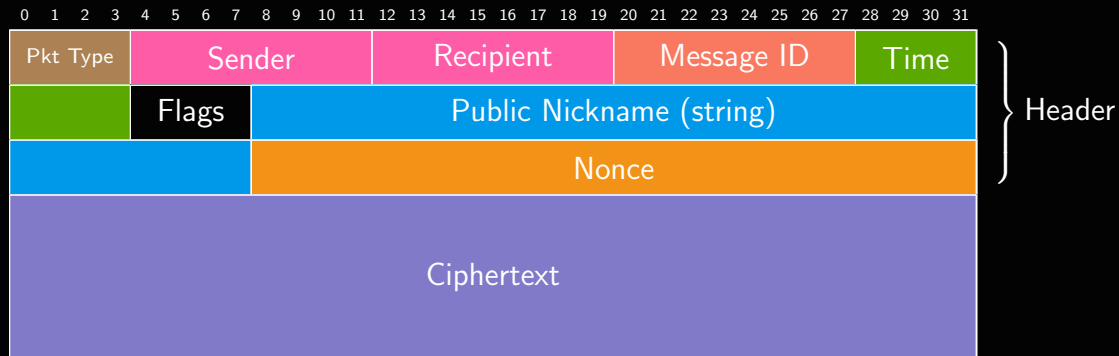


Message Packet (Threema Protocol Layer)



- Only the MSB of *Flags* is used

Message Packet on the Wire



Text Message

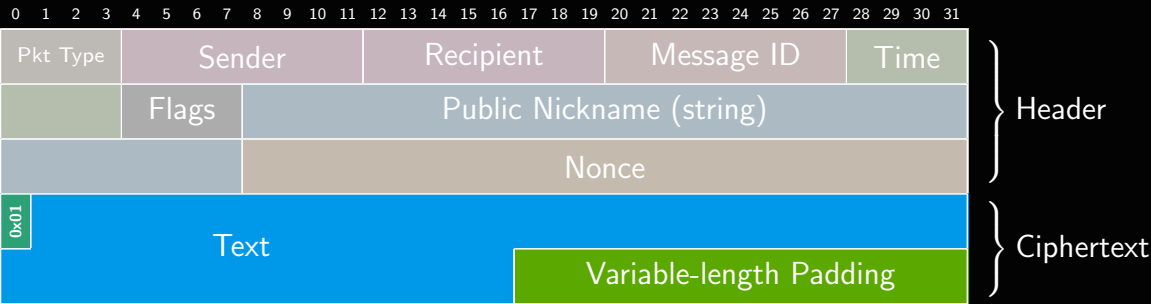
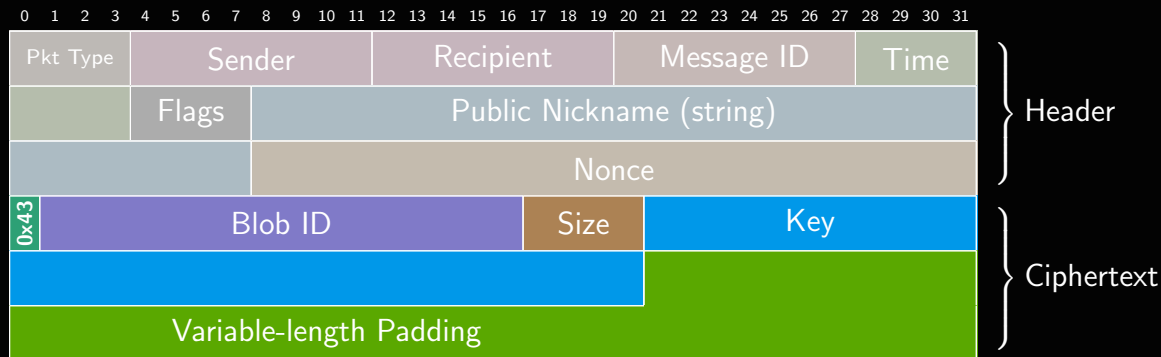
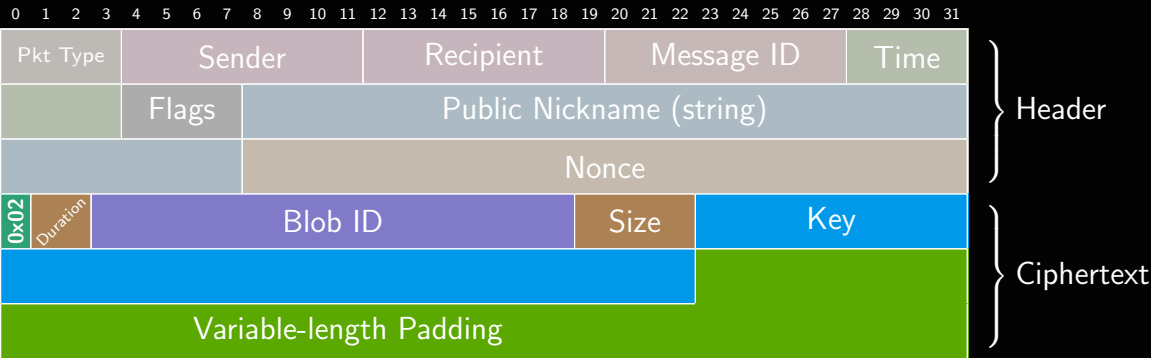


Image Message

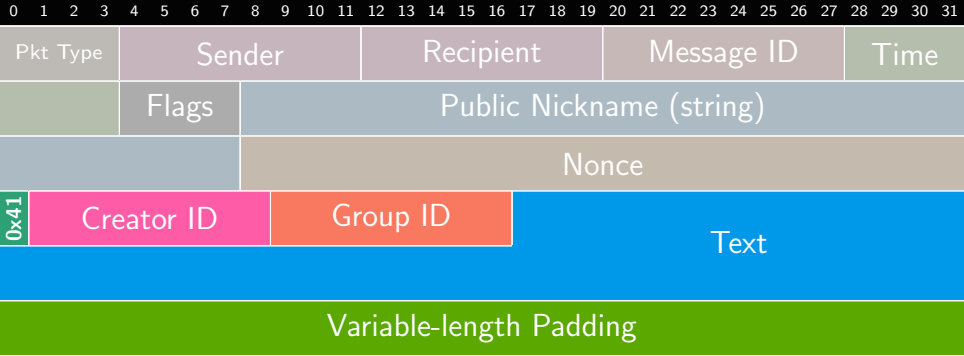


- Blob is symmetrically encrypted using *Key* and uploaded to asset server.
- Image captions are stored inside the image's EXIF data. These data leak upon creating such an image while the “save media to gallery” option is enabled.

Audio Message



Group Message Packet

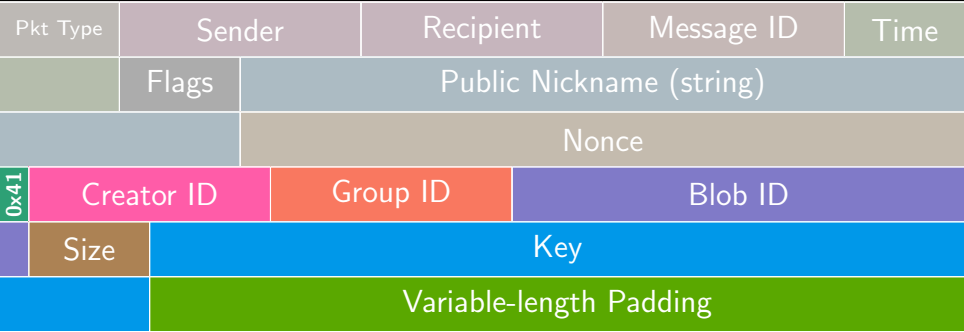


Message Header

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

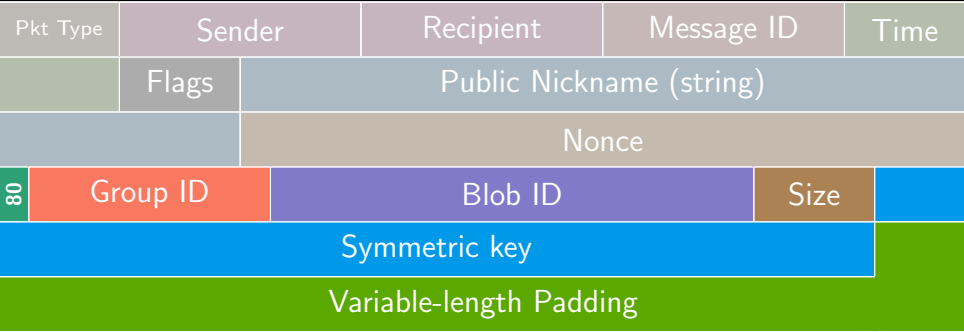


Message Header

Ciphertext

Group Picture Update

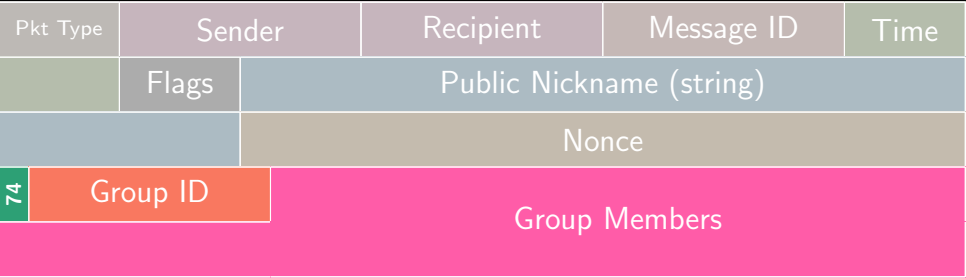
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31



} Message Header

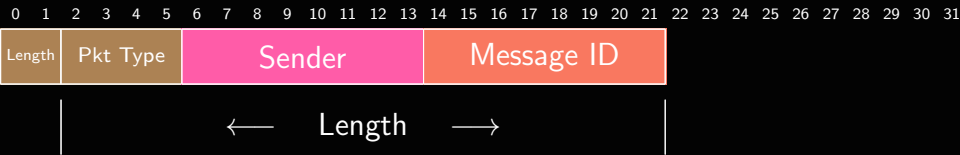
Create/Update Group (members)

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



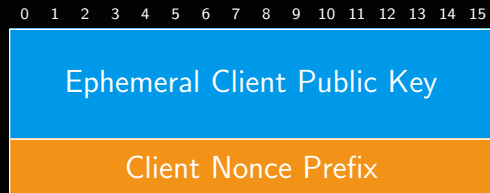
} Message Header

Acknowledgement Packet to Server

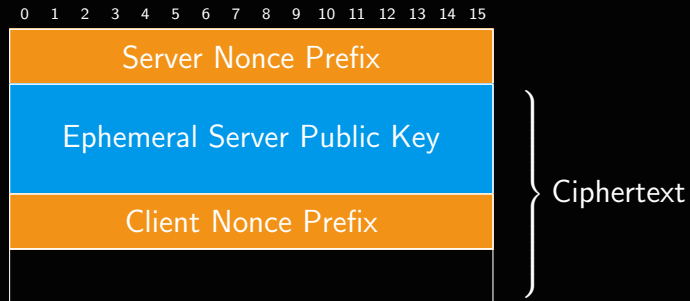


Client-Server Handshake

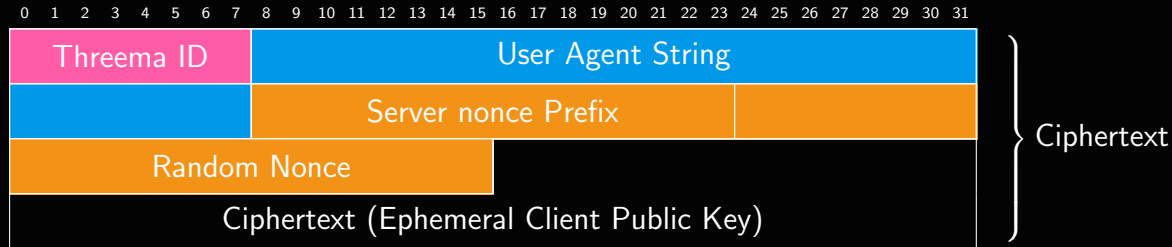
Client Hello



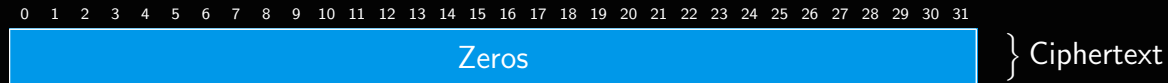
Server Hello



Client Authentication Packet



Server Acknowledgement



PKCS7 Padding

												03	03	03
										04	04	04	04	04
								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
									06	06	06	06	06	06