



Sommaire

1. Introduction.....	2
2. Pre-requisites	2
3. Procedure	2
3.1. Accepted Key type and format	2
3.2. Generating the key pair using PuttyGen	2
3.3. Next Step	5
3.4. Troubleshooting	5



1. Introduction

Our SFTP Server **XFERCOM.riziv.fgov.be** requires the use of a Key pair to authenticate the users

Following this procedure, you will be able to generate a key pair.

- The Public key part will be installed on our server.
- The Private key part will be used in your client software (Filezilla, Winscp,..)

2. Pre-requisites

In order to complete this procedure, you will need the following :

- Putty Key Generator software (PuttyGen) . It's part of the Putty software bundle
You can download it from <https://www.puttygen.com/download-putty>

3. Procedure

3.1. Accepted Key type and format

The accepted key types are the following :

- RSA 2048 / 4096
- DSA 2048 / 4096
- ECDSA NISTP256/NISTP384/NISTP521 (**preferred**)

The format of the key generated by putty is PPK.

Note: The PPK format is accepted by FileZilla Client and WinSCP.

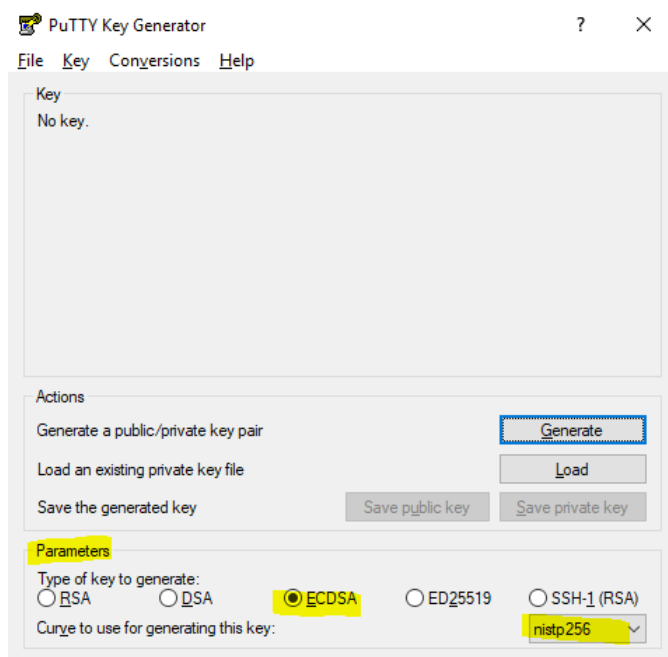
If you are using another SFTP client, you should convert it to the desired format (ie: pem)

3.2. Generating the key pair using PuttyGen

- Start PuttyGen

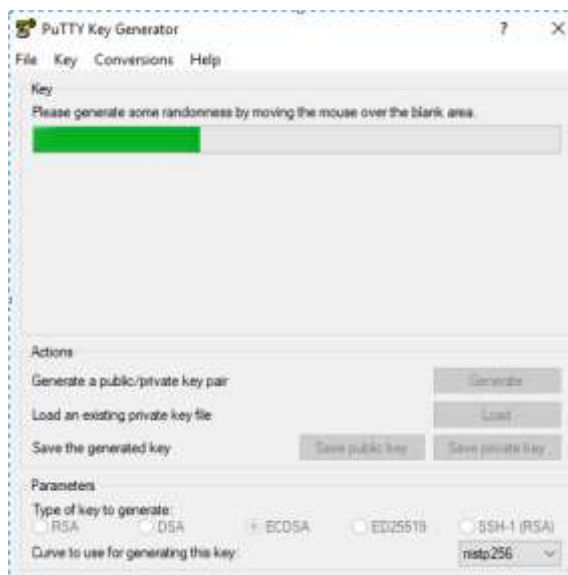


XFERCOM SFTP Server - Procedure Generating a key pair using PUTTYGEN



- From Parameters, select the key format
- Click on **Generate**

Note: You have to move your mouse over the blank area for the key to be generated



- Once your key is generated, the following screen is displayed



XFERCOM SFTP Server - Procedure Generating a key pair using PUTTYGEN

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ecdsa-sha2-nistp256  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEo7Zn5nmHV6  
CnBe1+10EZuGgodxlenot8hLus1ljsUAWiDAP+HHOZ3XRdDj  
+pJkfBHU/AYvi80lYG8GUUZr9E= ecdsa-key-20190405
```

Key fingerprint: ecdsa-sha2-nistp256 256 4d:e5:2c:e1:c9:12:04:00:85:94:e5:74:21:z

Key comment: ecdsa-key-20190405

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:
☐ RSA ☐ DSA ☒ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Curve to use for generating this key: nistp256

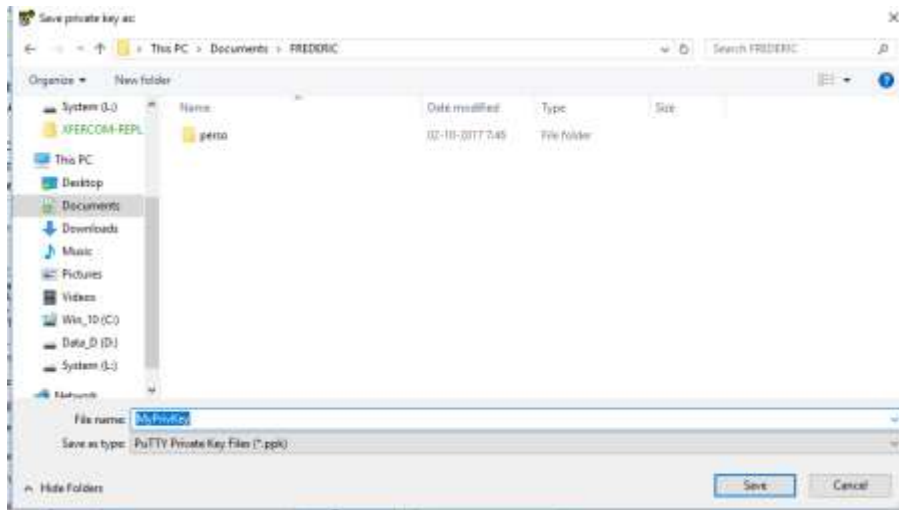
- Save you public key by clicking on **Save Public Key** button.
- enter a key passphrase and confirm it before clicking on **Save Private Key** button

Key fingerprint: ecdsa-sha2-nistp256 256 4d:e5:2c:e1:c9:12:04:00:85:94:e5:74:21:z

Key comment: ecdsa-key-20190405

Key passphrase:

Confirm passphrase:



- Click on Save
- You have now generated a key pair.

3.3. Next Step

- The **public Key** will have to be sent to RIZIV Network&Telecom by mail at network.ict@riziv-inami.fgov.be
- Your private key will be used on your client computer to establish the connection to our SFTP Server. **Please keep it in a safe place.**

Important notes :

If the private key is lost or compromised, you won't be able to connect to the xfercom server anymore. In this case, please contact RIZIV as soon as possible.

3.4. Troubleshooting

- Please refer to your ICT Service first
- If you are not able to solve your problem, please contact our Service desk
 - helpdesk@riziv-inami.fgov.be
 - Phone : 02/739.74.74

You should provide a screenshot of your configuration and a screenshot of the error.