Eurex Circular 099/18

Common Report Engine (CRE) security upgrade

Summary

In order to ensure reliable and secure communication with the infrastructure of the Common Report Engine (CRE), the SSH Key Exchange Algorithms, Ciphers and MACs have been updated accordingly.

In this circular, the supported versions of Key Exchange Algorithms, Ciphers and MACs are listed. These versions can be used and tested immediately to establish a successful connection to the CRE.

Please be aware that outdated Key Exchange Algorithms, Ciphers and MAC , which are not listed in this circular, will be decommissioned with effect from **10 March 2019**.

Therefore, we would like to encourage our Trading Participants to review and adapt their IT systems accordingly before **10 March 2019** in order to ensure a smooth transition when decommissioning takes place.

Attachments:

- none

⚠ Action required

Date: 17 December 2018

Recipients:
All Trading Participants of Eurex Deutschland and Vendors

Authorized by: Michael Peters

Target group:
- IT/System Administration

Contact:
Your Technical Key Account Manager, via your VIP number or e-mail: cts@deutsche-boerse.com

Common Report Engine (CRE) security upgrade

Only the following Key Exchange Algorithms, Ciphers, and MACs will be supported by the CRE:

Key Exchange Algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Ciphers:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

MACs:

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256

For documentation about accessing the Common Report Engine, please refer to the Common Report Engine User Guide published on the Eurex website www.eurexchange.com under the path:

Technology > T7 Trading architecture > System documentation > Release 7.0 > Eurex Reports

If you have any questions or need further information please contact your Technical Key Account Manger, via your VIP number, or e-mail cts@deutsche-boerse.com.

17 December 2018