GnuPG Packaging in Debian

Eric Dorland & Daniel Kahn Gillmor
On behalf of pkg-gnupg-maint
DebConf15
Heidelberg
Much appreciation!

- NIIBE Yutaka
- Daniel Leidert
- Thijs Kinkhorst
- Cyril Brulebois
- Peter Eisentraut
- Sune Vuorela
- Andreas Rönnquist
- David Prévot
- Jose Carlos Garcia Sogo
- Andreas Metzler
- Upstreams!!!
- Debian Security Team
- ...
Since last year...

- pkg-gnupg moved packaging to git

- Adopted:
  - gnupg2
  - libassuan
  - pinentry
  - gpgme
Since last year...

• GnuPG is reproducible!

• Version 2.1 in experimental for many months
  – In unstable for many hours!

• Dependency cleanup for default minimal server install
  – gnupg2→gnupg-agent→pinentry→GUI libs
  – (missed jessie, sorry)
We want 2.1

(For Debian in particular)

- Updated key storage (speed)
- Elliptic curve crypto (strength)
- Daemonized/split processes (system isolation)
- Removal of old/unused algorithms (simplicity)
Elliptic Curve Crypto

- New set of algorithms
  - NIST curves (p256, p384, p521)
  - Ed25519/Curve25519
  - Maybe goldilocks448 in the future?
- We need widespread encrypt/verify support before we start deploying them
- Key generation deliberately hidden behind --expert for now
2.1 Transition

- 2.0 goes away
  - (not co-installable with 2.1)
- 1.4 becomes gnupg1 (as /usr/bin/gpg1)
  - Most people won't have gnupg1 installed.
  - Who still needs it?
    - some corner cases dealing with old/weak crypto
  - We don't have to support it in everyone's gpg
Why a hard cutover?

- Too many moving parts already
- We want to focus our efforts
- Handle modern crypto by default
- Discourage older crypto
Transition plan

- Cutover will happen in experimental first (gnupg and gnupg2)
- We'll mail debian-devel-announce
- Mailing to reverse dependencies?

- Please test and report!
udebs (d-i)

- gpgv-udeb is needed in debian-installer
- gpgv-win32-udeb also for installer
- gnupg-udeb might go away
  - partman-crypto no longer uses it
Pinentry

- Upstream is transitioning to rely on more system libraries and toolkits
  - GNOME3
  - QT5
- Giving up on locked memory
  - Swap vs. hibernation
- Better integration, usability
Divergence from upstream

• Tuning of defaults
  – Too many fiddly “guides for GnuPG”
  – More guides should just say “Use up-to-date GnuPG”
    • We may diverge from upstream in testing/unstable to reduce text in sensible guides
    • If Debian users see interop problems, we may back out divergence before hitting stable

• Linux-specific hardening
  – e.g. prctl(SET_DUMPABLE, 0);

• Contributions back upstream where possible
Desktop Integration

• We had an agent “hijacking” conflict for too long
  – GNOME Keyring vs. GnuPG Agent
• The fight is over, and everyone won
  – Our heroes:
    • Neal Wallfield
    • Yumma Sato
    • Stef Walter
    • Michael Biebl
• Can we improve integration further?
Possible Futures

• autopkgtest
• Streamlining some known best practices
  – Smartcards
  – Offline primary keys
• Work with language teams for bindings?
  – assuan
  – gpgme
• UI/UX review
  – If it's not easy, people won't use it
• Other GUIs?
Other contributions

• Do you have ideas for improving GnuPG in Debian?
Questions?

Please get in touch!

- `<pkg-gnupg-maint@lists.alioth.debian.org>`
- `#debian-gnupg on irc.oftc.net`
- `https://wiki.debian.org/Teams/GnuPG/`