Documentation for SFTP

SFTP (which stands for SSH File Transfer Protocol as well as for Secure File Transfer Protocol) is a file transmission protocol which encrypts data transmitted to a special FTP server. This is made possible by the Secure Shell Network Protocol (SSH) which allows two computers to communicate via a secure, authenticated, and encrypted channel within an unsecured network.

Functionality

As it is our goal to offer you a trustworthy way of providing your data to us, we have set up an SFTP server which will allow you to transmit your data in the form of a csv file. The following parameters must thereby be taken into consideration.

Delivery of MiFID data:

prod.import.wmgruppe.de (194.187.221.157) and/or
test.import.wmgruppe.de (194.187.221.156)[1]
Protocol / Port / Limitation: SFTP, tcp/2222, ssh-key only

***Delivery of data for the* Prospectus Regulation**

prod.pvo.import.wmgruppe.de = 194.187.221.154
test.pvo.import.wmgruppe.de=194.187.221.155
Protokoll / Port / Einschränkung: SFTP, tcp/2222, ssh-key only

Please ensure that **port 2222 is not blocked by your firewall**. To upload your data, you will need to enter (for authorization purposes) your login data that will be provided to you by WM. In contrast to a conventional FTP connection, the SFTP connection encrypts your password as soon as you enter and transmit it. This helps ensure that your data (as well as your password) is transmitted securely at any given moment.

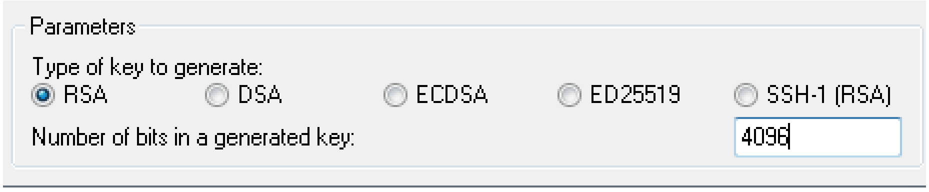
In order to implement the connection, it is important that you first create a so-called key pair. One way of doing this is by using the PuTTYgen program, which is available on the internet free of charge. In the next section we will explain how a key pair that comprises a public key as well as a private key can be generated.

The advantage of an authentication via a public key is that it not only provides more security, but also allows a single sign-on which means that once you have logged-in successfully you do not need to log-in anew every time you want to transmit your data to our SFTP server.

[1] As you are already an existing customer, we activated you for our production. Although, we do not believe that a test is necessary, it could be initiated beforehand if requested.

Generating a New Key Pair

To generate a new key pair, you have to select the correct parameters within the list of options presented by the PuTTYgen program. The key length (4096 bits) and the key type ((RSA, SSH-2, ECDSA or ED25519) must be determined as well.



Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 4096

You must then press the "Generate" button to create the key pair. Note: After you have activated the "Generate" button, please move your mouse cursor so that the program can determine the corresponding random values which will then be used for creating the new key. Having done so, you can then add a comment (optional) as well as a pass phrase (mandatory). This will allow your private key to be encrypted and saved securely on your hard disk. Please note that you must determine your passphrase and enter it again, for security purposes, in the next line.

Further Actions

After you have generated your key pair, please **send your public key to** wm-schnittstellenanbindung@wmdaten.de. As we will use this key to enable the files to which you have hitherto transmitted your data, it is important to state, which data types you plan to submit to WM:

1. EMT (opposite of Standard Format)
2. Standard Format (Standard in German speaking countries)
    a. Target market
    b. Target market funds
    c. Cost transparency
    d. Cost transparency funds
    e. Leverage identifier
    f. Cost transparency ex post
3. PRIIPs
4. Prospectus Regulation