SFTP reporting instructions for transaction reporting

1 Generation of SFTP Keys

The creation and management of SFTP keys used in transaction reporting is the responsibility of the reporter.

The reporter can create credentials individually for either the testing or production environment, or for both environments using a single form. When the connection is created for both environments using one form, the same SSH key is used for both environments.

1. The reporter sends the form containing, among other things, the public key of the SSH key pair they generated to the Financial Supervisory Authority (FIN-FSA).
2. The FIN-FSA sends the reporter the SFTP credentials and passwords via secure email.

2 Instructions/Information on Secure Email

The FIN-FSA provides the reporter with the username and password for the reporting system's SFTP service via secure email. A code is required to open the secure email, which the FIN-FSA sends via SMS to the contact person specified in the form.

The process of creating the credentials is partly manual. It can therefore take several days for a secure email to arrive, depending on the number of reporters registered.

3 Instructions for Generating the Reporter's Public Key

Generating a key pair may require support from an IT expert. The key pair can be generated, for example, using a freely downloadable program from the internet such as PuTTY Key Generator.

The reporter creates a key pair consisting of a public and a private key. The public key is saved, and the reporter sends the content of the public key through the form to the FIN-FSA. The private key is kept only by the reporter and is never shared.

The private part of the key (private key) should be stored with the same care as a password, for example, securely in a password manager, and avoid sharing it through unprotected methods such as email. The private key is used in the SFTP client software for securely sending and receiving files.

The key must meet the following requirements:

- The key must be of the RSA (SSH2) type.
- The key length must be 4096 bits or longer.
- The key must be provided in OPENSSH format.

An example of how the public key should look is included as an attachment to this guide.

4 Contact Information

Please feel free to contact us if you encounter any uncertainties related to the process/instructions or have any other questions.

For technical inquiries, please contact: trs-support@fiva.fi
For questions related to transaction reporting, please contact: kaupparapor-tointi@finanssivalvonta.fi

Attachment

Example_SSH_key.txt