GnuPG 2.1 Explained for Everyone

Niibe {Yutaka, Hitoe, Hiroshi, Ayumi}

John Paul Adrian Glaubitz

DEBCONF17
MONTRÉAL · CANADA

Contents

- GPG 2.1 is **not** beta software
- Everyone relies on GnuPG
- Debian and GnuPG
- 3 GPG Branches
- What's New in 2.1?
- Components: DEMO

GPG 2.1 is not beta

- It's new, but more than two years
- Many people misunderstand it's beta
- It's stable enough (<= 2.1.22)
  - I'm not sure for 2.1.23???
- 2.2 will be soonish

Everyone relies on GnuPG

- Somehow ... Directly / Indirectly
- Because:
  - Servers running GNU/Linux
  - In GNU/Linux distro, "release" has integrity check
    - See apt-secure(8)
  - Package upload to archive has integrity check...
  - ... where developers are authenticated by GPG

Debian and GnuPG (1)

- Congratulation Debian "Stretch"!
- Thank you Debian for migration to GPG 2.1!

Debian and GnuPG (2)

- Debian community is heavy user of GnuPG
- Debian is important for GnuPG, too
- GnuPG migration to 2.1 has been going well
  - Kudos to:
    - Debian GnuPG Maintainers: `dkg` and `eric`
    - All Debian Developers

GPG in Debian Stretch

- Package `gnupg` is now GPG 2.1!
  - `gpg` means GPG 2.1
- If GPG 1.4 is needed, install `gnupg1` package
  - The command is available as `gpg1`

3 Branches of GPG

GnuPG evolved:

- GPG 1.4 "classic"
- GPG 2.0 "stable"
- GPG 2.1 "modern"

GPG 1.4 "classic"

- Single binary executable
- v3 (PGP 2) keys are supported

GPG 2.0 "stable"

- Executable + Libraries
- gpg-agent as passphrase cache agent
- End-of-Life: 2017-12-31

GPG 2.1 "mordern"

- Executables + Libraries
- Private key is under control of gpg-agent
- dirmngr is now GnuPG proper

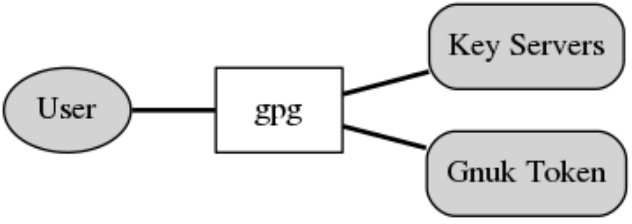
What's New in 2.1? (1)

- New features
  - ECC support
  - ToFU trust model
  - experimental: WKD, g13
- Major Changes
  - Keybox format for public key
  - libgcrypt native private key format

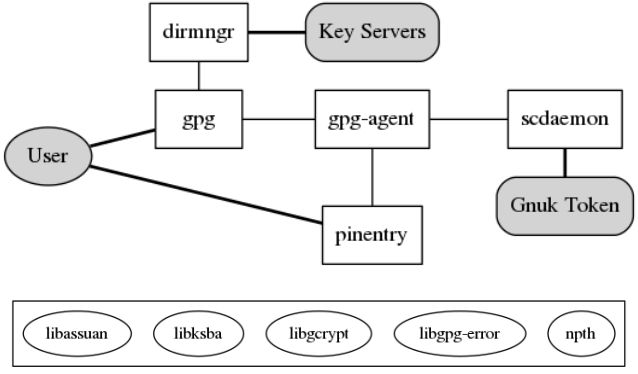
What's New in 2.1? (2)

- Architectural change
  - `gpg-agent` does private key operations
  - `dirmngr` is now part of GnuPG

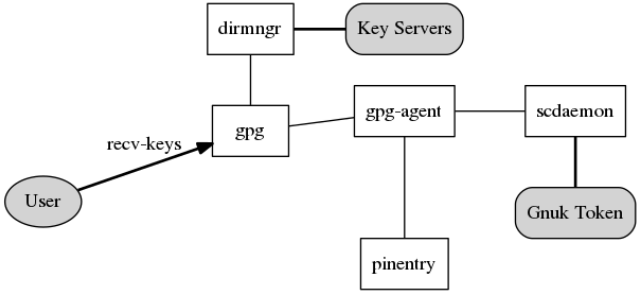
Architectural change (1)



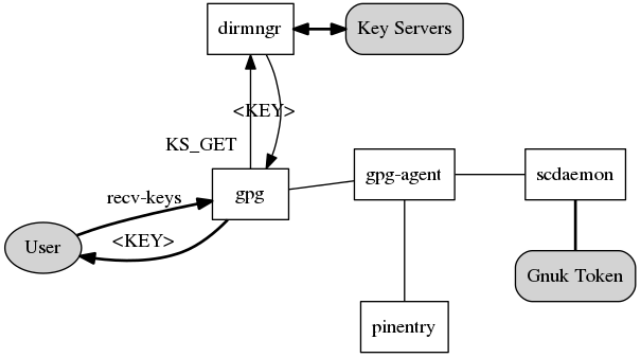
Architectural change (2)



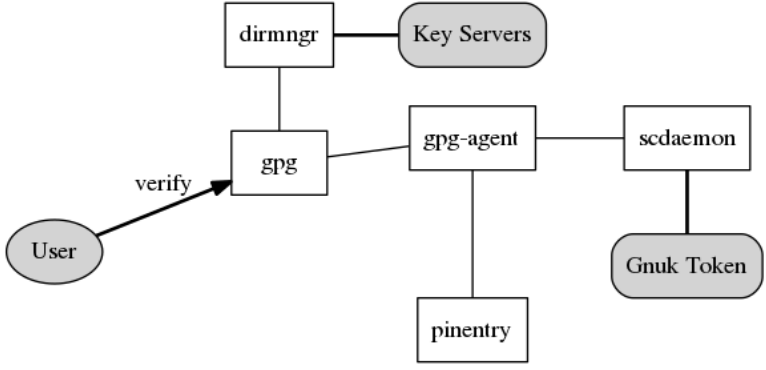
RECV-KEYS



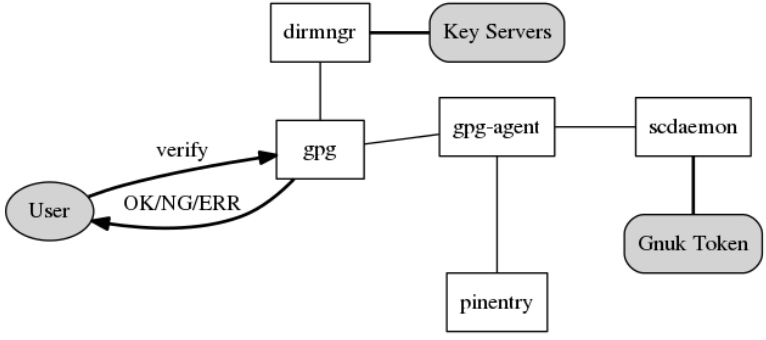
RECV-KEYS



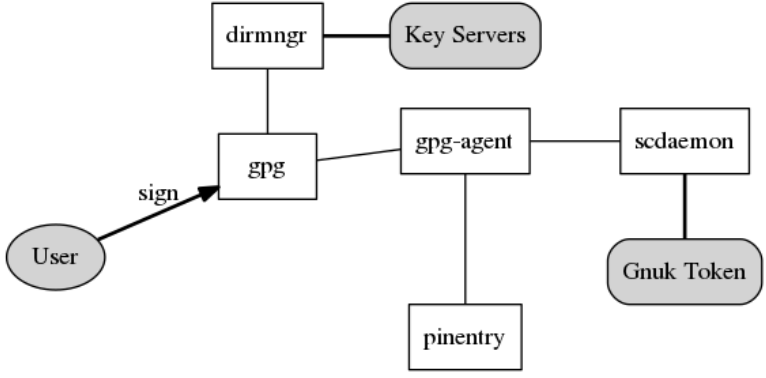
VERIFY



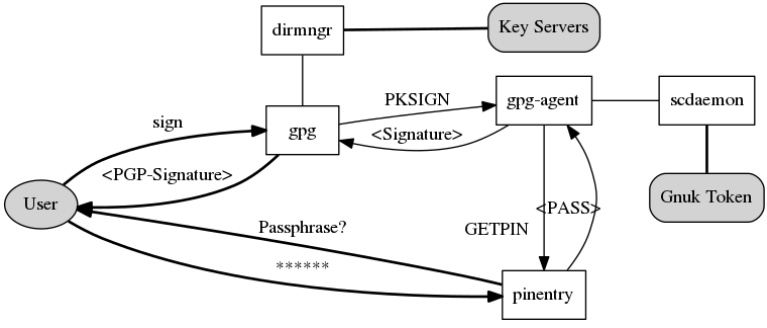
VERIFY



SIGN



SIGN



Summary

- Everyone relies on GnuPG
- GPG 2.1 is for **everyone**
- Package `gnupg` is now GPG 2.1!
- Components:
  - `gpg`, `gpg-agent`, `dirmngr`, `pinentry`
  - `scdaemon`
- GPG evolved and evolves

Enjoy GPG!

GnuPG Fundraising Rally:

https://www.gnupg.org/donate/

DEBCONF17
MONTRÉAL · CANADA

Questions?

Q1: Which is older Debian or GnuPG?

DEBCONF17
MONTRÉAL · CANADA

Questions?

Q1: Which is older Debian or GnuPG?

A1: Debian is older!

DEBCONF17
MONTRÉAL · CANADA