EUREX

Mandatory Interface Encryption

Q&A from Focus Calls

16 March 2023

Deutsche Börse AG (DBAG), Clearstream Banking AG (Clearstream), Eurex Frankfurt AG, Eurex Clearing AG (Eurex Clearing) and Eurex Repo GmbH (Eurex Repo) are corporate entities and are registered under German law. Eurex Global Derivatives AG is a corporate entity and is registered under Swiss law. Clearstream Banking S.A. is a corporate entity and is registered under Luxembourg law. Deutsche Boerse Asia Holding Pte. Ltd., Eurex Clearing Asia Pte. Ltd. and Eurex Exchange Asia Pte. Ltd are corporate entities and are registered under Singapore law. Eurex Frankfurt AG (Eurex) is the administrating and operating institution of Eurex Deutschland. Eurex Deutschland is in the following referred to as the "Eurex Exchange".

All intellectual property, proprietary and other rights and interests in this publication and the subject matter hereof (other than certain trademarks and service marks listed below) are owned by DBAG and its affiliates and subsidiaries including, without limitation, all patent, registered design, copyright, trademark and service mark rights. While reasonable care has been taken in the preparation of this publication to provide details that are accurate and not misleading at the time of publication DBAG, Clearstream, Eurex, Eurex Clearing, Eurex Repo as well as the Eurex Exchange and their respective servants and agents (a) do not make any representations or warranties regarding the information contained herein, whether express or implied, including without limitation any implied warranty of merchantability or fitness for a particular purpose or any warranty with respect to the accuracy, correctness, quality, completeness or timeliness of such information, and (b) shall not be responsible or liable for any third party's use of any information contained herein under any circumstances, including, without limitation, in connection with actual trading or otherwise or for any errors or omissions contained in this publication.

This publication is published for information purposes only and shall not constitute investment advice respectively does not constitute an offer, solicitation or recommendation to acquire or dispose of any investment or to engage in any other transaction. This publication is not intended for solicitation purposes but only for use as general information.
All descriptions, examples and calculations contained in this publication are for illustrative purposes only.

Eurex and Eurex Clearing offer services directly to members of the Eurex Exchange respectively to clearing members of Eurex Clearing. Those who desire to trade any products available on the Eurex market or who desire to offer and sell any such products to others or who desire to possess a clearing license of Eurex Clearing in order to participate in the clearing process provided by Eurex Clearing, should consider legal and regulatory requirements of those jurisdictions relevant to them, as well as the risks associated with such products, before doing so.

Only Eurex derivatives that are CFTC-approved may be traded via direct access in the United States or by United States persons. A complete, up-to-date list of Eurex derivatives that are CFTC-approved is available at: http://www.eurexchange.com/exchange-en/products/eurex-derivatives-us. In addition, Eurex representatives and participants may familiarise U.S. Qualified Institutional Buyers (QIBs) and broker-dealers with certain eligible Eurex equity options and equity index options pursuant to the terms of the SEC's July 1, 2013 Class No-Action Relief. A complete, up-to-date list of Eurex options that are eligible under the SEC Class No-Action Relief is available at: http://www.eurexchange.com/exchange-en/products/eurex-derivatives-us/eurex-options-in-the-us-for-eligible-customers... Lastly, U.S. QIBs and broker-dealers trading on behalf of QIBs may trade certain single-security futures and narrow-based security index futures subject to terms and conditions of the SEC's Exchange Act Release No. 60,194 (June 30, 2009), 74 Fed. Reg. 32,200 (July 7, 2009) and the CFTC's Division of Clearing and Intermediary Oversight Advisory Concerning the Offer and Sale of Foreign Security Futures Products to Customers Located in the United States (June 8, 2010).

Trademarks and Service Marks

Buxl®, DAX®, DivDAX®, eb.rexx®, Eurex®, Eurex Repo®, Eurex Strategy Wizard℠, Euro GC Pooling®, FDAX®, FWB®, GC Pooling®, GCPI®, MDAX®, ODAX®, SDAX®, TecDAX®, USD GC Pooling®, VDAX®, VDAX-NEW® and Xetra® are registered trademarks of DBAG. All MSCI indexes are service marks and the exclusive property of MSCI Barra. ATX®, ATX® five, CECE® and RDX® are registered trademarks of Vienna Stock Exchange AG. IPD® UK Quarterly Indexes are registered trademarks of Investment Property Databank Ltd. IPD and have been licensed for the use by Eurex for derivatives. SLI®, SMI® and SMIM® are registered trademarks of SIX Swiss Exchange AG. The STOXX® indexes, the data included therein and the trademarks used in the index names are the intellectual property of STOXX Limited and/or its licensors Eurex derivatives based on the STOXX® indexes are in no way sponsored, endorsed, sold or promoted by STOXX and its licensors and neither STOXX nor its licensors shall have any liability with respect thereto. Bloomberg Commodity Index℠ and any related sub-indexes are service marks of Bloomberg L.P. PCS® and Property Claim Services® are registered trademarks of ISO Services, Inc. Korea Exchange, KRX, KOSPI and KOSPI 200 are registered trademarks of Korea Exchange Inc. BSE and SENSEX are trademarks/service marks of Bombay Stock Exchange (BSE) and all rights accruing from the same, statutory or otherwise, wholly vest with BSE. Any violation of the above would constitute an offence under the laws of India and international treaties governing the same.
The names of other companies and third party products may be trademarks or service marks of their respective owners.

Eurex Deutschland qualifies as manufacturer of packaged retail and insurance-based investment products (PRIIPs) under Regulation (EU) No 1286/2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs Regulation), and provides key information documents (KIDs) covering PRIIPs traded on Eurex Deutschland on its website under the following link: http://www.eurexchange.com/exchange-en/resources/regulations/eu-regulations/priips-kids.

In addition, according to Art. 14(1) PRIIPs Regulation the person advising on, or selling, a PRIIP shall provide the KID to retail investors free of charge.

Content

Q&A Focus Call

1. **Is FQDN usage mandatory or we can continue to use the IPs which FQDN is resolved to?**
   The usage of FQDNs for TLS certificates is not mandatory but is recommended to ensure the highest level of security and to avoid potential compatibility and maintenance issues. Please refer to Question 1.10 in the FAQ document.

2. **What is the latency impact?**
   Please refer to Question 1.8 in the FAQ document.

3. **Why is full encryption mandatory for Co-Location LF session while for PS sessions password encryption is sufficient?**
   Please refer to Question 2.5 in the FAQ document.

4. **Are there plans to offer TLS 1.3 in addition, or instead of TLS 1.2?**
   Please refer to Question 1.14 in the FAQ document.

5. **Is the use if FQDN mandatory when working with network providers and accessing LF via NAT ip?**
   The usage of FQDNs for TLS certificates is not mandatory but is recommended to ensure the highest level of security and to avoid potential compatibility and maintenance issues. Please refer to Question 1.10 in the FAQ document.

6. **If clients are using referential data downloaded via files (CRE technology), is this release also applicable for referential files?**
   The Common Report Engine (CRE), Reference Data files and the Market Data Interfaces are not affected by Interface Encryption.

7. **Is there a controversy between saying that the "application level" is not affected, but needing to adapt the application**?
   After establishing the TCP connection, you must implement the TLS handshake. After establishing that TLS tunnel, no further change required.

8. **Does TLS affect internal NATting of source addresses?**
   Currently we are not aware of any issues where TLS affects internal NATting.

9. **Why did you decide to support TLS 1.2 instead of TLS 1.3?**
   Please refer to Question 1.14 in the FAQ document.

10. **Do clients need to change their application code or is it just configuration change on the client trading server?**
    This depends on the application.

11. **Is "payload" level encryption meant or just the login message?**
    The payload encryption covers all messages including the user/session login.

12. **Is payload encryption mandatory only for ETI LF sessions, or for ETI HF sessions too?**
    Payload encryption is only relevant for FIX LF and ETI LF (outside of the Equinix FR2 co-location facility). For ETI HF sessions password encryption only must be applied. Please refer to Question 2.5 in the FAQ document.

13. **Is Deutsche Börse going to provide an example of setting up Stunnel for certificates?**
    No, we do not intend to provide any information regarding the setup of Stunnel.

14. **Are there plans to encrypt more services, e.g., T7-GUIs, CRE, CUE, etc.?**
    Currently there are no immediate plans to encrypt any further services.

15. **Why do LF session inside Co-Location need encryption as the regulator are saying it is applicable over public networks only?**
    Please refer to Question 2.5 in the FAQ document.

16. **What is the rationale behind mandating payload encryption for LF session inside of Deutsche Börse´s Equinix FR2?**
    Please refer to Question 2.5 in the FAQ document.

17. **The KRITIS regulation says payload needs to be encrypted over a public network. If clients have a private network in the Co-Location and have LF sessions in the Co-Location, why do they need to encrypt payload given they are not in breach of the regulation?**
    Please refer to Question 2.5 in the FAQ document.

18. If clients are not able to use FQDN due to firewall and security requirements, are there any impacts for them?

The usage of FQDNs for TLS certificates is not mandatory but is recommended to ensure the highest level of security and to avoid potential compatibility and maintenance issues. Please refer to Question 1.10 in the FAQ document.

19. Is deutsche Börse taking care of FQDNs in DR scenarios as well (i.e., FQDN resolving to Simu IPs instead of Prod IPs)?

Yes, the FQDNs for the DR scenario are documented in the "T7 Disaster Recovery Concept 2023" document which is available of the Eurex and Xetra websites.

20. If client´s configuration is only allowing IP address, is there any guide on how to configure IP addresses for TLS?

The usage of FQDNs for TLS certificates is not mandatory but is recommended to ensure the highest level of security and to avoid potential compatibility and maintenance issues. Please refer to Question 1.10 in the FAQ document.

21. Can clients add simple Stunnel installation with tls 1.2 to encrypt their current drop copysession?

Please refer to Question 1.14 in the FAQ document.

22. Does Deutsche Börse have experience in using Stunnel?

Please refer to Question 1.14 in the FAQ document.

23. Does the DIGICERT certificate have a validity date? Do the clients get an info from the exchange when the certificate is ending?

Please refer to Question 3.4 in the FAQ document.

24. **Client has already TLS implemented, but following issues arises: There are two failover IPs provided, but only on one interface client gets a valid SSL answer which prevents automatic failover by the fix engine. Will this be changed in future?"**
    Only the active FIX LF gateway accepts TLS handshakes. The secondary FIX LF gateway only processes TCP accepts, but no further payload including TLS handshakes. There are no plans to change this behavior.

25. **The FQDN in Network Access guide 2.2.4 is wrong: The FQDN for standby and Active gateway is the same. Page 47, https://www.eurex.com/resource/blob/3431832/44d6ac66032f200c51af96af43eefc01/data/N7_-_Network_Access_Guide.v.2.2.4.pdf**
    Yes, unfortunately there was a small mistake with version 2.2.4 of the Network Access Guide. The mistake has been corrected in Version 2.2.5 which has been published in line with the system documentation for Release 11.1.

    Will EEX and the Partner Exchanges be migrated to TLS 1.2?
    Yes, EEX will also be migrated to TLS 1.2 as will all the other partner exchanges. The timeline for EEX and the partner exchanges is identical to the one for Xetra and Eurex and which has been communicated. Please refer to Question 1.2 in the FAQ document.

26. **Reg. ETI HF sessions in Co-Location: Are clients only required to encrypt the password field on session and user logon? Do they need to use new message templates?**
    Only password encryption is required for ETI HF sessions. Please refer to the ETI manual (for more ETI details) and to Question 3.3 in the FAQ document for more information.

27. **Are HF sessions (in Co-Location) encrypted by TLS from start to end of the connection? The documentation said it was only the "password" field of the Login message - and that the rest of the communication would be in the clear. An earlier answer seemed to say otherwise.**
    Only password encryption is required for ETI HF sessions. Please refer to the ETI manual (for more ETI details) and to Question 3.3 in the FAQ document for more information.

28. Just to get this clear: once a year we need to download your certificate and put into a local truststore?

No, that is not required. Please refer to Question 3.4 in the FAQ document.

29. Can openssl be used for password encryption? If yes, is there a minimum version?

The password encryption protocol is proprietary and must be implemented according to the ETI Manual (chapter 5.3.3. Password Encryption). OpenSSL can be helpful for the cryptographic part of the protocol (RSA encryption: padding schema OAEP, the mask generation function MGF1 and the hash function SHA256).

30. Ich intermediate or root will be replaced before expiration will we receive a note

No. The server and the intermediate certificate are provided by the server during TLS handshake. Please refer to Question 3.4 in the FAQ document.