Stateless OpenPGP CLI update

Daniel Kahn Gillmor <dkg@fifthhorseman.net>
IETF 116
OpenPGP session
2023-03-29
draft-dkg-openpgp-stateless-cli

- Common API for OpenPGP implementations
- Keeps no implicit state
- Uses stdin/stdout
- Initial focus on encryption, decryption, signing, verifying
  - Not much key or certificate management
- Useful in OpenPGP Interoperability Test Suite
- Small amount of uptake in deployments
Background: examples

$ sop generate-key "Alice <alice@example.net>" > alice.key

$ sop extract-cert < alice.key > alice.cert

$ sop encrypt --sign-with=alice.key bob.cert < msg.txt > msg.enc

$ sop decrypt -verify-with=alice.cert bob.key < msg.enc > msg.txt

$ sop inline-sign -as=clearsigned alice.key < foo-v0.3.sums > foo-v0.3.sums.signed
Updates to `sop` (from draft -04 to -06)

`--profile` for `generate-key` and `encrypt`

- `$ sop generate-key --profile=draft-ietf-openpgp-crypto-refresh-08 "Alice <alice@example.net>"`
  - Create keys following specific standards

- `$ sop encrypt --profile=draft-ietf-openpgp-crypto-refresh-08 --with-password=@ENV:PASSWORD`
  - Encrypt following specific standards
Profiles

- Profile names `rfc4880` and `draft-ietf-openpgp-crypto-refresh-08` mean what they say
  - (some subtleties with `sop encrypt`)
- “private” profile namespaces like notation namespaces
sop list-profiles

$ sop list-profiles generate-key
rfc4880 Widely-deployed baseline
draft-ietf-openpgp-crypto-refresh-08 Latest known draft standard
wacky@example.net My special feature
$

• Implementations can support up to **four** profiles per subcommand
• Keep it simple
• First profile listed is the default
• Special alias: **--profile=default**
Updates to **sop** (from draft -04 to -06)

**sop version --sop-spec**

- Indicate which version of SOP is implemented
- e.g., `draft-dkg-openpgp-stateless-cli-06`
- If known to be incomplete, prefix with `~`