My GPG Key is now available via Web Key Directory (WKD)

Date:	2022-12-29
modified:	2022-12-29
tags:	GPG, GnuPG, WKD, Web Key Directory
description:	Why and how I published my GPG public key via WKD direct mode
category:	Misc
slug:	my-gpg-key-is-now-available-via-web-key-directory-wkd
Author:	Dominik Wombacher
lang:	en
transid:	my-gpg-key-is-now-available-via-web-key-directory-wkd
Status:	published

First of all, what's **WKD** and what's the benefit using it? It's an easy way to retrieve GPG keys based on a given E-Mail address. It improves the user experience without leveraging any keyserver infrastructure. And that's exactly why I decided to make my key available via WKD, I think the whole keyserver concept is broken and I want to support a decentralized approach that gives the user control of his data.

So how to get it working? In a Nutshell, your public key has to be available in binary format at a specific URL on your Domain. There are multiple ways to achieve that, I decided to use Direct mode and just to export my key, name it appropriately, created the necessary folders and upload it to my webserver.

So far you could, and still can, find my latest GPG public key on my Contact page, you can now also retrieve it via *gpg* or other applications which support WKD, for example *Thunderbird*. For my mail address **dominik@wombacher.cc**, the WKD URL is `https://wombacher.cc/.well-known/openpgpkey/hu/i4spe47w9w9i1wncq7tpum5m4b81bko9`, the last part is the hash of my username **dominik** and the actual public key file.

There is a nice online tool available to verify if the setup is correct.

I had to do two other, minor, things to get all tests passed. 1/Creating an empty file called **policy** in the folder `/.well-known/openpgpkey/`, 2/sending a CORS header via nginx:

```
location /.well-known/openpgpkey/ {
  add_header Access-Control-Allow-Origin *;
}
```

Afterwards everything was fine and my key available via WKD:

```
Direct: key: https://wombacher.cc/.well-known/openpgpkey/hu/i4spe47w9w9i1wncq7tpum5m4b81bko9?l=dominik
Direct: found key: A6FB74CC95114AA977FFD04ACDDD24A5C0758945
Direct: Key contains correct User ID: Dominik Wombacher <dominik@wombacher.cc>
Direct: CORS header is correctly set up
Direct: Policy file is present
```

I think WKD is a really nice approach and solves the problems that came up by using keyservers, there are already lot of mail provider and applications which support it, so I guess that's the future of GPG key distribution.

Kudos to kuketz-blog.de (german) (Archive: [1]) and wiki.gnupg.org (Archive: [1], [2]), my main sources to understand and setup WKD.