WKD and WKS for PGP

Joost van Baal-Ilić <joostvb@debian.org>

DebConf23, sept 2023

thank you noodles for the pgp intro on monday morning.

pgp can be used to sign and encrypt files and email, so that people can be sure the file or message comes from the person who claims so, and the sender can be sure only the right recipient can read it.

about as old as debian

keyserver network: a way to find pgp keys of other people, and to publish your key.

in 2010: SKS Keyserver Network Attack
then: Web Key Directory and Web Key Service

```
gpg --locate-keys foobar@debian.org
```

2019: https://dkg.fifthhorseman.net/blog/wkd-for-debian.org.html

used by @debian.org, @kernel.org, @gentoo.org and others. ask your email provider to offer it too (and/or consider joining debian)