Putting Taiwan on the Kernel.org Keysigning Map

蔡鎮宇 Tsai, Chen-Yu <wens@csie.org>

蔡鎮宇 Tsai, Chen-Yu

- Embedded Linux hobbyist since 2011
  - Mainly focused on Allwinner SoC support
  - Kernel support co-maintainer since 2015/10
  - Kernel.org account holder since 2017/04

- Software engineer at CloudMosa, Inc.
  - Based in Taipei, Taiwan
  - Writes tools to manage Linux servers

Overview

- PGP
- PGP in Open Source Development
- Getting your PGP key signed
- Kernel.org Keysigning Map
- Kernel.org Accounts
- Helping Others

PGP

- Encryption program
  - OpenPGP standard
  - GnuPG
- Encrypt and/or sign data
- Verify signed data

PGP Keys

- Asymmetric public/private key pairs
- Identity
  - UID = full name + email
- Usage
  - [C]ertify
  - [S]ignature
  - [E]ncryption
  - [A]uthentication

PGP in Open Source Development

- Signature verification
  - Tarballs
  - Emails
  - Git tags
  - Git commits

Signed Tarballs

- Separate signature file
  - `X.asc` or `X.sign`

- `gpg2 --verify X.asc`
  - Much like `md5sum` or `sha256sum`

Signed Emails

- `signature.asc` attachment
- Requires email client support

Signed Emails (Mutt)

```
[-- Begin signature information --]
Problem signature from: KeyID B0591588A496E5D16E037A636F7F4A3D8CFEAA53
                created: Mon Mar 19 08:04:29 2018
Can't verify due to a missing key or certificate
[-- End signature information --]
```

Signed Emails (Mutt)

```
[-- Begin signature information --]
Good signature from: Mark Brown <broonie@sirena.org.uk>
                aka: Mark Brown <broonie@debian.org>
                aka: Mark Brown <broonie@kernel.org>
                aka: Mark Brown <broonie@linaro.org>
                aka: Mark Brown <Mark.Brown@linaro.org>
                aka: Mark Brown <broonie@tardis.ed.ac.uk>
            created: Thu May 17 15:09:11 2018
WARNING: It is NOT certain that the key belongs to the person named as shown above
Fingerprint: 3F25 68AA C269 98F9 E813  A1C5 C3F4 36CA 30F5 D8EB
[-- End signature information --]

[-- The following data is signed --]
...
[-- End of signed data --]
```

Signed Git Tags

- Git tags can be signed
  - `` `git tag -s` ``
- Pull request tags can be verified
  - `` `git verify-tag` ``

- Ref: Kernel Maintainer PGP guide

Finding Others' Public Keys

- `gpg --locate-keys <email>`
  - Uses web key directory by default
- `gpg --search-keys <email>`
  - Checks key server for matching keys
  - Asks user to select from a list

Trust in PGP

- Decentralized trust model
  - Direct trust
  - Web of Trust
  - Trust on First Use (TOFU)

Web of Trust

- Complicated and hard to maintain
- Key Signatures
- Validity and Trust
  - Validity (full, marginal, unknown)
  - Trust settings (ultimate, complete, marginal)

Trust on First Use (TOFU)

- SSH-like
- Defaults to marginally trusted
- GPG issues warning if it sees conflicting key/UID pairs
  - User intervention required / intended

Verifying Keys

- Check fingerprint against known source
  - Kernel.org lists public key fingerprints for
    - Linus Torvalds
    - Greg Kroah-Hartman
  - Hosted via HTTPS
  - OS packages
- PGP pathfinder
  - Multiple trust paths from trusted person

What About Maintainers?

- Signing tags for pull requests
- Signing pull requests or other emails
- Opening a kernel.org account
- Participating in kernel.org web-of-trust
  - Getting your PGP key signed by other kernel developers

Getting Your PGP Key Signed

- Local key holders
  - Kernel.org Keysigning map
- Attend Conferences
- Video Conference with people you already know

Kernel.org Keysigning Map

Kernel.org Keysigning Map

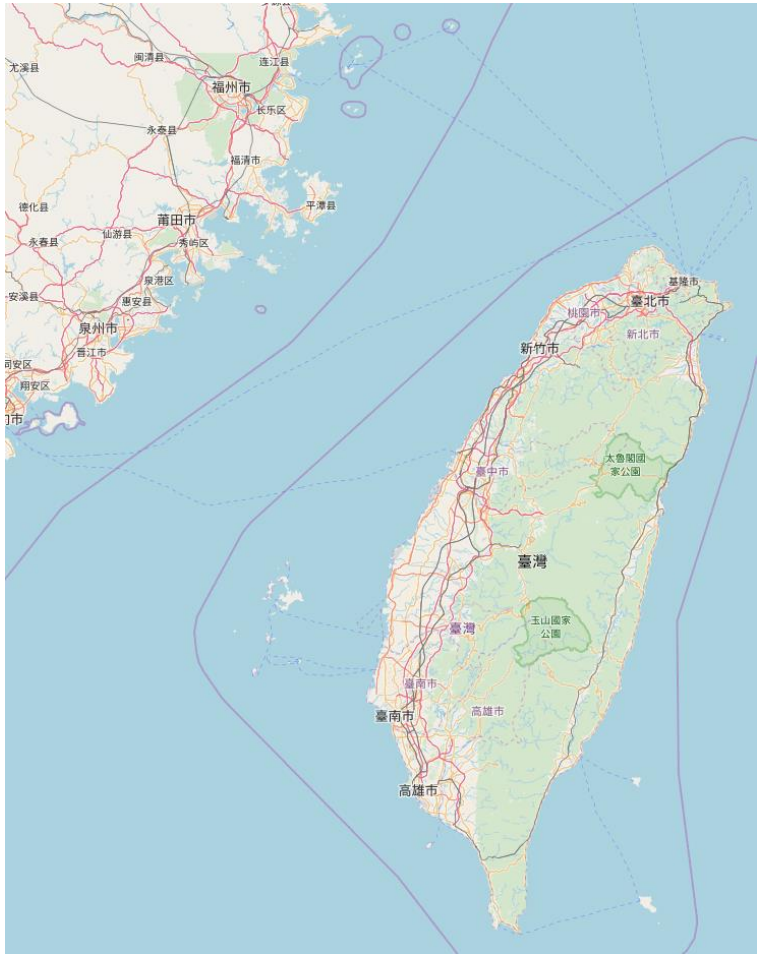
- Public kernel.org account holders
  - Very small subset of kernel developers
  - Willing to sign other people's PGP keys
    - Sometimes w/ caveats

Dirk Hohndel

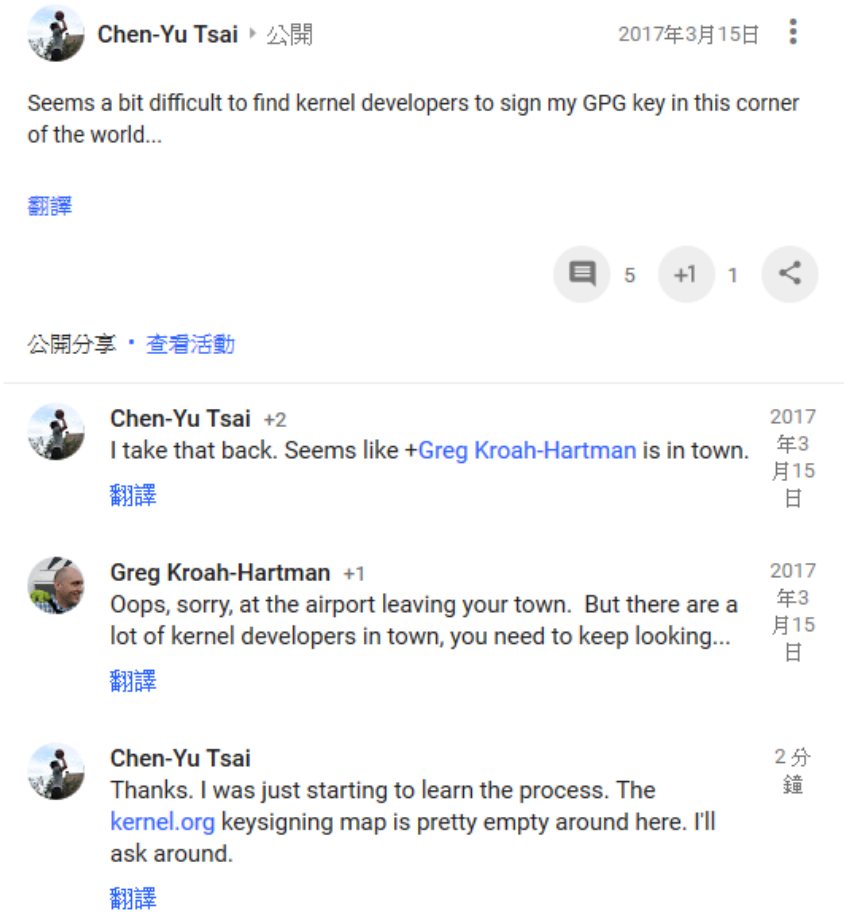
Contact: dirk@hohndel.org
Key stats: DF188DFE

I only sign keys of people that I have had some interactions with - just seeing a passport is not sufficient, I need to be able to recognize you based on prior conversation.

Keysigning Map – Taiwan (then)



Locals.....



Chen-Yu Tsai ▸ 公開 2017年3月15日

Seems a bit difficult to find kernel developers to sign my GPG key in this corner of the world...

翻譯

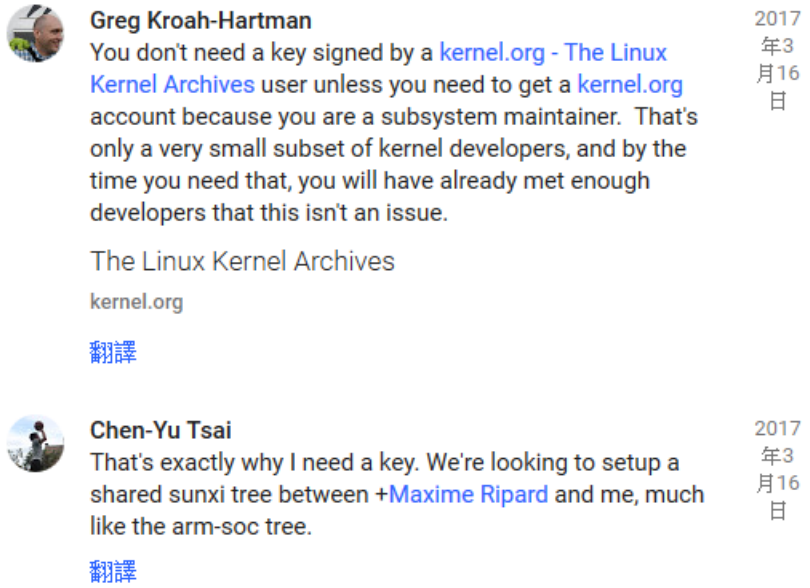
5 +1 1

公開分享 · 查看活動

Chen-Yu Tsai +2 2017年3月15日
I take that back. Seems like +Greg Kroah-Hartman is in town.
翻譯

Greg Kroah-Hartman +1 2017年3月15日
Oops, sorry, at the airport leaving your town. But there are a lot of kernel developers in town, you need to keep looking...
翻譯

Chen-Yu Tsai 2分鐘
Thanks. I was just starting to learn the process. The kernel.org keysigning map is pretty empty around here. I'll ask around.
翻譯



Greg Kroah-Hartman 2017年3月16日
You don't need a key signed by a kernel.org - The Linux Kernel Archives user unless you need to get a kernel.org account because you are a subsystem maintainer. That's only a very small subset of kernel developers, and by the time you need that, you will have already met enough developers that this isn't an issue.

The Linux Kernel Archives
kernel.org

翻譯

Chen-Yu Tsai 2017年3月16日
That's exactly why I need a key. We're looking to setup a shared sunxi tree between +Maxime Ripard and me, much like the arm-soc tree.
翻譯

https://plus.google.com/u/0/115208016645517532827/posts/NwVyr59xJwB

Conferences

- Open Source Summit
  - NA, JP, CH, EU
- Embedded Linux Conference
  - Co-located with OSS in NA and EU
- Linaro Connect

Video Conferencing

- People you already know and trust
  - Best if you have actually met

Kernel.org Accounts

- For Linux kernel maintainers or high-profile developers [1]
- Hosted git repository
- @kernel.org email address
- https://korg.wiki.kernel.org/userdoc/accounts

[1] https://www.kernel.org/category/faq.html

Helping Others

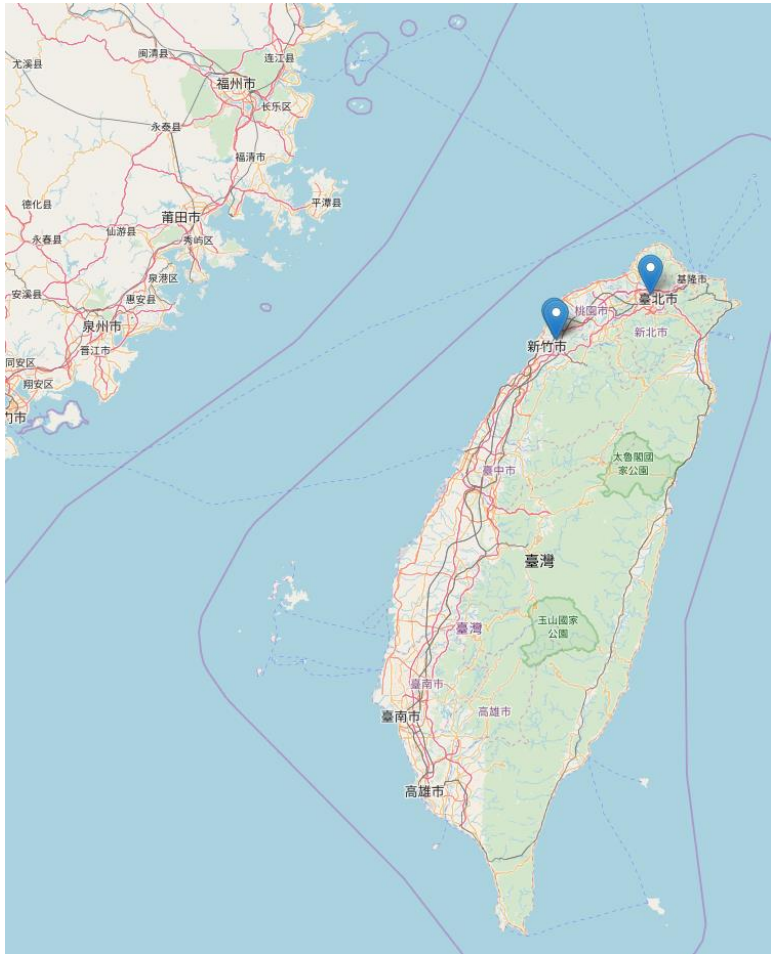
- Greentime Hu from Andes Tech.
  - Upstreaming nds32 port
  - Cross-signed key
  - Helped with kernel.org account and typical git repo workflow (fixes/next/PR)

Helping Others

- Helping new kernel developers adapt
  - Patch submission process
  - Unspoken rules and preferences
  - Common feedback
- Helping Taiwanese IC design houses
  - Upstreaming is different from in-house development

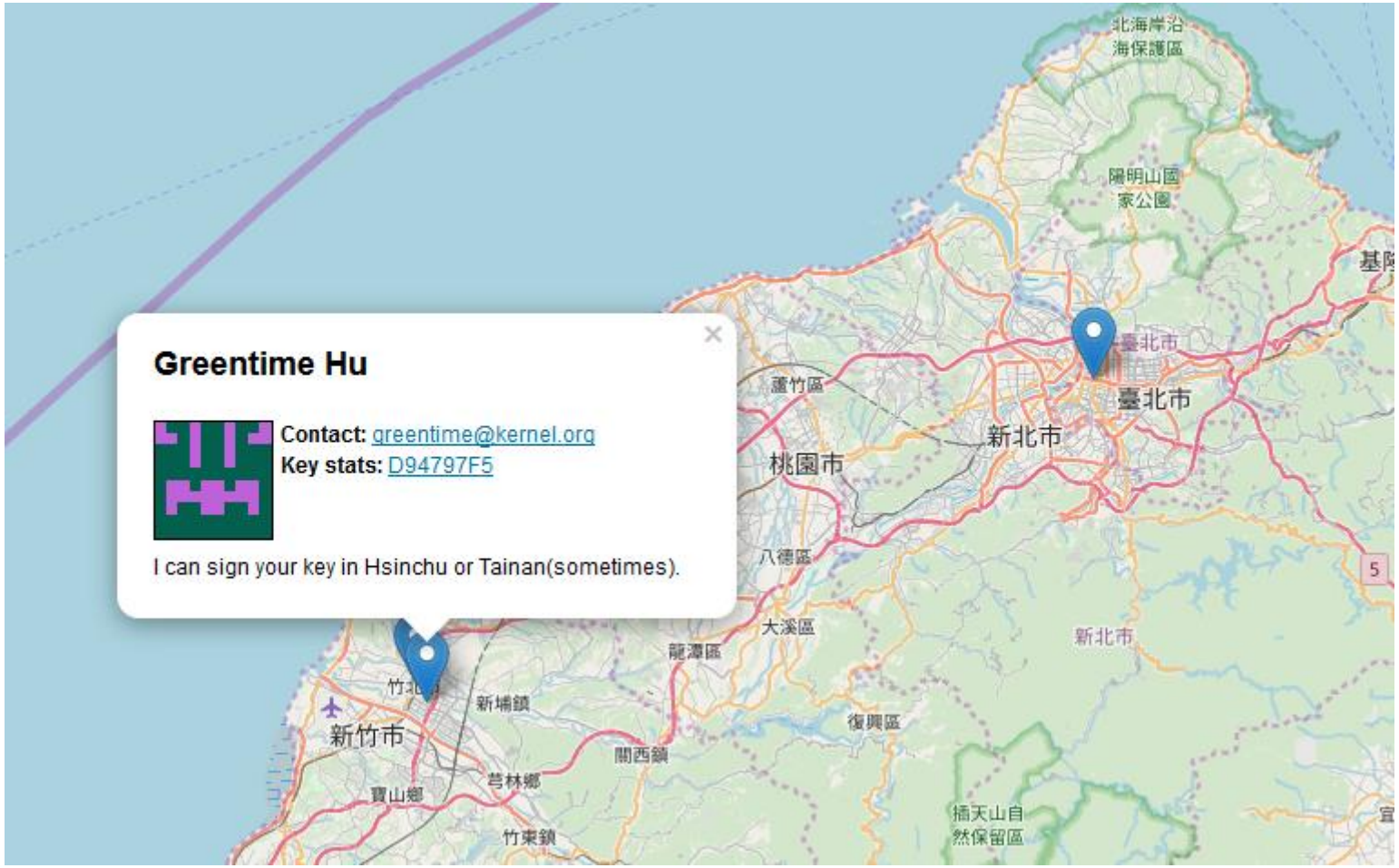
Kernel.org Keysigning Map

Keysigning Map - Taiwan

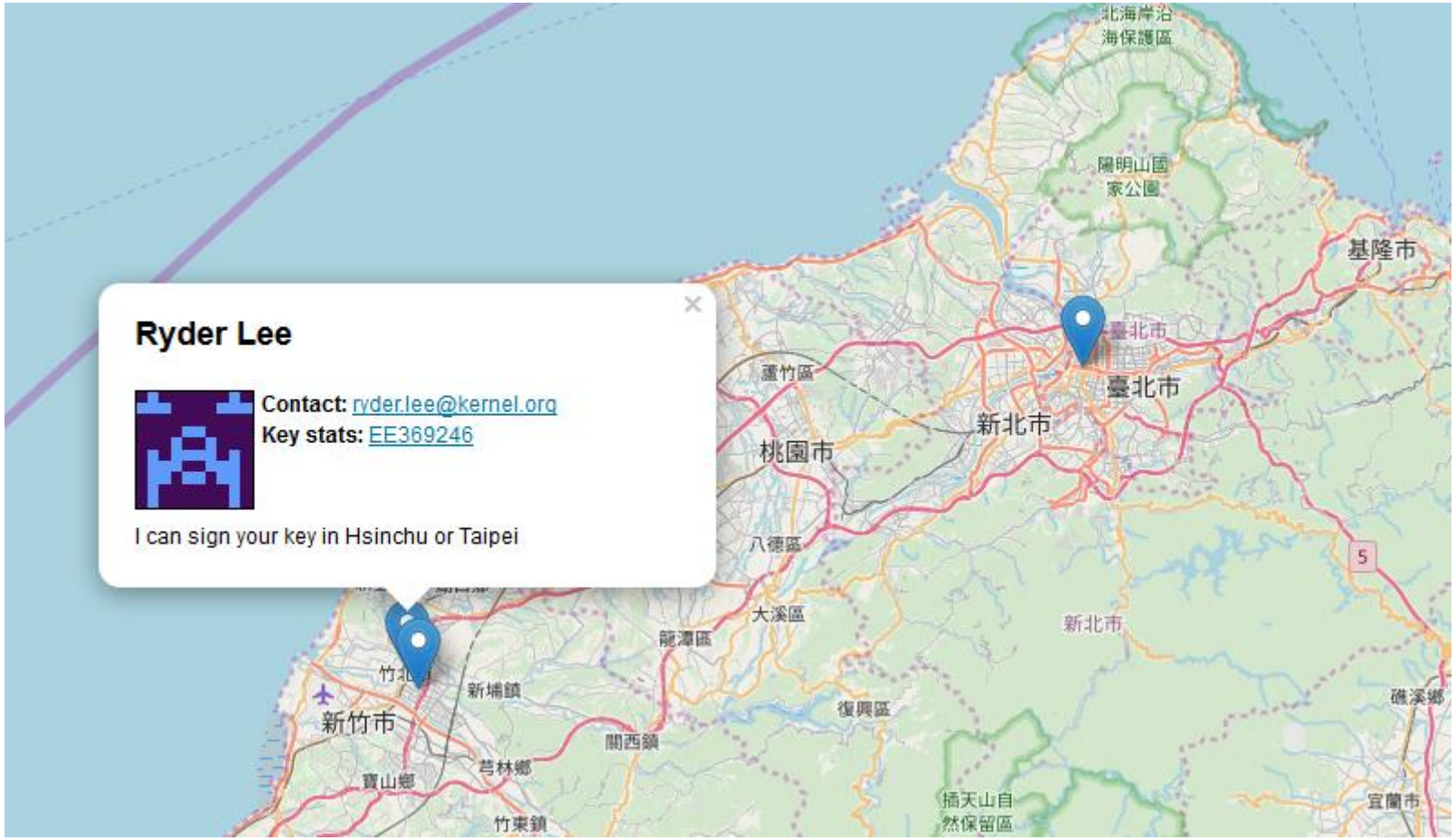


Keysigning Map – Taiwan #1

Keysigning Map – Taiwan #2



Keysigning Map – Taiwan #3



Q&A

References

- Kernel Maintainer PGP guide
  - https://www.kernel.org/doc/html/latest/process/maintainer-pgp-guide.html
- Web of Trust
  - https://www.rubin.ch/pgp/weboftrust.en.html
  - https://www.gnupg.org/gph/en/manual/x334.html