



Hosting a Web Key Directory

Ideally a Web Key Directory will be created and maintained through a Web Key Service but organisations or individuals may want to just host a Web Key Directory without a Web Key Service.:

Requirements

- A web server that provides https with a trusted certificate.
- A client machine with python and pyme installed (debian package python-pyme)
- The script: generate-openpgpkey-hu  (in the Mercurial repository "wkd-tools" )

Usage

You can either export all the keys in your keyring which belong to a domain or provide an explicit keyring containing the keys you want to publish.

The call:

```
./generate-openpgpkey-hu example.com hu
```

Will create a directory called hu containing all the keys with @example.com mail addresses.

If there are multiple valid keys for a user in your keyring this command will error out. In that case you can prepare a keyring with only the keys you want to publish.

e.g.:

```
gpg --export 94A5C9A03C2FE5CA3B095D8E1FDF723CF462B6B1 | \  
gpg --no-default-keyring --keyring ./wkd-keyring.gpg --import
```


And then provide that keyring to generate-openpgpkey-hu:

```
./generate-openpgpkey-hu example.com hu wkd-keyring.gpg
```

Publishing

The hu directory has to be published on your server as `https://example.com/.well-known/openpgpkey/hu/`

On your server create the according directory and set the permissions according to your system.

This example Makefile  automates the hu directory generation and publishing. Edit the variables at the top of the makefile to your RSYNC_TARGET The KEYRING variable is optional and can be empty.