**Introduction**

The SFTP protocol is used to connect to the data exchange service. It operates on top of the SSH protocol, a login + secret key pair is used for authorization.

To get access to the service, you need to generate a key, the public part of the key must be sent to your supervising manager in the TransContainer, in turn, the manager must send an Application to the Service Desk for the “OS and DBMS Support” command, which must specify the **name of the depot** and the **public key**.

 **Connection Settings**

Protocol: SFTP

Server: trcont1.edifact.ru

Port: 22

Username: Your login issued by your manager

Path to the folder to data transfer: /files

**Key Generation in Windows OS**

To generate a key, you need to download and install the full PuTTY package (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html)



Install the entire contents of the package.

Run puttygen.exe (default path "C:\Program Files\PuTTY\puttygen.exe")



Optimal Security Settings:

 Type of Generated Key: ECDSA

Key Length: 384 or 521



Click the Generate button. To fill in the field, you need to rotate the mouse until the progress bar is completely filled



As a result, we get the Generated Key:



You may set a password to ensure protection.

To get access, you need to send to your manager all the text from the field

Public key for pasting into OpenSSH authorized\_keys file



Save the received key by clicking on the Save private key button





Connecting from Windows OS

To connect to the server, you need to install the WinSCP software (<https://winscp.net/eng/download.php>)



You need to run pagent (included in the PuTTY package) to connect. It is located in the tray



Add the key generated in the previous step in the window



Run WinSCP



Click Enter

In the left window you will see the “Files” folder



All documents for exchange must be placed in it, after copying and updating the contents of the directory, the files will disappear, this indicates a successful data transfer.

**Key Generation in Linux OS (MAC, Unix, etc)**

ssh-keygen utility: which is included in the openssh-client package.

To generate a key of the required strength, run the command under the user with whom you are going to transfer data.

ssh-keygen -t ecdsa -b 521