Flow of encryption:

0)when a message server is register to auth,he send a aes symmetric key,used to open the ticket received from the client(created by auth).  
1)client request symmetric key(1027)-send serverID,nonce

2)Auth send back(1603)-clientID,Encrpypted Key(only client can open it, by using the password hash) and ticket(can open only by MessageServer

Encrtpted key is the MessageServer aes key encrypted by the user password hash. Contain iv,nonce,aes key for the message

Ticket is handled by client,he only receive it and send it to messageServer.

Nonce-is send to auth server when requesting symmetric key and send back from auth to client encrypted and should be the same as sent.

A diagram of a triangle with arrows and letters

Description automatically generated with medium confidence3)client send to messageServer ticket(unhandled) and authenticator