Interop Testing v6

Justus Winter <justus@sequoia-pgp.org>

IETF 118, 2023-11-09

https://tests.sequoia-pgp.org

https://tests.sequoia-pgp.org/v6.html

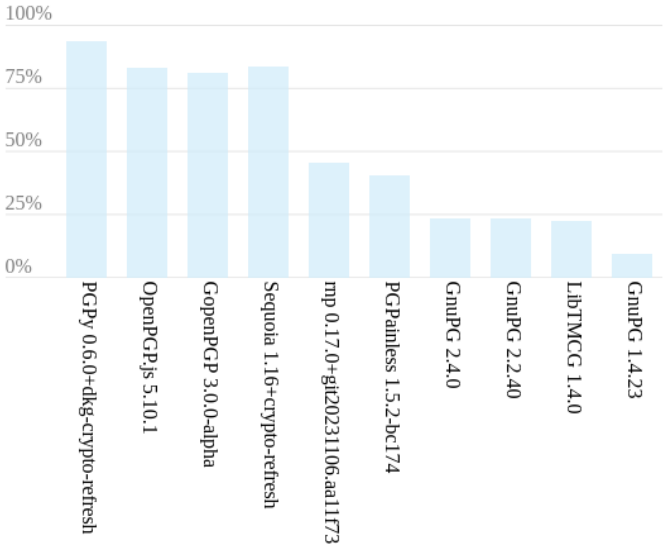
https://sequoia-pgp.org/talks/2023-11-ietf/interop-testing-v6.pdf

Testing the Crypto Refresh!

- interop testing OpenPGP since 2019
- circa 131 tests
- around 1510 test vectors
- found loads of bugs across many different implementations
- includes some v6 tests
  - test vectors from the draft
  - asks implementations to generate v6 keys
- https://tests.sequoia-pgp.org
  - runs all tests
  - enter "v6" in the search bar
- https://tests.sequoia-pgp.org/v6.html
  - happy to test your preview releases
  - runs only v6 tests

Results around IETF116

Results now around IETF118



What can you do?

- suggest tests, write tests, review tests
- help with test suite development and maintenance
- implementers:
  - consider implementing your own SOP frontend
    - if you do, clue me how to build it and keep it up-to-date
    - preferably, get it into Debian
  - do you have a development version? a v6 branch?
  - implement SOP's '–profile'
- get in touch
  https://gitlab.com/sequoia-pgp/openpgp-interoperability-test-suite