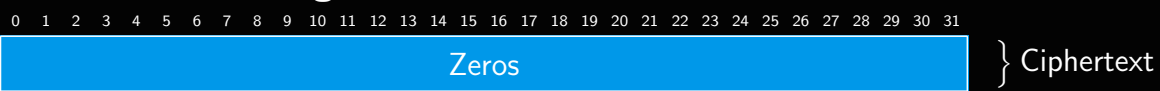
PKCS7 Padding

												03	03	03
											04	04	04	04
						08	08	08	08	08	08	08	08	08
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		

Group Management Message - Add Users

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

0x4A | Group ID

Member IDs

Variable-length Padding

} Ciphertext
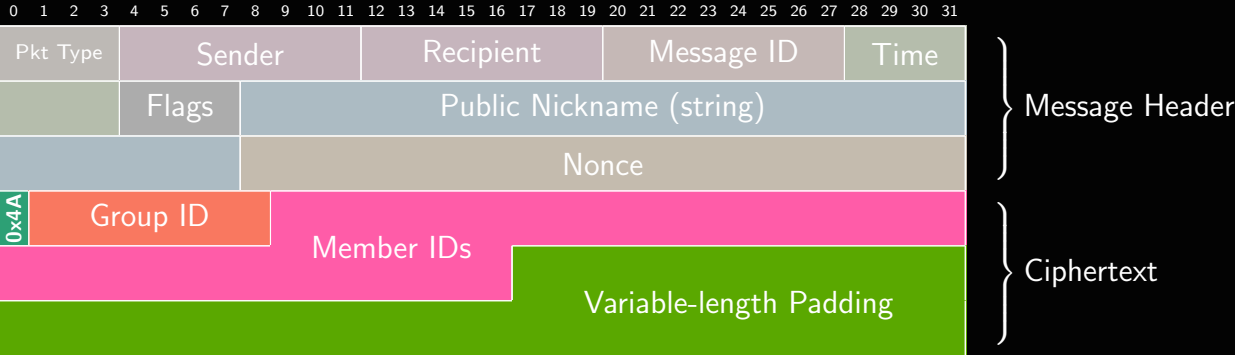
Group Management Message - Rename Group