Identity-Based Symmetric Key Cryptography Mechanisms
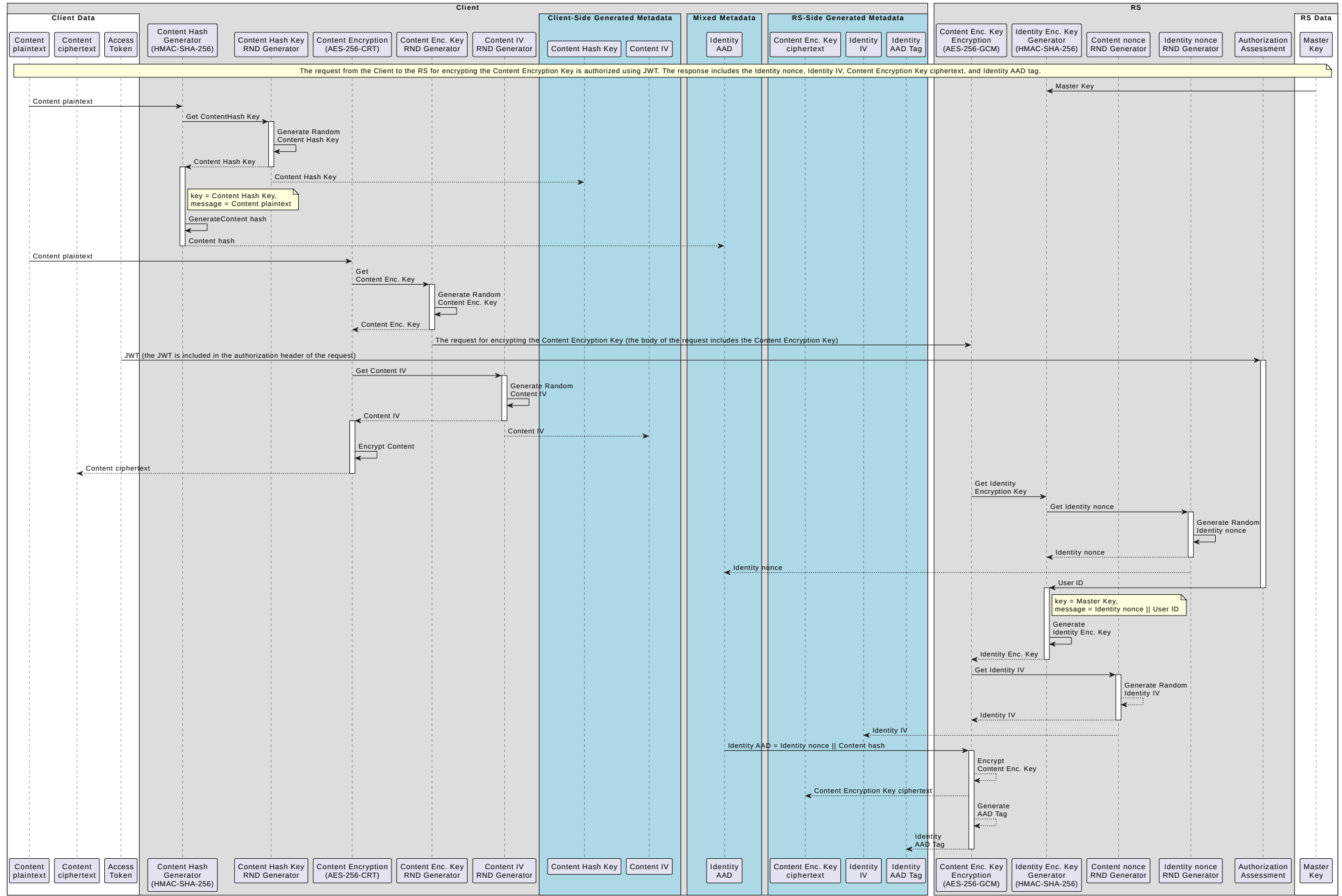
Acronyms

- RS: Resource Server

Sequence Diagram for Encryption:

The diagram contains the following participants and columns:

Client Data: Content plaintext | Content ciphertext | Access Token

Client: Content Hash Generator (HMAC-SHA-256) | Content Hash Key RND Generator | Content Encryption (AES-256-CRT) | Content Enc. Key RND Generator | Content IV RND Generator

Client-Side Generated Metadata: Content Hash Key | Content IV

Mixed Metadata: Identity AAD

RS-Side Generated Metadata: Content Enc. Key ciphertext | Identity IV | Identity AAD Tag

RS: Content Enc. Key Encryption (AES-256-GCM) | Identity Enc. Key Generator (HMAC-SHA-256) | Content nonce RND Generator | Identity nonce RND Generator | Authorization Assessment

RS Data: Master Key

The request from the Client to the RS for encrypting the Content Encryption Key is authorized using JWT. The response includes the Identity nonce, Identity IV, Content Encryption Key ciphertext, and Identity AAD tag.

Master Key

Content plaintext

Get ContentHash Key

Generate Random Content Hash Key

Content Hash Key

Content Hash Key

key = Content Hash Key, message = Content plaintext

GenerateContent hash

Content hash

Content plaintext

Get Content Enc. Key

Generate Random Content Enc. Key

Content Enc. Key

The request for encrypting the Content Encryption Key (the body of the request includes the Content Encryption Key)

JWT (the JWT is included in the authorization header of the request)

Get Content IV

Generate Random Content IV

Content IV

Content IV

Encrypt Content

Content ciphertext

Get Identity Encryption Key

Get Identity nonce

Generate Random Identity nonce

Identity nonce

Identity nonce

User ID

key = Master Key, message = Identity nonce || User ID

Generate Identity Enc. Key

Identity Enc. Key

Get Identity IV

Generate Random Identity IV

Identity IV

Identity IV

Identity AAD = Identity nonce || Content hash

Encrypt Content Enc. Key

Content Encryption Key ciphertext

Generate AAD Tag

Identity AAD Tag

Sequence Diagram for Decryption:

Client
- Client Data
  - Content plaintext
  - Content ciphertext
  - Access Token
- Content Hash Generator (HMAC-SHA-256)
- Content Decryption (AES-256-CRT)
- Client-Side Generated Metadata
  - Content Hash Key
  - Content IV
- Mixed Metadata
  - Identity AAD
- RS-Side Generated Metadata
  - Content Enc. Key ciphertext
  - Identity IV
  - Identity AAD Tag

RS
- Content Enc. Key Decryption (AES-256-GCM)
- Identity Enc. Key Generator (HMAC-SHA-256)
- Authorization Assessment
- RS Data
  - Master Key

The request from the Client to the RS for decrypting the Content Encryption Key is authorized using JWT. The response includes the Content Encryption Key.

Master Key

Content ciphertext

Content IV

The request for decrypting the Content Encryption Key
(the body of the request includes the Content Encryption Key ciphertext, Identity IV, Identity AAD, and Identity AAD Tag)

JWT (the JWT is included in the authorization header of the request)

Identity AAD

User ID

Get the Identity Enc. Key using the Identity nonce extracted from the Identity AAD

key = Master Key,
message = Identity nonce || User ID

Generate Identity Enc. Key

Identity Enc. Key

Content Encryption Key ciphertext

Identity IV

Identity AAD Tag

Decrypt Content Enc. Key ciphertext

Content Enc. Key

Decrypt Content

Content plaintext