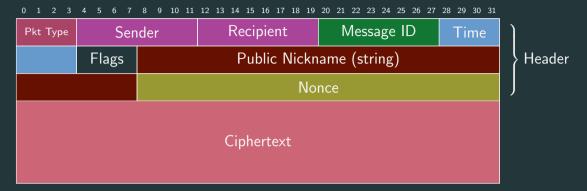
Message Packet (Threema Protocol Layer)



• 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

0 1 2 3	4 5 6 7	8 9 10 11	12 13 14 15 16 17 1	.8 19	20 21 22 23 24 25 26 27	28 29 30 31		
Pkt Type	Ser	ıder	Recipient		Message ID	Time		
	Flags	Public Nickname (string)					Header	
				No	nce			
0×01	1	ext		V	ariable-length Pad	ding	_ }	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		
	Ser	ıder	Recipie	ent	Message ID	Time		
	Flags	gs Public			ıblic Nickname (string)			
				No	nce			
Blop ID				Size	Kε	ey .)	
								Ciphertext
		Va	ariable-length	n Paddi	ng			

- 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

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	Sen	der	der Recipient Message ID Ti		Time			
	Flags		Public Nickname (string)					Message Header
	Nonce					J		
Creator ID Group ID)			
Text							Ciphertext	
Variable-length Padding						$^{-}$ J		

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		
Р		Ser	nder	Recipient Message ID Time					
		Flags		Public Nickname (string)			}	Message Header	
				Nonce					
0×41	Cre	eator ID	Group ID Blob ID						
	Size		Key					}	Ciphertext
Variable-length Padding									

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 2	28 29 30 31	
Pkt Type	Ser	ıder	Recipient			
	Flags		Public Nickn	Message Header		
			No	J		
⊜ Gr	oup 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	Ser	nder	Recipient	Message ID	Time	
	Flags		Public Nickn	Message Header		
	Nonce					J
<mark>7</mark> Gr	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
		← Length	\longrightarrow