Derivatives and Cash Markets

Transport Layer Security (TLS) and Password Encryption

Frequently Asked Questions

Version: 2.3
Date: 05 October 2023

Introduction

This document is intended to provide answers to the most commonly asked questions related to the implementation of ETI / FIX LF Transport Layer Security (TLS) and ETI HF Password Encryption. The document will be updated at regular intervals to include the answers to additional questions as and when they are received. The FAQs have been sorted into relevant categories to ease navigation. If you do not find the answer to your question here, please contact your Technical Key Account Manager (TKAM) for further assistance.

Version History

Date	Version	Reason
19.01.2023	1.0	Initial Version
21.03.2023	1.1	Included answers to the questions from the Mandatory Interface Encryption – Focus Call from 16.03.23
29.03.2023	1.2	Updated the response to Question 1.14
10.05.2023	1.3	Updated the root certificates for Simulation Question 1.12 Updated response regarding the usage of Stunnel Question 1.18
22.05.2023	2.0	Updated the document to include the support for ETI LF password encryption in the Equinix FR2 facility and support for TLS 1.3 Added Questions 1.19 & 1.20
31.05.2023	2.1	Updated Question 1.19
31.07.2023	2.2	Updated Question 1.12
05.10.2023	2.3	Addition of Question 1.21

Contents

1. General

In this section general questions relating to TLS payload and ETI password encryption are addressed.

Question 1.1:	How does the encryption of FIX LF / ETI LF differ from the ETI HF encryption?
Answer:	FIX LF and ETI LF sessions outside of the Equinix FR2 co-location facility encrypt the whole communication by Transport Layer Security (TLS). This is referred to as "**Payload Encryption**" throughout this document. ETI HF does not use TLS to encrypt the whole traffic, but rather sends only the session and user password encrypted and keeps the rest of the traffic unchanged. This is referred to as "**Password Encryption**" throughout this document. ETI LF sessions within the Equinix FR2 co-location facility can also use password encryption.

Question 1.2:	Will TLS just be provided for Eurex and Xetra or are EEX, Vienna and the other Partner Exchanges also in scope for this method of connectivity?
Answer:	All markets are affected however the point in time where encryption will become mandatory can vary depending on the individual markets. Currently all partner exchanges have indicated that they will adopt the same timeline as Deutsche Börse.

Question 1.3:	How is TLS implemented, on the network level (i.e. on the router and leased line connectivity) or on the session level connectivity (i.e. each session has TLS on it, so multiple TLS sessions connect to Deutsche Börse?
Answer:	TLS is provided via a specific port on the existing gateways, so it is at a port-level but only for FIX LF and ETI LF sessions. The HF sessions will only have session and user password encryption and not TLS. ETI LF sessions within the Equinix FR2 co-location facility can also have session and password encryption.

Question 1.4:	How can FIX LF sessions be setup for TLS?
Answer:	The sessions themselves are not set up. Usage of TLS is performed by connecting the session to a specific port on the existing gateways as documented in the Network Access Guide.

Question 1.5:	What type of encryption is going to be used? Where and when will the encryption be applied?
Answer:	Payload encryption will be provided via TLS. A specific port is provided for FIX LF and ETI LF. Details of the ports can be found in the Network Access Guide. The implementation dates are shown in the circulars (Eurex 005/2023 and Xetra 002/2023). Password encryption will make use of Deutsche Börse's public RSA key.

Question 1.6:	The circular (085/2022) states HF sessions are also required to use TLS, does that include PS (Partition Specific) sessions?
Answer:	HF = Partition Specific (PS) will not use TLS encryption but are affected by the password encryption only.

Question 1.7:	Will the session password encryption for HF sessions have an impact on latency?
Answer:	No

Question 1.8:	Can latency impact for the ETI LF sessions if they route via the dedicated TLS payload encrypted gateways and ports be expected?
Answer:	Yes, but in the single digit microsecond range per roundtrip.

Question 1.9:	Is there a list of the FQDNs together with the associated IP addresses
Answer:	The FQDNs and the related IP addresses can be found in the Network Access Guide.

Question 1.10:	Can the IP addresses be used instead of the Fully Qualified Domain Names (FQDNs) for the connection to the encrypted ports?
Answer:	For the encrypted connectivity option, Deutsche Börse recommends the use of the FQDNs as opposed to the IP addresses. If IP addresses are used for the Transport Layer Security connectivity instead of the fully qualified domain names, warnings may be raised by the client library about a mismatch between the CommonName stored in the server's certificate and the URL used to access the server. Non-deterministic side-effects in the communication between server and client are possible and reaction to such a mismatch depends highly on the client library used and the way it is configured. The use of IP addresses as opposed to FQDNs also makes it more difficult for a client to reliably verify the identity of the server which it is connecting to. The IP address of the gateways can be dynamically assigned and changed in future whilst the FQDN will remain stable.

Question 1.11:	Is there a list of error code that will be returned when we connect in simulation and production along with their meaning if there is a problem
Answer:	Regarding the TLS protocol please refer to RFC5246 (TLS 1.2) (https://www.rfc-editor.org/rfc/rfc5246) or RFC8446 (TLS 1.3) (https://www.rfc-editor.org/rfc/rfc8446) for a detailed specification including the related errors/alerts and their meaning. The error codes of the FIX LF and ETI protocol do not differ from the ones used for a non-encrypted connection.

Question 1.12:	How exactly should TLS be used for both FIX and ETI
Answer:	The connection on the TLS port, as listed in the Network Access Guide, is used exclusively for encrypted data and therefore the client must not send any application data before the TLS handshake process has been successfully completed. Following a successful TCP connect, a TLS handshake must be initiated by the client. During a TLS handshake, the server and the client exchange messages to acknowledge each other, verify each other, establish the cryptographic algorithms they will use, and agree on session keys. TLS renegotiations are not allowed by the server. Please refer to the Network Access Guide for the supported cipher suites. Both the TLS 1.2 and TLS 1.3 versions of the protocol are supported (RFC5246 / RFC8446) and the use of a widely tested implementation such as OpenSSL is recommended. Client certificates are not needed. Server certificates may be checked by the client with the following root certificates, but this is optional: **Simulation and Production (ETI)** "DigiCert Global Root CA": https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem **Simulation and Production (FIX LF)** "DigiCert Global Root G2": https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem In addition to the above certificates, which are currently in use, to ensure the seamless transition to new server certificates in the future, the following certificate should also be added as part of any regular trust store. "DigiCert TLS RSA4096 Root G5": https://cacerts.digicert.com/DigiCertTLSRSA4096RootG5.crt.pem Any potential intermediate certificates will be delivered by the server during the TLS handshake process. After a successful TLS handshake application data may be exchanged via the TLS tunnel according to the existing ETI/FIX LF protocol.

Question 1.13:	Are there plans to encrypt more services, e.g. Reference Data, Market Data, T7-GUIs, CRE, CUE...?
Answer:	Currently there are no immediate plans to encrypt any further services

Question 1.14:	Why did you decide to support TLS 1.2 instead of TLS 1.3. Are there plans to offer TLS 1.3 in addition, or instead of, TLS 1.2?
Answer:	Deutsche Börse now supports both the TLS 1.2 and TLS 1.3 in parallel.

Question 1.15:	Can OpenSSL be used for password encryption? If yes, is there a minimum version?
Answer:	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). Deutsche Börse has provided an example python script "STEP" (Sample Tool ETI Password Encryption) which provides a sample implementation of the ETI password encryption on the client side. The script can be downloaded from the Eurex website under the following link. Support > Initiatives & Releases > T7 Release 11.1 > Trading Interfaces

Question 1.16:	For ETI HF sessions in colocation is it only required to encrypt the password field in the session and user logon and are new message templates required?
Answer:	Only password encryption is required for ETI HF sessions. Password encryption can also now be used for ETI LF sessions in the Equinix FR2 co-location facility. Please refer to the ETI manual (for more ETI details)

Question 1.17:	Two failover IP addresses are provided for FIX LF but only one interface gets a valid SSL answer, will this change?
Answer:	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 behaviour.

Question 1.18:	Can we add a simple Stunnel installation with TLS 1.2 to encrypt our current sessions?
Answer:	Deutsche Börse does not have any of its own information or experience regarding the usage of Stunnel but has been informed by some participants that Stunnel is used with their application.

Question 1.19:	What type of encryption should be used in the event of a split location.
Answer:	For participants with ETI LF sessions configured for use in split locations (i.e. two connections terminating in different locations which share the same member LAN), the use of payload encryption is still mandatory.

Question 1.20:	Do you have an example how to encrypt the password for ETI password encryption
Answer:	Yes, please refer to the “STEP” tool which you will find on the Eurex website here: Support > Initiatives & Releases > T7 Release 11.1 > Trading Interfaces

Question 1.21:	When implementing TLS or password encryption, is it a mandatory requirement to also change the session password?
Answer:	The implementation of TLS or password encryption does not require a specific password change. However, Deutsche Börse strongly recommends a password change as a prudent precautionary measure to ensure the highest level of security, especially for those sessions whose original passwords may never have been changed.

2. Co-Location and Equinix FR2

In this section questions relating to the Co-Location and Equinix FR2 facility are addressed.

Question 2.1:	Are HF/PS sessions only going to be allowed in Equinix FR2 or will co-location facilities for example in the UK also be allowed HF/PS sessions?
Answer:	No, HF/PS Sessions for Production will only be permitted in the Equinix FR2 facility and this will be the only form of co-location. HF simulation sessions and sessions used during the Disaster Recovery scenario will still be possible outside of Equinix FR2.

Question 2.2:	Will only ETI LF sessions outside of Equinix FR2 have to make use of TLS?
Answer:	Yes, the TLS connectivity option only applies to ETI LF sessions outside of the FR2 facility. and all FIX LF sessions regardless of their location.

Question 2.3:	If installations in Equinix FR2 are not public network, is it still necessary to use TLS for FIX LF sessions?
Answer:	Yes, all FIX LF sessions are affected and must be adapted to use TLS payload encryption.

Question 2.4:	What happens to existing HF sessions which are currently used from outside of the Equinix FR2 facility?
Answer:	To continue using existing HF sessions the appropriate MIC or 10 GB connectivity option must be ordered within FR2. Alternatively existing HF sessions must be cancelled and replaced with LF sessions.

Question 2.5:	Why do FIX LF and ETI LF sessions always have to be encrypted, even in the Equinix FR2 co-location facility?
Answer:	Based on discussions with Trading Participants and to provide the maximum level of flexibility and compatibility with the implementation of the security requirements, Deutsche Börse now offers Trading Participants the flexibility to choose between the implementation of payload encryption or password encryption for ETI LF sessions within the Equinix FR2 co-location facility. FIX LF sessions have to use payload encryption regardless of the source location.

3. Certificates

In this section questions relating to the usage of certificates are addressed.

Question 3.1:	Is a certificate required either self-created or a server certificate from the exchange?
Answer:	Customer certificates won't be required. For ETI LF sessions, please refer to chapter 5.1 of the Enhanced Trading Interface Manual for Release 11.1 available on the Eurex / Xetra website. The ETI interface currently provides two connectivity options. In addition to the existing unencrypted connections via the familiar port, the ETI interface also provides TLS v1.2 and TLS v1.3 encrypted payload connections for LF sessions via a dedicated TLS port. After the TCP connect to the TLS port, a TLS handshake must be initiated by the client and the following communication is then TLS encrypted. Please refer to the Network Access Guide for the list of the TLS ports and supported cipher-suites. The session and application layer are not affected. An LF session can only be logged in once (either plain text or TLS encrypted payload) at the same point in time. The server certificate is issued by a DigiCert intermediate certificate, which is provided by the server together with its own certificate during the TLS handshake. The following step is optional: If verification of the ETI LF (gateway) server certificate is desired, the DigiCert CA root certificates have to be stored in an accessible trust store. The FIX LF interface also provides two connectivity options shown in chapter 4.1.1 of the FIX LF manual for Release 11.1 available on the Eurex / Xetra website. The FIX LF interface also provides two connectivity options: - the (current) FIX via the existing port – resulting in plain text payload - the (new) FIXS via the TLS port – resulting in TLS encrypted payload. FIX LF sessions can only establish connections to one of these ports at the same point in time. The session and application layers are not affected by the connectivity option chosen. FIXS implements a transport layer encryption using simple TLS (version 1.2/1.3) with certificate validation of server with CA (DigiCert) pinning. Please refer to the Network Access Guide for the list of supported cipher-suites

Question 3.2:	What kind of certificates are required for **payload encryption** and where can they be obtained?
Answer:	For FIX LF/ ETI LF payload encryption the DBAG servers present a valid certificate signed by DigiCert CA during connection. The client application should verify the validity of the presented server certificate however the verification of the certificate is optional. DBAG will update the server certificate regularly before expiry and client applications are not affected by these updates.

Question 3.3:	What kind of certificates are required for ETI **password encryption** and where can they be obtained?
Answer:	There is no certificate required for ETI password encryption. The password encryption must be done using DBAG's public RSA key which must be downloaded in advance from the Eurex or Xetra website. Separate public RSA keys are provided for the simulation and production environments. DBAG will update their public RSA key regularly before expiry. Participants can either download the updated public RSA key again from the Eurex or Xetra website or take it from ETI's session response message. Please refer to the ETI Manual (chapter 5.3.3. Password Encryption) for more details.

Question 3.4:	Does the DigiCert certificate have a validity date and what about the server / intermediate certificates?
Answer:	The DigiCert root certificates ("DigiCert Global Root CA" and "DigiCert Global Root G2") have a validity date (10/Nov/2031 and 15/Jan/2038) - see https://www.digicert.com/kb/digicert-root-certificates.htm for more details. The server and the intermediate certificate are provided by the server during TLS handshake.