"इंटरएक्टिव संदेशों का एन्क्रिप्शन" पर सदस्य अक्सर पूछे जाने वाले प्रश्न (एफएक्क्यू)

संस्करण 1.7

अप्रैल 2026

अस्वीकरण:

"यह दस्तावेज़/एफएक्क्यू सदस्यों की समझ में आसानी के लिए उपरोक्त विषय से संबंधित प्रश्नों का संक्षिप्त रूप में सारांश प्रस्तुत करता है। यहाँ दी गई जानकारी और/या विषय-वस्तु (सामूहिक रूप से 'सूचना') केवल सामान्य जानकारी है और एनएसई ने समय-समय पर इस संबंध में विस्तृत परिपत्र जारी किए हैं, जैसा कि यहाँ उल्लेख किया गया है। यद्यपि यह सुनिश्चित करने के लिए उचित सावधानी बरती गई है कि जानकारी पर्याप्त और विश्वसनीय है, एनएसई द्वारा इसकी सटीकता या पूर्णता के बारे में कोई प्रतिनिधित्व नहीं किया गया है और एनएसई, इसके सहयोगी और सहायक कंपनियाँ इस जानकारी पर निर्भरता से उत्पन्न होने वाले किसी भी प्रत्यक्ष या परिणामी नुकसान, जिसमें बिना किसी सीमा के लाभ की हानि भी शामिल है, के लिए किसी भी प्रकार का कोई दायित्व स्वीकार नहीं करते हैं। पाठकों से अपेक्षा की जाती है कि वे स्वयं परिश्रम करें और उन्हें सलाह दी जाती है कि वे केवल इस दस्तावेज़ पर भरोसा न करें। ऐसा कोई भी भरोसा पाठक के अपने जोखिम पर होगा। यहाँ कही गई कोई भी बात एनएसई को किसी भी तरह से बाध्य नहीं करेगी। पाठकों की सुविधा के लिए ऑनलाइन अनुवाद सेवाओं का प्रयोग करते हुए एफएक्क्यू की विषय-वस्तु का (हिंदी) भाषा में अनुवाद किया गया है। जबकि यह सुनिश्चित करने के लिए उचित सावधानी बरती गई है कि अनुवाद सटीक रहें, अनुवाद प्रक्रिया की तकनीकी सीमाओं के कारण अनुवाद में अशुद्धियां हो सकती हैं। पाठक मूल संस्करण (अंग्रेजी) के साथ अनुवादित सामग्री की सटीकता को सत्यापित कर सकते हैं। एफएक्क्यू में विसंगतियों या मतभेदों या अनुवाद से उत्पन्न होने वाले अनुपालन या प्रवर्तन उद्देश्यों के लिए कोई कानूनी प्रभाव नहीं होगा, जोकि उपयुक्त सर्कुलर के अधीन होंगे।

पृष्ठभूमि

वर्तमान में, सदस्य एक्सचेंज द्वारा प्रदान किए गए नीट एडाप्टर/नीट एप्लिकेशन का उपयोग करके या एन्क्रिप्टेड डेटा प्रवाह के माध्यम से सीधे कनेक्शन के माध्यम से एक्सचेंज ट्रेडिंग सिस्टम से जुड़ते हैं। सुरक्षा स्थिति को बढ़ाने के लिए, केवल इंटरैक्टिव संदेशों को एन्क्रिप्ट करने की अनुमति है।

महत्वपूर्ण नोट: पुराने और/या नए एन्क्रिप्शन के माध्यम से लॉगिन स्वीकार करने के लिए एक अंतरिम सह-अस्तित्व चरण को एक्सचेंज द्वारा अनुमति दी जाएगी, जिसके बाद मौजूदा एन्क्रिप्शन को लॉगिन के लिए अस्वीकार कर दिया जाएगा।

अक्सर पूछे जाने वाले प्रश्न

नोन-तकनीकी क्वेरी:

1. **एन्क्रिप्टेड डेटा प्रवाह के लिए कौन से सभी सेगमेंट उपलब्ध हैं?**
   वर्तमान में, एक्सचेंज टेस्ट बाजार में कॉम, एफओ, सीडी और सीएम सेगमेंट में और लाइव और सिमुलेशन वातावरण में कॉम और सीडी सेगमेंट में नया एन्क्रिप्टेड डेटा प्रवाह प्रदान कर रहा है।

सेगमेंट	टेस्ट वातावरण में रिलीज	लाइव वातावरण में रिलीज़	सिम्युलेटेड वातावरण में रिलीज
एफओ	22-सितंबर-25 को जारी किया गया	11-अप्रैल-2026	घोषित किए जाने हेतु
सीडी	19-सितंबर-25 को जारी किया गया	06-अक्टूबर-2025	हाँ
सीएम	04-Feb-25 को जारी किया गया	11-अप्रैल-2026	घोषित किए जाने हेतु
कॉम	27-नवंबर-25 को जारी किया गया	13-दिसंबर-2025	हाँ

2. **एन्क्रिप्टेड डेटा प्रवाह का टेस्ट करने के लिए एक्सचेंज टेस्ट बाजार पर्यावरण कॉन्फ़िगरेशन पैरामीटर क्या है।**
   मापदंडों का विवरण निम्नलिखित लिंक के तहत दिया गया है:
   https://www.nseindia.com/static/trade/platform-services-test-and-simulated-market-facility

   सदस्यों से अनुरोध है कि वे टेस्ट बाजार में एन्क्रिप्टेड डेटा प्रवाह के लिए इंटरैक्टिव सत्र के लिए उल्लिखित मापदंडों को कॉन्फ़िगर करें।

3. **लाइव वातावरण के लिए लागू इंटरैक्टिव मापदंडों का परिपत्र क्या है?**

सेगमेंट	पुराने इंटरएक्टिव पैरामीटर	नए इंटरएक्टिव पैरामीटर
वायदा और विकल्प (एफओ)	NSE/MSD/67674	NSE/FOP/72763
मुद्रा डेरिवेटिव (सीडी)		NSE/CD/70422
पूंजी बाजार (सीएम)		NSE/CMTR/72769
कमोडिटी डेरिवेटिव (कॉम)		NSE/COM/71599
प्रतिभूति ऋण और उधार बाजार (एसएलबीएम)		-

4. **एन्क्रिप्टेड डेटा प्रवाह के लिए एक्सचेंज सिमुलेशन बाजार परिवेश कॉन्फ़िगरेशन पैरामीटर क्या है.**
   सदस्यों से अनुरोध है कि वे सिमुलेशन बाजार में एन्क्रिप्टेड डेटा प्रवाह के लिए इंटरैक्टिव सत्र के लिए नीचे दिए गए मापदंडों को कॉन्फ़िगर करें। मापदंडों का विवरण निम्नलिखित लिंक के तहत दिया गया है:
   https://www.nseindia.com/static/trade/platform-services-test-and-simulated-market-facility

5. **क्या मैं टेस्ट वातावरण, सिमुलेशन वातावरण और लाइव वातावरण में एक ही सीए प्रमाणपत्र का उपयोग कर सकता हूं?**
   सदस्य टेस्ट वातावरण और सिम्युलेटेड वातावरण में एक ही सीए प्रमाणपत्र का उपयोग कर सकते हैं। हालाँकि, लाइव वातावरण और टेस्ट, सिम्युलेटेड वातावरण के लिए सीए प्रमाणपत्र अलग हैं। सदस्य केवल लागू वातावरण के लिए सीए प्रमाणपत्र का उपयोग कर सकते हैं, अन्यथा वे एक्सचेंज वातावरण में लॉगिन करने में सक्षम नहीं होंगे।

6. **टेस्ट वातावरण के लिए हम नया सीए प्रमाण पत्र कहां से डाउनलोड कर सकते हैं?**
   सदस्यों से अनुरोध है कि वे नीचे दिए गए एक्स्ट्रानेट पथ से सीए प्रमाण पत्र डाउनलोड करें: -

सेगमेंट	टेस्ट और सिमुलेशन वातावरण में "नए सीए प्रमाणपत्र" के लिए एक्स्ट्रानेट पथ
सेंटीमीटर	/common/Test_Environment/CM_NEW_CA_Certificate_2025.zip
एफ एंड ओ	/faoftp/faocommon/Test_Environment/FO_NEW_CA_Certificate_2025.zip
कॉम्पैक्ट डिस्क	/cdsftp/cdscommon/Test_Environment/CD_NEW_CA_Certificate_2025.zip
कॉम	/comtftp/comtcommon/Test_Environment/COM_NEW_CA_Certificate_2025.zip
एसएलबीएम	/slbftp/slbcommon/Test_Environment/SLBM_NEW_CA_Certificate_2025.zip

नोट: *सदस्यों से अनुरोध है कि वे नए सीए प्रमाणपत्र, नए आईपी और पोर्ट मापदंडों के संयोजन का उपयोग करें।*

तकनीकी क्वेरी:

7. **AES256 एन्क्रिप्शन के लिए किस मोड का उपयोग किया जाता है?**
   सममित क्रिप्टोग्राफी का जीसीएम मोड AES256 बिट्स एन्क्रिप्शन और डिक्रिप्शन के लिए उपयोग किया जाता है।

8. **क्या प्रमाणीकरण टैग का उपयोग GCM मोड में किया जाता है?**
   - प्रमाणीकरण टैग सुविधा का उपयोग अब जीसीएम मोड में किया जा रहा है।
   - MD5 चेकसम का उपयोग केवल प्रारंभिक संदेश, "सुरक्षित बॉक्स पंजीकरण अनुरोध" के लिए किया जाएगा। बाद के संचार के लिए, MD5 के स्थान पर प्रमाणीकरण टैग का उपयोग किया जाएगा।

9. **क्रिप्टोग्राफ़िक आरंभीकरण वेक्टर (IV) की लंबाई कितनी होनी चाहिए?**
   - एक्सचेंज द्वारा प्रदान किया गया IV 16 बाइट्स (8 बाइट्स स्थिर और 8 बाइट्स गतिशील) है।
   - सदस्य अनुप्रयोग में, एन्क्रिप्शन और डिक्रिप्शन कार्रवाई स्थिर और गतिशील आरंभीकरण वैक्टर (IVs) का एक संयोजन का उपयोग कर किया जाता है।
   - स्थिर और गतिशील IV विनिमय से प्राप्त GR प्रतिसाद संदेश से लिया गया है।
   - स्थैतिक IV अपरिवर्तित रहता है, हालांकि प्रत्येक संदेश के लिए गतिशील IV को संशोधित किया जाता है।
   - सदस्य सिस्टम को इसकी दो प्रतियां **बनानी होंगी** - एक एन्क्रिप्शन के लिए और **दूसरी** डिक्रिप्शन **के लिए**।

   IV में **दो भाग होते हैं**:
   - **पहले 8 बाइट्स** → *स्थैतिक भाग*
   - **अगले 8 बाइट्स** → *गतिशील भाग*

   यदि सदस्य सिस्टम **लिटिल-एंडियन** है, **तो एन्क्रिप्शन और डिक्रिप्शन प्रतियां बनाने से पहले** डायनेमिक 8-बाइट भाग **को बाइट-स्वैप** (ट्विडल्ड) होना चाहिए।
   एक बार दोनों IV प्रतियां तैयार हो जाने के बाद, उनका उपयोग एन्क्रिप्शन और डिक्रिप्शन के लिए स्वतंत्र रूप से किया जाएगा।
   गतिशील IV भाग को विनिर्देश के अनुसार अद्यतन किया जाना चाहिए:

- **एन्क्रिप्शन के दौरान** वृद्धि
- एन्क्रिप्शन के दौरान **बढ़ाया जाता है**
- डिक्रिप्शन के दौरान **घटाया जाता है**

यह सुनिश्चित करता है कि दोनों पक्ष (एक्सचेंज और सदस्य आवेदन) उचित IV बनाए रखते हैं।

10. क्या होगा यदि संदेश का आकार 128 बिट्स के गुणक में नहीं है।
संदेश का आकार 128 बिट्स के गुणकों में हो सकता है या नहीं भी हो सकता है।

11. गेटवे के साथ कनेक्शन के बाद पहला संदेश क्या होगा?
पहला संदेश हमेशा पंजीकरण संदेश (SECURE_BOX_REGISTRATION_REQUEST_IN) होना चाहिए।

12. क्या होगा यदि कोई उपयोगकर्ता गेटवे पर पहले संदेश के रूप में SECURE_BOX_REGISTRATION_REQUEST_IN के अलावा अन्य संदेश भेजता है?
यदि उपयोगकर्ता SECURE_BOX_REGISTRATION_REQUEST_IN के अलावा कोई अन्य संदेश भेजता है, तो एक्सचेंज उपयोगकर्ता को डिस्कनेक्ट कर देगा। यहां तक कि दिल की धड़कन भी SECURE_BOX_REGISTRATION_REQUEST_IN से पहले नहीं भेजनी चाहिए।

13. ऑर्डर संदेश की लंबाई की गणना कब की जानी चाहिए?
एन्क्रिप्शन के बाद 22 बाइट नेटवर्क हेडर के लिए लंबाई की गणना करने की अनुशंसा की जाती है।

14. क्या डेटा पैडिंग के लिए कोई एन्कोडिंग तंत्र का उपयोग किया जाता है?
कोई एन्कोडिंग का उपयोग नहीं किया जाता है।

15. पैकेट के किस हिस्से को एन्क्रिप्ट किया जाना चाहिए?
22-बाइट नेटवर्क हेडर को छोड़कर पैकेट एन्क्रिप्ट किया जाना चाहिए।

16. md5 चेकसम की गणना कब की जानी चाहिए?
- विनिमय करने के लिए डेटा भेजते समय, वास्तविक आदेश संदेश पर पहले MD5 चेकसम की गणना करें, और उसके बाद पैकेट एन्क्रिप्ट करें। एक्सचेंज से पैकेट प्राप्त करते समय, पहले पैकेट को डिक्रिप्ट करें, और उसके बाद MD5 चेकसम की जाँच करें।
- MD5 चेकसम का उपयोग केवल प्रारंभिक संदेश, "सुरक्षित बॉक्स पंजीकरण अनुरोध" के लिए किया जाएगा। बाद के संचार के लिए, प्रमाणीकरण टैग 22 बाइट्स नेटवर्क शीर्ष लेख में md5 के बजाय पॉप्युलेट किया जा करने के लिए।

17. एक्सचेंज से कनेक्ट करने के लिए एन्क्रिप्शन परिवर्तनों को कैसे लागू किया जा सकता है?
विस्तृत विवरण और सभी पुस्तकालय कॉल का उल्लेख सभी खंडों के लिए एनएनएफ प्रोटोकॉल दस्तावेज़ के अनुलग्नक अनुभाग में किया गया है। एपीआई दस्तावेज़ों तक पहुंचने का लिंक इस प्रकार है: https://www.nseindia.com/trade/platform-services-neat-trading-system-protocols

18. क्या नोन-एन्क्रिप्टेड चैनल पर सदस्य संदेश संरचना में बदलाव को भी अपडेट करेंगे?
नोन-एन्क्रिप्टेड चैनल पर कनेक्ट होने वाले सदस्य अब मौजूदा संदेश संरचनाओं के साथ जारी रखने में सक्षम नहीं होंगे। केवल एन्क्रिप्शन चैनल के माध्यम से एक्सचेंज से कनेक्ट करने का विकल्प चुनने वाले सदस्यों को सभी परिवर्तनों को लागू करने की आवश्यकता है।
नोन-एन्क्रिप्शन चैनल बंद कर दिया गया।

19. कार्यान्वयन के लिए किस RHEL संस्करण का उपयोग करने की उम्मीद है?
कोई भी RHEL संस्करण जो OpenSSL 3.4.0 और TLS 1.3 का समर्थन करता है, कार्यान्वयन के लिए उपयोग किया जा सकता है।

20. एन्क्रिप्टेड सदस्यों के लिए नेटवर्क हेडर में क्या परिवर्तन होते हैं?
एन्क्रिप्टेड चैनल पर कनेक्ट होने वाले सदस्यों के लिए, ऑर्डर प्रविष्टि, संशोधन, रद्दीकरण अनुरोध संदेश से अनुक्रम संख्या प्रतिक्रिया पुष्टिकरण के साथ-साथ अस्वीकृति संदेश में वापस प्रतिध्वनित होगी।

21. क्या हर बार जब हम कोई संदेश भेजते हैं तो एक संदर्भ बनाया जाना चाहिए?
नहीं, लेकिन प्रत्येक संदेश के लिए IV को प्रारंभ करने की आवश्यकता है।

22. क्या आप एन्क्रिप्शन के माध्यम से लॉगिन अनुक्रम के विस्तृत चरणों को संक्षेप में प्रस्तुत कर सकते हैं जिसका पालन किसी भी सेगमेंट के लिए किया जा सकता है?
चरण 1: सदस्य अनुप्रयोग TLS 1.3 सुरक्षा प्रोटोकॉल का उपयोग कर TCP पर एक्सचेंज गेटवे रूटर सर्वर से कनेक्ट हो जाएगा।
TLS 1.3 सुरक्षा प्रोटोकॉल के भाग के रूप में, यह अनुशंसा की जाती है कि सदस्य अनुप्रयोग एक्सचेंज द्वारा प्रदान किए गए सीए प्रमाण पत्र का उपयोग कर गेटवे रूटर सर्वर प्रामाणिकता की जाँच करें ।

चरण 2.a: GR अनुरोध और GR प्रतिसाद संदेश भेजे जाएंगे और TLS 1.3 सुरक्षा प्रोटोकॉल का उपयोग करके सदस्य अनुप्रयोगों द्वारा प्राप्त किए जाएंगे।

चरण 2.b: जीआर प्रतिक्रिया: आईपी पता, पोर्ट, सत्र कुंजी, **क्रिप्टोग्राफ़िक कुंजी और क्रिप्टोग्राफ़िक IV** (आरंभीकरण वेक्टर) और **क्रिप्टोग्राफ़िक अतिरिक्त कुंजी** जीआर प्रतिसाद संदेश के भाग के रूप में सदस्य अनुप्रयोगों के लिए प्रदान की जाएगी।

चरण 3: गेटवे रूटर सर्वर के साथ सफल संचार पोस्ट करें, सदस्य अनुप्रयोग एक्सचेंज के आवंटित गेटवे सर्वर के साथ एक नया TCP कनेक्शन स्थापित करेंगे।

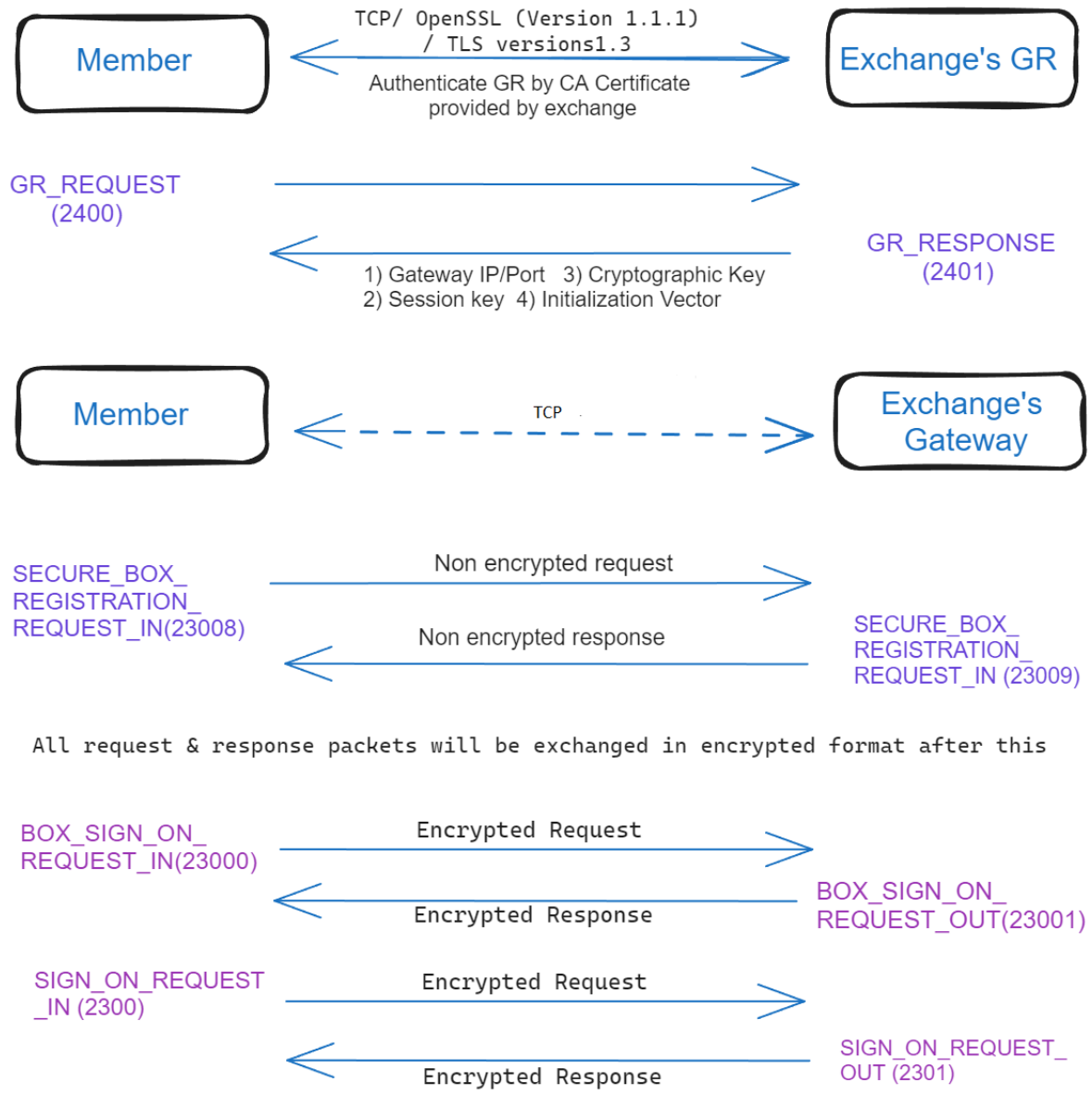
चरण 4.ए: एक बार गेटवे सर्वर आईपी और पोर्ट के साथ टीसीपी कनेक्शन स्थापित हो जाने के बाद,
सदस्य SECURE_BOX_REGISTRATION_REQUEST भेजेंगे (TCP के माध्यम से कनेक्ट करने के बाद पहला संदेश एक नोन-एन्क्रिप्टेड विशेष पंजीकरण संदेश (SECURE_BOX_REGISTRATION_REQUEST) होगा जो यह इंगित करने के लिए होगा कि सदस्य अनुप्रयोग एन्क्रिप्शन का उपयोग कर रहा है)

चरण 4.b: एक्सचेंज SECURE_BOX_REGISTRATION_RESPONSE भेजेगा। यदि कोई त्रुटि है, तो MESSAGE_HEADER में त्रुटि कोड फ़ील्ड SECURE_BOX_REGISTRATION_RESPONSE में प्रासंगिक त्रुटि कोड से भर जाएगा और बॉक्स कनेक्शन समाप्त हो जाएगा।

चरण 5.a: सभी संदेश, पहले संदेश के बाद, जो इस कनेक्शन पर दोनों पक्षों (सदस्य अनुप्रयोग और विनिमय) से आदान-प्रदान किए जाते हैं एन्क्रिप्ट किया जाएगा और 32-बाइट सत्र कुंजी, **क्रिप्टोग्राफ़िक कुंजी और क्रिप्टोग्राफ़िक IV** (प्रारंभ वेक्टर) और **क्रिप्टोग्राफ़िक अतिरिक्त कुंजी** जो गेटवे रूटर हैंडशेक के समय एक्सचेंज से प्रदान किया गया था।

चरण 5.b: BOX_SIGN_ON_REQUEST_IN (23000) गेटवे का आदान-प्रदान करने के लिए सदस्य द्वारा भेजा गया पहला एन्क्रिप्टेड संदेश होगा। और एक्सचेंज एन्क्रिप्टेड **BOX_SIGN_ON_REQUEST_OUT (23001) के साथ जवाब देगा**, जिसे सदस्य को अपने अंत में डिक्रिप्ट करना होगा।

एन्क्रिप्शन लॉगिन प्रवाह:



23. क्या किसी भी नीट एडाप्टर (एनए) उपयोगकर्ताओं को टेस्ट वातावरण में जीआर सर्वर प्रमाणपत्र के लिए नए सीए प्रमाणपत्र को कॉन्फ़िगर करने के लिए किसी विशिष्ट चरणों का पालन करना होगा?

क्रमांक	टेस्ट परिवेश से कनेक्ट करने के लिए GR सर्वर प्रमाणपत्र को कॉन्फ़िगर करने के लिए निम्न चरणों का पालन करें
1	जांचें कि "<Cert_name>.pem" पथ **installation_directory/<broker_id>/NA_/CONFIG** पर मौजूद है, यदि फ़ाइल मौजूद नहीं है तो "<Cert_name>.pem" प्रमाणपत्र को **NA Installation_directory/<broker_id>/NA_/CONFIG में कॉपी करें।**

2	1. नीचे दिए गए परिवर्तन करने से पहले NA को रोकें। 2. **NA installation_directory/<broker_id>/NA_/CONFIG/na_.ini** फ़ाइल में CERTIFICATE_PATH पैरामीटर की जाँच करें और नीचे दिए गए मान को अपडेट करें: **CERTIFICATE_PATH= ../CONFIG/<Cert_name>.pem** 3. फिर **na_.ini** कॉन्फ़िगरेशन फ़ाइल को सेव करें। 4. एनए शुरू करें।

24. लाइव वातावरण में, क्या किसी उपयोगकर्ता को नीट एडाप्टर (एन ए) में कोई कॉन्फ़िगरेशन करना पड़ता है जैसा कि बिंदु संख्या 23 में कहा गया है।

सीए प्रमाणपत्र पहले से ही लाइव वातावरण में एनईएटी एडाप्टर एप्लिकेशन के भीतर पहले से इंस्टॉल हैं, इसलिए उपयोगकर्ताओं से केवल एक्सचेंज द्वारा दिए गए एक्सई को डाउनलोड और इंस्टॉल करने का अनुरोध किया जाता है।

**********अंत**********