Fileset upload to the JePPIX MPW web service

The MPW web service is an infrastructure that guarantees the revision control and secure upload of your PIC design (encrypted file exchange) and allows for easy updates from the Foundry throughout the entire manufacturing process. You either already have an account, or you will receive your account details when the administrative work has been done.

After your design is completed, you have to upload it to the JePPIX MPW server so it will become available to the foundry for download. Your design consists of a *fileset* that has all the necessary files. It is a *single zip file*. You have to check the foundry design manual for details. Typically, your mask design software will generate the proper files for you.

When needed, the fileset can be encrypted before you upload. The instructions are found below.

Uploading an encrypted fileset to the MPW server

There are two ways for generating an encrypted design fileset.

1. **RECOMMENDED.** Use a public key encryption method. We support only PGP/GnuPG. With this method you encrypt your zipped fileset with the public key of the foundry (which can be found here). This method is very secure and easy to use, but more difficult to set up the first time. The advantage is that no private keys have to be exchanged.

2. When generating the zip file, you can protect it with a password. Check the manual of the zip software that you use to find out how to do this. This password then has to be shared with the foundry by other private means. We **DO NOT RECOMMEND** this method as its employment is not secure in all cases. If by any reason you are not allowed to use PGP/GnuPG, then you can use the password-protected zip file method.

PGP/GPG/GnuPG

We briefly explain how to use this method for Windows, Linux and macOS.

Windows

For windows we recommend using *gpg4win*. The procedure is:

Install software and run once to generate your key pair:

- Download gpg4win from http://gpg4win.org and install with default options.
- Run "Kleopatra" as suggested and create your openPGP key pair.
- Import the foundry's public key (https://www.jeppix.eu/mpw-services/get-started/mpw-server/).

Encrypt a fileset:

- Choose sign/encrypt and select your zipped mask fileset.
- Select encrypt for yourself (so you can decrypt the file yourself if needed)
- Select encrypt for the foundry.
- Click sign/encrypt.
- Upload the resulting `fileset.zip.gpg` file to the MPW server.

In case you want to receive encrypted files, others (e.g. the foundries) need to have your *public* key, so they can use it to encrypt the file they want to send to you. Your public key can be safely shared with anyone. **WARNING: Never send your *private* key.**

Generate your public key:

- In Kleopatra, right click on your key, then click ‘Export Certificates…’ and save the key to a text file *mypublickey*.asc.
- Send this file to the foundry by email or include it in your fileset.

Linux

Install software and run once to generate your key pair:

- Use your package manager to install the package *gpg* or *gnupg*. There are also graphical interfaces available, but here we only show the use of the command line tool.
- Run “gpg --gen-key” to generate your key pair.
- Run “gpg --import *pubkey*” to import the foundry’s public key (https://www.jeppix.eu/mpw-services/get-started/mpw-server/).

Encrypt a fileset:

- Run “gpg --encrypt *fileset*.zip”
- Upload the resulting *fileset*.zip.gpg file to the MPW server.

In case you want to receive encrypted files, others (e.g. the foundries) need to have your *public* key, so they can use it to encrypt the file they want to send to you. Your public key can be safely shared with anyone. **WARNING: Never send your *private* key.**

Generate your public key:

- Run “gpg --armor --export > *mypublickey*.asc”.
- Send this file to the foundry by email or include it in your fileset.

macOS

Download GPG Suite from https://gpgtools.org
Extensive tutorials and FAQ are available https://gpgtools.tenderapp.com/kb/how-to
In case you want to receive encrypted files, others (e.g. the foundries) need to have your *public* key, so they can use it to encrypt the file they want to send to you. Your public key can be safely shared with anyone. **WARNING: Never send your *private* key.**