Eurex Clearing Circular 107/18

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Please be aware that outdated Key Exchange Algorithms, Ciphers and MACs, which are not listed in this circular, will be decommissioned with effect from **10 March 2019**.

Therefore, we would like to encourage our Clearing Members 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

Date: 17 December 2018

Recipients: All Clearing Members, Non-Clearing Members and Registered Customers of Eurex Clearing AG and Vendors

Authorized by:
Heike Eckert

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 Clearing website www.eurexclearing.com under the following path:

Technology > Eurex Clearing's C7 > System documentation > Eurex Reports

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

17 December 2018