Meghalaya State API Gateway Document (API CLIENT)

Process Flow

1. Bearer authentication will be shared with client application for sending as request header to API.
2. App ID will be shared to the API client which has to be passed as a mandatory parameter for each API call
3. A private secret key and IV will be shared with client application for purpose of encrypting requests and decrypting responses
    a. Encryption and Decryption algorithm used is AES-256-CBC
    b. Encryption with openssl_encrypt and then base64_encode
    c. Decryption with base64_decode and then openssl_decrypt
4. The first request from client application is for generating token. app_id and encrypted request data will be sent as parameters to the API. Encrypted JSON Response containing a token and an encrypted random generated user data will be sent to the client application.
5. When the JSON response is received, the client will decrypt the JSON response using the private Secret Key and IV.
6. In the subsequent requests the client application will send the app_id, token and the encrypted random generated user data along with the other parameters. The token, encrypted random generated user data should be encrypted along with the other parameters.
7. Then the encrypted request will be decrypted at the API Server using private Secret Key and IV of the client application.
8. Firstly the validity of the token will be checked, if token is invalid or expired,accordingly a response will be sent to the client. In this scenario, the client application will fire a request to get fresh token again (step 4).
9. If the token is valid, the client request will be processed and a response from the API will be encrypted using the private Secret Key and IV of the client application, and then sent back as JSON response.
10. Step 5 will be again repeated by the client to avail the decrypted response.