Member FAQ's on "Encryption of Interactive Messages"

Version 1.5

September 2024

Disclaimer:

"This document/FAQ summarizes the queries relating to encrypted data type offered by Exchange in a concise manner for the Member's ease of understanding. The information and/ or content (collectively 'Information') provided herein is general information only and NSE has issued detailed circulars to that effect from time to time, as referred herein. While reasonable care has been exercised to ensure that the Information is adequate and reliable, no representation is made by NSE as to its accuracy or completeness and NSE, its affiliates and subsidiaries accept no liability of whatsoever nature for any direct or consequential loss, including without limitation any loss of profits, arising from reliance on this Information. The readers are expected to undertake their own diligence and are advised not to solely rely on this document. Any such reliance shall be at the reader's own risk. Nothing stated herein shall bind NSE, in any manner whatsoever."

Background

Currently, members connect to Exchange Trading System using Exchange provided NEAT Adapter / NEAT application or via Direct Connection through Encrypted data flow. In order to enhance the security posture, only encrypt of interactive messages are permissible.

Important Note: An interim coexistence phase for accepting login via old and/or new CA certificate shall be allowed by the Exchange, after which existing CA certificate shall be expired and disallowed for login.

Frequently Asked Questions (FAQs)

NON-TECHNICAL QUERY:

1. **Which all segments are available for encrypted data flow?**
   Currently, Exchange is providing encrypted data flow in COM, FO, CD, SLBM and CM segments in test market, Live and Simulation environments.

Segment	Releases in Test Environment	Releases in LIVE Environment	Releases in Simulated Environment
FO	Released on 31-Aug-23	07-October-2023	11-October-2023
CD	Released on 31-Aug-23	16-October-2023	18-October-2023
CM	Released on 27-Sep-23	06-November-2023	08-November-2023
CO	Released on 20-May-23	07-July-2023	29-August-2023
SLBM	Released on 20-Nov-23	04-December-2023	Not Available

2. **What is the Exchange test market environment configuration parameters to test encrypted data flow.**
   The details of parameters are provided under following link : https://ims.connect2nsccl.com/MemberPortal/view/testMrktHome.jsp or https://enit.nseindia.com/MemberPortal/view/testMrktHome.jsp

   Members are requested to configure below parameters for interactive session for encrypted data flows in the test market.

Segment	Gateway Router	
	IP Address	Port (to be used with New CA Certificate)
Capital Market	172.19.245.107	**10263**
Futures & Options	172.19.245.107	**10262**
Currency Derivatives	172.19.245.107	**10261**
Commodity Derivatives	172.19.245.107	**10264**
Securities Lending & Borrowing Market	172.19.245.107	**10268**

3. **What is the circular of interactive parameters applicable for Live environment.**

Segment	**Interactive Parameters**
Futures & Options (FO)	NSE/MSD/61777 & NSE/MSD/62602
Currency Derivatives (CD)	
Capital Market (CM)	
Commodity Derivatives (CO)	
Securities Lending & Borrowing Market (SLBM)	

4. **What is the Exchange Simulation market environment configuration parameters for encrypted data flow.**
   Members are requested to configure below parameters for interactive session for encrypted data flows in the Simulation market.

Segment	**Parameters**		**Encrypted Flow (NEW CA Certificate)**
Commodity Derivatives	**Gateway Router**	**IP Address**	172.19.245.108
		Port	**10274**
Futures & Options	**Gateway Router**	**IP Address**	172.19.245.108
		Port	**10272**
Currency Derivatives	**Gateway Router**	**IP Address**	172.19.245.108
		Port	**10271**
Capital Market	**Gateway Router**	**IP Address**	172.19.245.108
		Port	**10273**

5. **Can I use same CA certificate in test environment, Simulation environment and Live environment?**
   Members may use same CA certificate in test environment and simulated environment. However, the CA certificate for LIVE environment and test, simulated environments are different. Members may strictly use the CA certificate for the applicable environment only, else they will not be able to login to the Exchange environment.

6. **For test environment from where can we download new CA certificate ?**
   Members are requested to download the CA certificate from below mentioned Extranet path:-

Segment	**Extranet Path for "New CA Certificate" in Test & Simulation environment**
Capital Market	/common/Test_Environment/New_CM_CA_Certificate.zip
Futures & Options	/faoftp/faocommon/Test_Environment/New_FO_CA_Certificate.zip
Currency Derivatives	/cdsftp/cdscommon/Test_Environment/New_CD_CA_Certificate.zip
Commodity Derivatives	/comtftp/comtcommon/Test_Environment/ New_COM_CA_Certificate.zip

Securities Lending & Borrowing Market	/slbftp/slbcommon/Test_Environment/New_SLBM_CA_Certificate.zip

Note: *Members are requested to use combination of new CA certificate, new IP and Port parameters.*

TECHNICAL QUERY:

7. **Which mode is used for AES256 Encryption?**
   GCM mode of symmetric cryptography AES 256 bits is used for Encryption and Decryption.

8. **Is authentication tag used in GCM mode?**
   Authentication tag feature is currently not being used in GCM mode. We might explore this feature in future.

9. **What should be the length of Cryptographic Initialization Vector (IV)?**
   - The IV provided by Exchange is 16 bytes, however currently only 12 bytes are in use. Exchange does not set the IV length explicitly.
   - The default IV length used by AES256 is 12 bytes if not explicitly specified.
   - IV length can be checked using EVP_CIPHER_CTX_iv_length(ctx) function.

10. **What if the message size is not in the multiple of 128 bits.**
    Message size may or may not be in multiples of 128 bits.

11. **What will be the first message after connection with Gateway?**
    The first message should always be Registration message (SECURE_BOX_REGISTRATION_REQUEST_IN).

12. **What if a user sends messages other than SECURE_BOX_REGISTRATION_REQUEST_IN as first message to Gateway?**
    If the user sends any message other than SECURE_BOX_REGISTRATION_REQUEST_IN, the Exchange will disconnect the user. Even heartbeat should not be sent before SECURE_BOX_REGISTRATION_REQUEST_IN

13. **When should be the length of the order message be calculated?**
    It is recommended to calculate length for the 22 byte network header post encryption.

14. **Is there any encoding mechanism used for padding data?**
    No encoding is used.

15. **Which part of the packet should be encrypted?**
    Packet excluding the 22-byte network header should be encrypted.

16. **When should the md5 checksum be calculated?**
    While sending data to exchange, calculate MD5 checksum first on actual order message and then Encrypt the packet. While receiving packet from Exchange, Decrypt the packet first and then verify MD5 checksum.

17. **How can one implement Encryption changes to connect to Exchange?**
    The detailed description and all the library calls are mentioned in the Annexure section of NNF protocol document for all segments. The link to access the API documents is as follows: https://www.nseindia.com/trade/platform-services-neat-trading-system-protocols

18. **Will the members on Non-encrypted channel also update the message structure changes?**
    The members connecting on non-encrypted channel shall no more be able to continue with existing message structures. Only the members opting to connect to the exchange via encryption channel need to apply all changes.

19. **Which RHEL version is expected to use for implementation?**
    Any RHEL version that supports OpenSSL 1.1.1 and TLS 1.3 can be used for implementation.

20. **What changes in the network header for encrypted members?**
    For members connecting on encrypted channel, sequence number from the order entry, modification, cancellation request message will be echoed back in response confirmation as well as rejection message.

21. **Should a context be created every time we send a message?**
    Context creation or Initialization should be done only once post connection with NET machine. Later for all the messages, only EVP_EncryptUpdate, EVP_DecryptUpdate should be called.

22. **Can you summarize a detailed steps of login sequence via encryption which can be followed for any segment?**
    Step 1: Member applications will connect to Exchange Gateway Router server on TCP using TLS 1.3 security protocol.
    As part of TLS 1.3 security protocol, it is recommended that member applications verify Gateway Router server authenticity using the **CA certificate** provided by the Exchange.

    Step 2.a: GR request and GR response messages will be sent and received by member applications using TLS 1.3 security protocol.

    Step 2.b: GR Response: IP address, Port, Session key and **cryptographic key and cryptographic IV** (Initialization Vector) will be provided to member applications as part of GR response message.

    Step 3: Post successful communication with Gateway router server, member applications will establish a new TCP connection with the allocated gateway server of Exchange.

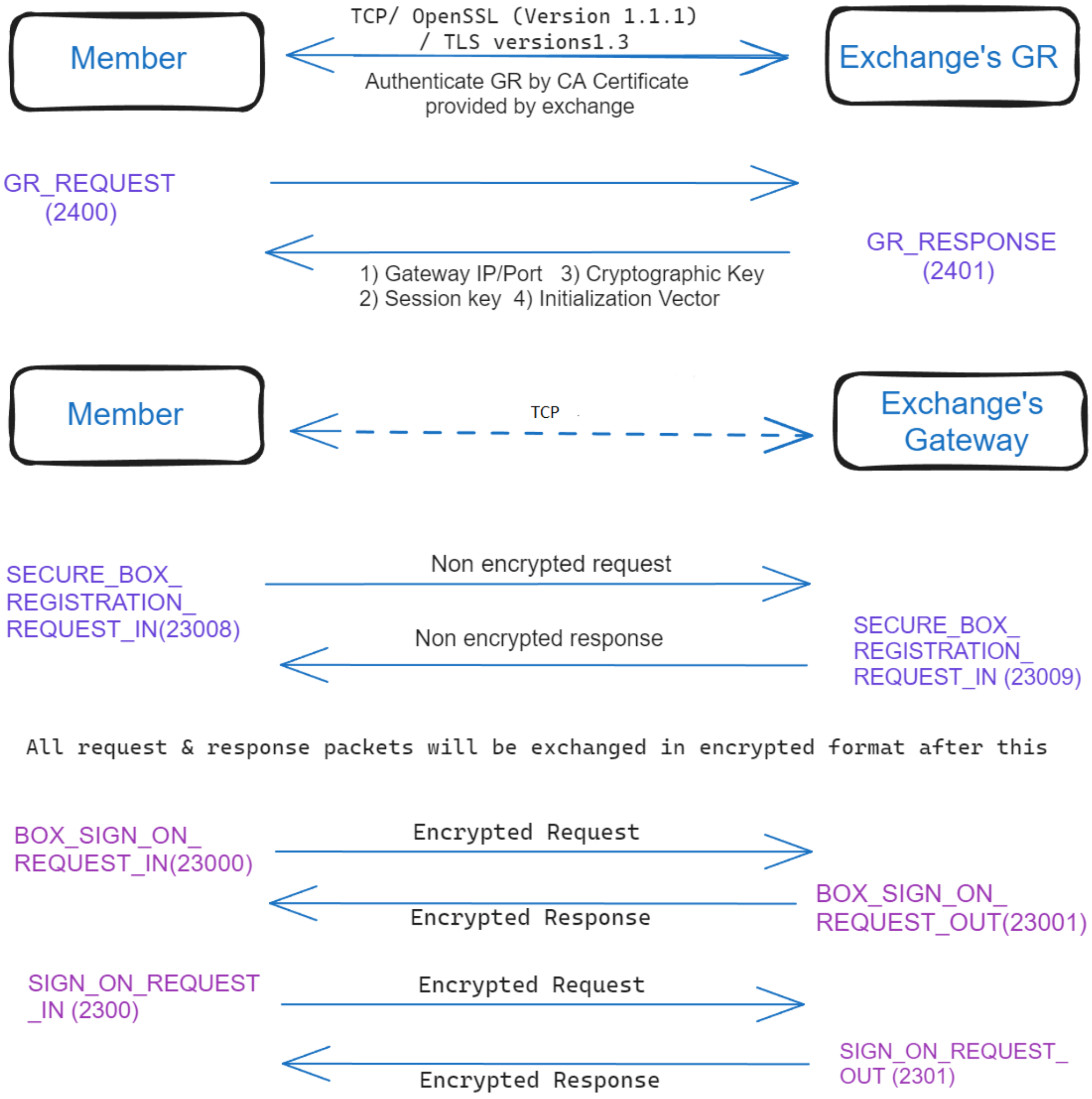
    Step 4.a: Once TCP connection is established with Gateway Server IP & Port,
    member will send **SECURE_BOX_REGISTRATION_REQUEST** (first message after connecting through TCP will be a non-encrypted special registration message (SECURE_BOX_REGISTRATION_REQUEST) to indicate that member application is using encryption)

    Step 4.b: Exchange will send the **SECURE_BOX_REGISTRATION_RESPONSE**. If there is any error, then Error Code field in MESSAGE_HEADER will be populated with relevant error code in the SECURE_BOX_REGISTRATION_RESPONSE and the Box connection will be terminated.

    Step 5.a: All the messages, after the first message, that are exchanged on this connection from both sides (member applications and Exchange) will be encrypted and decrypted using the 32-byte session key that was provided from Exchange at the time of Gateway Router handshake.

Step 5.b: BOX_SIGN_ON_REQUEST_IN(23000) will be the first encrypted message sent by member to exchange gateway. And exchange will respond with the encrypted **BOX_SIGN_ON_REQUEST_OUT(23001)**, which member has to decrypt at his end.

ENCRYPTION LOGIN FLOW:


Member
TCP/ OpenSSL (Version 1.1.1) / TLS versions1.3
Authenticate GR by CA Certificate provided by exchange
Exchange's GR
GR_REQUEST (2400)
GR_RESPONSE (2401)
1) Gateway IP/Port 3) Cryptographic Key
2) Session key 4) Initialization Vector
Member
TCP
Exchange's Gateway
SECURE_BOX_ REGISTRATION_ REQUEST_IN(23008)
Non encrypted request
Non encrypted response
SECURE_BOX_ REGISTRATION_ REQUEST_IN (23009)
All request & response packets will be exchanged in encrypted format after this
BOX_SIGN_ON_ REQUEST_IN(23000)
Encrypted Request
Encrypted Response
BOX_SIGN_ON_ REQUEST_OUT(23001)
SIGN_ON_REQUEST _IN (2300)
Encrypted Request
Encrypted Response
SIGN_ON_REQUEST_ OUT (2301)

23. Does any Neat Adapter (NA) users have to follow any specific steps to configure the new CA certificate to the GR server certificate in the test environment?

Sr. No.	Do the following steps to configure the GR server certificate for connecting to test environment
1	Check that "<Cert_name>.pem" is present at path **installation_directory/<broker_id>/NA_<segment>/CONFIG,** if file is not present then copy the "<Cert_name>.pem" certificate into **NA Installation_directory/<broker_id>/NA_<segment>/CONFIG.**
2	1) Stop the NA before doing below changes. 2) Check the CERTIFICATE_PATH parameter in **NA installation_directory/<broker_id>/NA_<segment>/CONFIG/na_<segment>.ini** file and update the value as below: **CERTIFICATE_PATH= ../CONFIG/<Cert_name>.pem** 3) Then save the **na_<segment>.ini** configuration file. 4) Start the NA.

24. In Live environment, does any user has to do any configuration in the NEAT adapter (NA) as stated in point no. 23.

The CA certificates are already pre-installed within the NEAT Adapter application in the LIVE environment, hence users are only requested to download & install the exe as given by the Exchange.

***********END***********