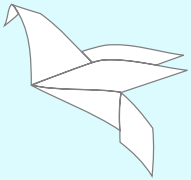
Sequoia-PGP, OpenPGP v5, Authentication, and Debian

DebConf 22, Kosovo

Justus Winter <justus@sequoia-pgp.org>

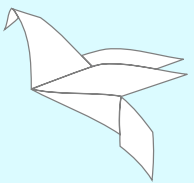
2022-07-18

https://sequoia-pgp.org/



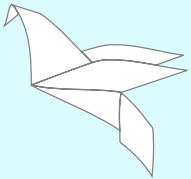
Outline

1. Sequoia-PGP
   - Introduction
   - Status
   - Notable Projects
2. OpenPGP v5
   - Getting Unstuck
   - Highlights
3. Authentication
4. And Debian
5. The Wrap



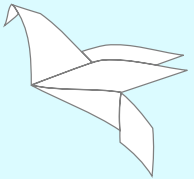
What is Sequoia-PGP?

- A 5 year old OpenPGP implementation in Rust
- Motivation
  - GnuPG is hard to modify
  - Code and API grew organically over 24 years
  - Lack of tests
  - Tight component coupling
  - Many developers unsatisfied with GnuPG's API
- Why Rust?
  - Rust is a memory-safe systems language
  - Terrific tool for the job!
  - Challenges
    - Packaging
    - Platform support



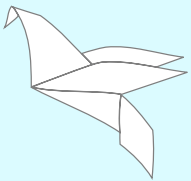
Social Goals

- Inclusive environment
- Free Software
- Community-centered project
  - Development in the open
  - Collaborating with other OpenPGP implementors
  - Working with application developers



Technical Goals

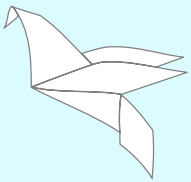
- First-class library API, second-class command-line interface
- Friendly API
  - Magnificent documentation
- Unopinionated low-level API & opinionated high-level API
- Loose component coupling
- Tests, tests, tests, ...
- All modern platforms
- Tight integration with host systems
  - Key stores, TPM, OpenPGP cards



The Team

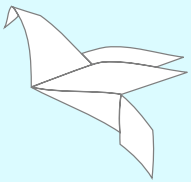
Figure: The gang. Neal H. Walfield, Kai Michaelis, Justus Winter, Nora Widdecke, Wiktor Kwapisiewicz, Heiko Schaefer, Lars Wirzenius.

- Founded in 2017 by Neal, Kai, and me
  - Former GnuPG developers, ~2.5 yrs experience each
- Currently six people
- Funding
  - p≡p foundation (vast majority)
  - NLnet (individual projects)
  - Wau Holland Stiftung
  - private donations
  - Actively looking to diversify our funding!



Status

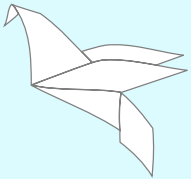
- sequoia-openpgp (core library)
  - Released 1.0 in December of 2020
  - Stable API for 1.5 yrs
  - Some warts, but held up fine
- sq (command-line frontend)
  - Stateless interface, useful for OpenPGP users
  - Scriptable interface is coming (Lars' NLnet project)
- Certificate store is coming (Nora's NLnet project)
- Secret key store is coming (Neal's NLnet project)
  - OpenPGP card support (Heiko's project)
  - TPM support (Wiktor's past NLnet project)
- Network services (HKP, WKD, soon DANE)
- Miscellaneous
  - Ports, e.g. rpm-sequoia
  - GnuPG interoperability
  - Lots of ideas and prototypes



OpenPGP CA

Figure: https://openpgp-ca.org: Tirelessly approving (cert, userid)-bindings since 2019.

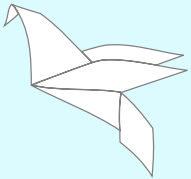
- Manages OpenPGP certs in organizations
- Allows O(1) authentication for users
- Shifts authentication to the CA admin
- Uses existing WoT mechanisms
- Federated: scoped trust signatures bridge organization boundaries



Hagrid aka keys.openpgp.org

Figure: Thought of, spec'ed out, written, maintained, developed, and run by these people (in reverse-alphabetical order): Vincent Breitmoser, Nora, Neal, Kai, Justus, dkg.

- Hagrid (the software) powers keys.openpgp.org (the service)
- Earliest spin-off
- Requires user's consent to publish user ids
  - Consent can be revoked, information unpublished
- GDPR-compliant, hosted in the EU
- Formalizing governance by forming a board
- WKD-as-a-service: can host WKD for your domain



OpenPGP Interoperability Test Suite

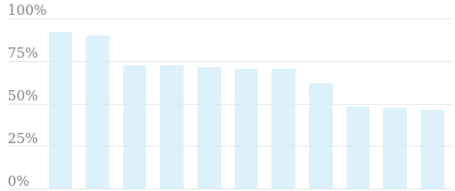
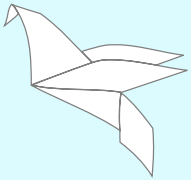


Figure: Test results from https://tests.sequoia-pgp.org.

- Tests interoperability, capabilities, correctness, robustness
- Uses the Stateless OpenPGP Command-Line Interface (SOP, https://gitlab.com/dkg/openpgp-stateless-cli)
- Circa 98 tests
- Around 1100 test vectors
- Found at least 92 bugs in 10 implementations
- Benchmarks coming



Sequoia RNP Octopus

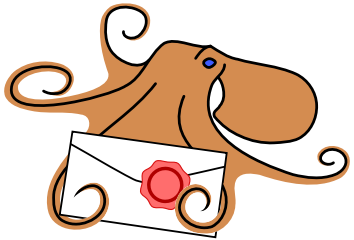
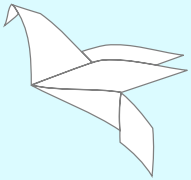


Figure: This project is called the Octopus, because octopuses can fit themselves in [unusual places, like the RNP-shaped hole in Thunderbird].

- Thunderbird uses RNP, replaced Enigmail+GnuPG
- Thunderbird doesn't use Enigmail's OpenPGP abstraction
  $\rightarrow$ reimplementation of RNP's API
- GnuPG integration, WoT, Parcimonie,
  no surreptitious forwarding, all of Sequoia



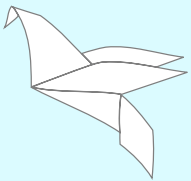
Sequoia GnuPG Chameleon

Figure: If you squint, it looks like gpg.

- Many existing programs use GnuPG
  - Direct invocation, GPGME, libraries like GMime
- Infeasible to port them all
- No migration path for users and developers
- Vendor lock-in

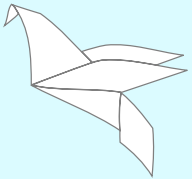
  $\rightarrow$ reimplementation of the gpg CLI
- Also gpgv, and apt already works with that :)

```
% ls -l /usr/bin/gpgv
lrwxrwxrwx 1 root root 22 Jun 22 11:20 /usr/bin/gpgv -> gpgv.sequoia-chameleon*
```



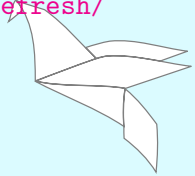
Outline

1. Sequoia-PGP
   - Introduction
   - Status
   - Notable Projects
2. OpenPGP v5
   - Getting Unstuck
   - Highlights
3. Authentication
4. And Debian
5. The Wrap



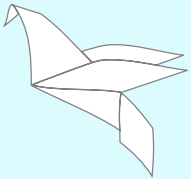
OpenPGP v5

- RFC4880 is from 2007
- RFC4880bis was never ratified
- IETF OpenPGP Working Group formed a Design Team
  - Stephen Farrell, dkg, Paul Wouters, Jeffrey Lau, NIIBE, Daniel Huigens, and me
  - Weekly, 1h meetings since 2021-07-16
  - Weekly notes on openpgp-dt@
  - Discussion and wordsmithing in Gitlab
  - Sporadic discussions on openpgp-dt@
- Draft 6 is in WG Last Call:
  https://datatracker.ietf.org/doc/draft-ietf-openpgp-crypto-refresh/
- Session at IETF
  - (preliminary) Friday, July 29, 2022, 14:00-16:00 UTC
- RFC9760 may come later this year



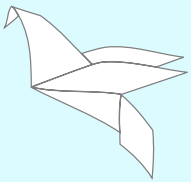
OpenPGP v5 Highlights

- Authenticated Encryption
  - Revised SEIPDv2 replaces AEDv1 from RFC4880bis
  - Per-message keys derived from session keys
    - Key separation
    - You can always encrypt your replies
  - Also protects SKESKs, secret key material
- Argon2
- Non-deterministic signatures
- Padding
- Simplified certificate metadata
- v5 fingerprints: SHA2-256
  - 32 octets, 64 hex digits
  - v5 Key IDs are the left-most 8 octets



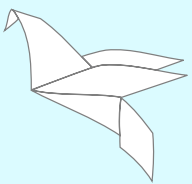
OpenPGP v5 Algorithms

- Public key algorithms
  - MTI: EdDSA and ECDH
  - MAY: ECDSA, RSA
  - out: DSA, ElGamal
- Curves
  - MTI: Ed25519 and "ECDH using Curve25519"
  - SHOULD: Ed448 and X448
  - MAY: Nist and Brainpool curves
- Hash algorithms
  - MTI: SHA2-256
  - in: SHA{2,3}-*
  - out: MD5, SHA-1, and RIPE-MD/160
- Ciphers
  - MTI: AES-128
  - in: Camellia-*
  - out (archive exception): IDEA, TripleDES, or CAST5
- AEAD modes
  - MTI: OCB
  - in: EAX, GCM (FIPS approved)



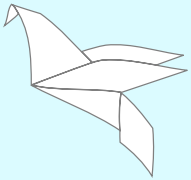
Outline

1. Sequoia-PGP
   - Introduction
   - Status
   - Notable Projects
2. OpenPGP v5
   - Getting Unstuck
   - Highlights
3. Authentication
4. And Debian
5. The Wrap



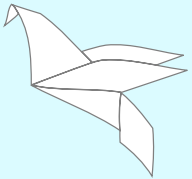
Authentication

- Mapping handles to cryptographic identities
- Essential part of cryptosystem
- Trust models
  - Always trust: no cost, vulnerable to active attackers
  - TOFU: occasional conflict resolution, asymptotic trust (ssh)
  - Delegation: O(1) (centralized: TLS, federated: OpenPGP CA)
  - Fingerprints: O(n)
  - Security numbers: O(n) but worse (p≡p, Signal)
  - Any combination of the above
- Ergonomically, O(n) is like using symmetric crypto!
- Don't ask questions users cannot answer
  → TOFU and/or delegation



Outline

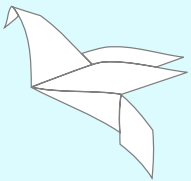
1. Sequoia-PGP
   - Introduction
   - Status
   - Notable Projects
2. OpenPGP v5
   - Getting Unstuck
   - Highlights
3. Authentication
4. And Debian
5. The Wrap



Delegating Authentication

- Done wrong: delegating to random strangers (TLS)
- Done right: delegating to someone aligned with you
- Like Debian's keyring-maint
  - Curated keyrings, like debian-keyring.gpg
  - Would be nice to have cryptographic artifacts
- Anyone can do it, but keyring-maint is in a great position
- With a CA, we can now authenticate all Debian members:

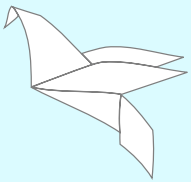
```
$ openpgp-ca ca init -n "Justus' Example Debian CA" debian.org
$ openpgp-ca user import --email ... --key-file ... # for all users
$ openpgp-ca user export > debian.pgp
$ sq-wot -k debian.pgp -r 04F293BD... lookup --email dkg@debian.org
[✓] C29F8A0C... <dkg@debian.org>: fully authenticated (100%)
  ○ 04F293BD... ("Justus' Example Debian CA <openpgp-ca@debian.org>")
  │   certified the following binding on 2022-07-06
  └ C29F8A0C... "<dkg@debian.org>"
```



Bridging Organizational Boundaries

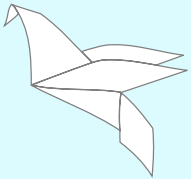
- Bridges are trust signatures between CA certs
- Uni- or bi-directional
- Scoped to the target domain
  $\rightarrow$ no trust necessary, bridge to openpgp-ca@nsa.gov!
- Let's bridge from Debian to Sequoia-PGP:

```
$ openpgp-ca bridge new sequoias-ca.pgp --commit
$ openpgp-ca bridge export > bridges.pgp
$ sq keyring merge debian.pgp bridges.pgp justus.pgp > my-keyring.pgp
$ sq-wot -k my-keyring.pgp -r 04F293BD... lookup --email justus@sequoia-pgp.org
[✓] CBCD8F03... <justus@sequoia-pgp.org>: fully authenticated (100%)
  ○ 04F293BD... ("Justus' Example Debian CA <openpgp-ca@debian.org>")
  │   certified the following certificate on 2022-07-06
  │   as a fully trusted meta-introducer (depth: unconstrained)
  ├ 34F9E4B6... ("OpenPGP CA <openpgp-ca@sequoia-pgp.org>")
  │   certified the following binding on 2022-02-09
  └ CBCD8F03... "<justus@sequoia-pgp.org>"
```



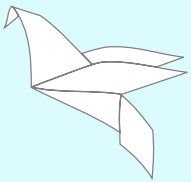
Authorization and Supply Chain Security

- In the future, OpenPGP CA could do authorization, e.g.
  - dkg@debian.org is a "Debian developer"
  - justus@sequoia-pgp.org may sign source distributions
- Then,
  - Monkeysphere could grant access to porter boxes to every "Debian developer"
  - Debian packagers can authenticate source distributions



Wissenswertes Zusammengeschnürt

- Sequoia is improving the OpenPGP ecosystem
- OpenPGP is alive and well
  - Implementations: OpenPGP.js, GopenPGP, PGPainless, RNP, ...
  - Specs: v5, SOP, openpgp-cert-d, WoT
  - Soon: key maintenance, symmetric reencryption, encrypted forwarding
  - OpenPGP Interoperability Test Suite
- Lots of innovative projects
- OpenPGP CA makes the Web of Trust a true grassroot authentication mechanism
  - Don't make every user a CA
  - Instead, let them partially delegate to a CA they trust
  - Provide tooling to run such CAs
  - Finally, bridging organizations adds federation
- Debian, please don't roll your own crypto protocol...



Contact Information & Questions

- https://sequoia-pgp.org
- #sequoia on OFTC
- justus@sequoia-pgp.org
  `CBCD 8F03 0588 653E EDD7 E265 9B7D D433 F254 904A`
- openpgp-ca@sequoia-pgp.org
  `34F9 E4B6 A0A7 0BFE C5AE 4519 8356 989D F197 7575`
  (create a trust signature scoped to sequoia-pgp.org to use:
  gpg –edit-key 8356989DF1977575 ; tsign ; 2 ; 255 ; sequoia-pgp.org)

I'm happy to take your questions!

Find me and talk to me!