Stateless OpenPGP Signature Verification (with gpgv)

IETF 120 Hackathon

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

Stateless OpenPGP CLI

Draft-dkg-openpgp-stateless-cli – useful for test suites and generic implementations

- `sop generate-key “Alice <alice@example.org>” > alice.key`
- `sop extract-cert < alice.key > alice.cert`
- `sop sign alice.key < msg.txt > msg.txt.sig`
- `sop verify msg.txt.sig alice.cert < msg.txt`
- `sop encrypt …`
- `sop decrypt …`
- …

`sopv` – Verification-only subset

- `sop version` (*info about the implementation*)
- `sop verify` (*verify detached signatures*)
- `sop inline-verify` (*verify inline signatures*)

  Succeeds if at least one signature is valid.

gpgv – GnuPG's verification-only

- Succeeds only when all signatures are valid
- Only works with binary-formatted OpenPGP certs
- Interface ambiguities for detached vs. inline
- GnuPG upstream has been hesitant to implement SOP

sopv-gpgv – a wrapper

- https://gitlab.com/dkg/sopv-gpgv
- In Debian's NEW queue
- Offers a sopv alternative (other sopv alternatives are already in debian)
- TODO: Feedback for existing users of gpgv to move to sopv