In Defence of GnuPG

Key Sovereignty in an Age of Digital Feudalism

Özcan Oğuz

ozcan@oyd.org.tr

1st February 2026, Brussels

FOSDEM 2026, Decentralized Internet and Privacy Devroom

Who am I?

- A daily and regular user of GnuPG
- Founding member of Free Software Association in Turkey and Hackerspace Istanbul
- Co-author of the 600+ page e-book "ÖYD Security Guide"

Every few years a cycle comes again…

“GPG is dead”

- Too hard to use
- Too old
- Too complicated for "normal" users
- Too nerdy
- Replaced by *$NEW_APP*

...or sometimes...

- You cannot secure your e-mail anyway
- Only nerds use it so it's lame
- Web of Trust is broken so just leave it
- I installed {some_app_from_google_play} now I am secure already
- GnuPG has `$STH_IRRELEVANT` issue so use modern crypto
- I have nothing to hide, nobody needs it
- ...

What is actually assumed?

- Users are stupid and lazy
- Security must be invisible
- Freedom is optional
- If it’s not perfect, it’s worthless
- Someone else should manage identity

This is not a UX debate

This is about power

Who controls:

- keys,
- identity,
- trust,
- revocation,
- continuity?

Digital feudalism

- Infrastructure owned by few
- Value produced by many
- Power justified by “convenience”
- Users treated as incapable

“You don’t need to understand”

is the new serfdom

- “There’s an app for that”
- “Just trust the platform”
- “We’ll handle the keys”

This is not empowerment.

GPG comes from a different era

- Hacker culture
- General-purpose tools
- User responsibility
- Self-determination

Not:

- App stores
- Walled gardens
- Invisible cryptography

GnuPG *is* hard

So were computers

- Complexity didn’t disappear
- It was **hidden**
- At the cost of:
  - Right to fix
  - User autonomy
  - Inspectability

Encryption followed the same path

- Capital avoided user-controlled crypto
- Now sells “privacy” as a product
- Fear is profitable
- Control remains centralized

“Just use Signal”

Signal is excellent… and limited

- Forward secrecy ✔
- Usability ✔
- Walled garden ✖
- No federation ✖
- App-bound identity ✖

“Just use Matrix”

- Open protocol ✔
- Federation ✔
- Still:
  - Instant messaging only
  - Purpose-specific crypto
  - Not a general identity system

The Pattern

Most modern tools are:

- Single-purpose
- Provider-mediated
- Opaque key management
- Symmetric communication
- Non-portable identity

What GnuPG actually gives you?

Total key ownership

You can:

- Export
- Revoke
- Extend
- Backup
- Print
- Hold in your hand
- Go offline forever

Identity without permission

- No central authority
- No mandatory server
- No app owner
- No phone number
- No account

You are your own CA.

Web of Trust

Uncomfortable, not broken

- Trust is social
- Trust is explicit
- Trust is revocable
- Trust requires effort

Freedom always does.

“Forward secrecy is missing”

True.

But:

- GnuPG protects **identity**
- Not just sessions
- Long term verifiability matters

Threat models matter

- Not everyone fights the NSA
- Corporations, employers, states exist
- "OpenPGP has no post-quantum" is no longer true
- Perfect security vs. durable access

One key, many uses

- E-mail
- IM encryption
- Files or backups
- Digital signature
- Packages
- SSH authentication
- Code signing
- Passwords
- Offline communication
- Login to your computer
- Verify websites

Single source of concern

- One identity
- One backup strategy
- One trust root
- Hardware tokens supported

This is simplicity.

GPG is not an app

- Not platform bound
- Not provider bound
- Not server bound
- Not revocable by policy

“E-mail is dead”

It is not. Say it again in the room K.4.201

- Thunderbird integrates it
- Even Enigmail is still alive
- Keyservers keep growing
- WKD just works
- GNU/Linux packages use GnuPG
- Servers rely on it

“I just want to install an app”

- Installing an app cannot give you privacy on its own
- Privacy and security is a human matter, not software
- But still you can try OpenKeychain!
- Use "Password Store" to manage your passwords
- Start using GnuPG is way more easier than opening an account in X

“GnuPG requires maintenance constantly”

- Sometimes, but it is not a bug
- Security requires an ordinary doubt
- Being alerted on privacy is better than vulnerability caused by laxity
- Yet, it requires less maintenance than banks require you to change your password every 3 months with a different one

The real risk

Calling GnuPG “too hard” means accepting:

> *Users should not control their own identity*

GPG is not obsolete.

It is inconvenient because freedom is inconvenient.

GnuPG is an idea...

- No server to ban
- No company to pressure
- No app store to delist
- No switch to flip

...and ideas are bulletproof

GnuPG have survived:

- Cryptowars
- Political pressure
- User abandonment
- Black propaganda

It will outlive apps.

Thank You!

ozcan@oyd.org.tr
https://ooguz.dev
0x2D33E2BD3D975818
oo@5222.de (XMPP+OMEMO)