ETI Encryption FAQs

Version 1.0

30th April 2024.

Frequently asked questions while implementing TLS and EVP_AES cryptography.

Procedure related queries:

1. *What version of TLS protocol should be used while initiating TLS handshake?*
    - The minimum and maximum version should be TLS v1.3.

2. *For implementing TLS v1.3, how to check the authenticity of established TLS connection with connection gateway?*
    - Member will get a Self-Signed CA certificate valid for one year. IT is currently made available on the website at a specific location. Gateway certificate received during TLS handshake with Connection Gateway must be verified with the certificate provided by exchange.

3. *Is there any change in ETI version?*
    - ETI Version 2.4 has been introduced, which consists of all the necessary message structure related with encryption/decryption. The ETI version is supplied in the field DefaultCstmApplVerID(1408) of Session Logon Request (10000)
    - ETI Version 2.3 will still be present as a backward compatible feature for non-encrypted channels.

4. *While sending Connection Gateway Request (10020) to Connection Gateway receiving Forced Logout Notification with VarText as "TLS handshake failed => immediate disconnect". What does this mean?*
    - This may happen because of following reason:
        i. If member is connecting from a non-TLS socket to a TLS connection gateway.
        ii. If a member is sending message from a TCP socket to a TLS Connection gateway.
    - Necessary steps to be taken to fix this issue are as follows:
        - First check the connection Gateway IP and Port.
        - Ensure that TLS socket has been created and handshake has been initiated before sending request to a TLS connection gateway.
        - Verify that both Session and Connection Gateway is using TLS.

5. *Will gateway also encrypt the response?*
    - All responses [except Session Registration Request (10053) and Connection Gateway Response (*10022*)] will be encrypted and member application must decrypt the response before consuming it.

6. *What are the major changes in ETI v2.4?*
    - All messages under ETI v2.4 will be in an encrypted channel.
        i. Connection Gateway Response (10022) Template ID has been changed and the structure has been modified.

ii. Session Registration Request (10053) has been added as a new request message.
iii. Session Registration Response (10054) has been added as a new response message.

7. *Is there any change in existing message structure?*
   - Members will receive Connection Gateway Response (10022) structure while connecting through TLS channel. In Connection Gateway Response (10022), two more fields have been added i.e., SecurityKey and InitializationVector.

8. *What will happen if we send gateway request via a TLS socket to non-TLS Connection Gateway?*
   - The session would be disconnected with decode error.

9. *What is SecurityKey and InitializationVector in Connection Gateway Response (10022)?*
   - The SecurityKey (32 bytes) and InitializationVector (16 bytes) received in Gateway Response (10022) must be used for encryption/decryption using EVP_AES_256_GCM mode.

10. *Will member get SecurityKey and InitializationVector everytime sending Connection Gateway Request (10020)?*
    - With every Connection Gateway Request (10020) with ETI v2.4, member will get unique and randomized SecurityKey and InitializationVector in Connection Gateway Response.

11. *What is Session Registration Request (10053)?*
    - This is the first message that member must send to TLS Gateway. The message conveys that all successive messages will be encrypted over network.

12. *Should Session Registration Request (10053) be encrypted?*
    - Session Registration Request (10053) must not be encrypted.

13. *What if Session Registration Request (10053) failed?*
    - Member will get a Standard reject response message(10010) in unencrypted format and hence application must not decrypt it.

14. *What is Session Registration Response (10054), and should it be decrypted?*
    - Member will get Session Registration Response (10054) in response of Session Registration Request (10053). Gateway will not encrypt the Session Registration Response (10054). Hence Session Registration Response (10054) must not be decrypted.

15. *Will first request's response from Gateway be encrypted?*
    - First response from gateway, either Session Registration Response (10054) or any reject message will not be encrypted.

16. *Should entire message be encrypted/decrypted?*
    - Message Header i.e., 16 Bytes of MessageHeaderIn for ETI Message Request and 8 bytes of MessageHeaderOut of ETI Message Response must not be encrypted/decrypted. The message barring the header should be encrypted/decrypted.

17. *What if member sends Connection Gateway Request (10020) to TLS Connection Gateway with TLS socket but filled ETI version 2.3?*
    - Member will get ERROR "Invalid DefaultCstmApplVerID" in Reject Message (10010).

18. *What if member sends Gateway request to TLS connection gateway with version 2.4 and sends Session Logon Request (10000) with ETI version 2.3?*
    - If message is encrypted, then it will reject the request with the error "Invalid DefaultCstmApplVerID".
    - If message is not encrypted, then it will reject and will give decode error and session will get disconnected immediately.

19. *I am getting the error "Invalid DefaultCstmApplVerID" followed by data in non-readable format?*
    - This error is encountered when:
        i. Key or IV is used wrong so gateway is unable to decrypt the message properly.
        ii. Context for encryption and decryption is used same.

20. *What if member sends Connection Gateway Request (10020) to TLS connection gateway with version 2.4 and sends Session Logon Request (10000) with ETI version 2.3?*
    - If Session Logon Request (10000) has been sent to Gateway in unencrypted format, then Gateway will send Reject Message (10010) with decode error.
    - If Session Logon Request (10000) has been sent in encrypted format, then gateway will first check that whether Session Registration Request (10053) has been sent or not if not sent then, it will reject the message with VarText "invalid first message => immediate disconnect". If Session Registration Request (10053) has been sent, then it will reject with VarText "Invalid DefaultCstmApplVerID".

21. *What if member sends Session Logon Request (10000) as a first message to TLS gateway?*
    - If the message is encrypted, then gateway will give decode error and session will be disconnected.
    - If the message is not encrypted, then gateway will send Reject Message (10010) with response as "Invalid First message => immediate disconnect".

22. *We can send Session Logon Request (10000) with encryption but not able to decrypt the response. How to fix it?*
23. *We can send Session Logon Request (10000) with encryption, and we are decrypting it as well, but further messages being encrypted/decrypted give data in unreadable format?*
    - Ensuring that separate context is used for encryption and decryption.

- The encrypt and decrypt length passed to encryption algorithm should be equivalent to decode or encode length.
- This problem may also arise due to initialize operation of AES 256 GCM happening every time while encrypting or decrypting.

24. *Do we need to set IV length to 16 bytes explicitly?*
    - IV length must be set to 16.

25. *If session is already logged in to NTA, what will happen if Session Registration Request (10053) is sent to gateway, what error will come?*
    - The response would be Reject message (10010). The request will be rejected with error "session already logged in" and session will be disconnected.

26. *If session is already logged in to NTA, and sent Session Logon Request (10000) to gateway, what error will come?*
    - If message is unencrypted, the request will be rejected with error “First message not session registration request => immediate disconnect”
    - If message is sent in encrypted format, it will throw decode error.

27. *What if Session Registration Request (10053) is sent twice, what will be the response?*
    - For the second request, the request will be rejected with error "Session already registered" and the session will be disconnected.

28. *When sending Session Logon Request (10000) getting error as "Invalid first message => immediate shutdown". How to fix it?*
    - In ETI version 2.4, First message must be Session Registration Request (10053) and Session Logon (10000) should be second message to gateway.

29. *The response for Session Registration Request (10053), i.e., Session Registration Response (10054) is comprehensible. But when we send Session Logon Request (10000), we get a Reject Reason (10010) which is not coherent (unable to decode). How to fix it?*
    - It may arise because of following reason:
        i. This may happen due to same context used for encrypting and decrypt method. Please make sure that you are creating different context for encrypt and decrypt procedure.
        ii. It is also possible that encryption of Session Logon (10000) did not happen properly hence gateway could not decrypt it, hence error came. To fix it, make sure that IV length is set while initializing it.

30. *For Session Registration Request (10053) and Session Logon Request (10000), we get the respective response while we send User Logon (10018) or Subscribe (10025), Gateway is throwing decode error?*
    - For this, the possible reason may be, cipher context initialization is done every time while encrypting or decrypting. To fix it, make sure that you are initializing cipher once only and calling encrypt/decrypt function while encrypting and decrypting the data respectively.

31. *We are sending Session Logon Request (10000) for which we are getting response of message code 10010. But in this response, we are not getting proper reason.*
    - This issue may arise due to improper encryption of Session Logon Request (10000).

32. *We received rejection from Exchange in non-readable format. What may be the issue?*
    - It may arise, because of improper decryption of the response, received from gateway.

33. *Currently, Connection Gateway Response ID is 10021, but in New Encryption document it has been changed to 10022. Will Connection Gateway Response ID be changed to 10022 according to new encryption document?*
    - The template ID 10022 is now used for TLS Connection Gateway Response. Conversely, the template ID 10021 remains backward compatible with the non-TLS gateway responses. The template ID 10022 incorporates the additional field SecurityKey and InitializationVector in response.

34. *For Encrypted messages (for example 10100). What is the expected value on Message Header BodyLen? Is it going to be encrypted message length?*
    - The Message Header BodyLen functionality remain consistent with previous standards. This is in accordance with the principle that the plaintext length and ciphertext length will remain equivalent in the AES 256 GCM encryption algorithm.

35. *As per our testing in BSE-QA environment, after receiving Gateway Response 10022 from BSE, we send SSL_shutdown to close the SSL connection with BSE connection Gateway. During testing we received error 5 (SSL_ERR_SYSCALL) can you confirm if BSE performs SSL_shutdown?*
    - The SSL_ERR_SYSCALL error in OpenSSL serves as an umbrella term that denotes system errors. Frequently, this error arises due to the closure of the underlying socket or other system-level issues.

Implementation related queries

1. *Which encryption methodology to be used?*
   - TLS v1.3 at Connection Gateway and
   - EVP_AES_256_bits_GCM mode at Gateway.

2. *Will existing non encryption connection gateway and gateway still be in use?*
   - Yes, we have implemented TLS and EVP_AES in different connection gateway so it will not impact the existing ones.

3. *How to create Context for EVP_AES_256_bits_GCM mode?*
   - Different Context should be created for encryption and decryption operation as follows:

```
//Creating different contexts for encryption and decryption
EVP_CIPHER_CTX *encrypt
EVP_CIPHER_CTX *decrypt
  //
encrypt=EVP_CIPHER_CTX_new()
EVP_CIPHER_CTX_init(encrypt)
decrypt=EVP_CIPHER_CTX_new()
EVP_CIPHER_CTX_init(decrypt)
```

4. *How to initialize the cipher Context created above?*
   - Initialization of context with key and iv should be done only once as follows:

```
//For Decryption, sequence of function calls should be:
EVP_DecryptInit_ex(decrypt, EVP_aes_256_gcm(), NULL, NULL, NULL)
EVP_CIPHER_CTX_ctrl(decrypt, EVP_CTRL_GCM_SET_IVLEN, 16, NULL)
EVP_DecryptInit_ex(decrypt, NULL, NULL, key, iv)
  //
//For Encryption, sequence of function calls should be:
EVP_EncryptInit_ex(encrypt, EVP_aes_256_gcm(), NULL, NULL, NULL)
EVP_CIPHER_CTX_ctrl(encrypt, EVP_CTRL_GCM_SET_IVLEN, 16, NULL)
EVP_EncryptInit_ex(encrypt, NULL, NULL, key, iv)
```

5. *In which sequence, we should call function for encrypt and decrypt?*
    - Every time only EVP_DecryptUpdate or EVP_EncryptUpdate function should be called for subsequent decryption or encryption of the messages.

```
EVP_EncryptUpdate(encrypt, ciphertext, &len, plaintext, plaintext_len)
```

```
EVP_DecryptUpdate(decrypt, plaintext, &len, ciphertext, ciphertext_len)
```

    - Here, plaintext_len/ciphertext_len should be equal to the size of message that has to be encrypted/decrypted excluding header length.
    - e.g.: - For Session Logon (10000), plaintext_len = Total message length - Header In length = 280 - 16 = 264.
    - Similarly, For Session Logon Response (10001), ciphertext_len = Total message length - Header Out length = 104 - 8 = 96.s

Document Control Page

Sr. No.	Version	Date	Description
1.	1.0	30th April 2024	Original Document