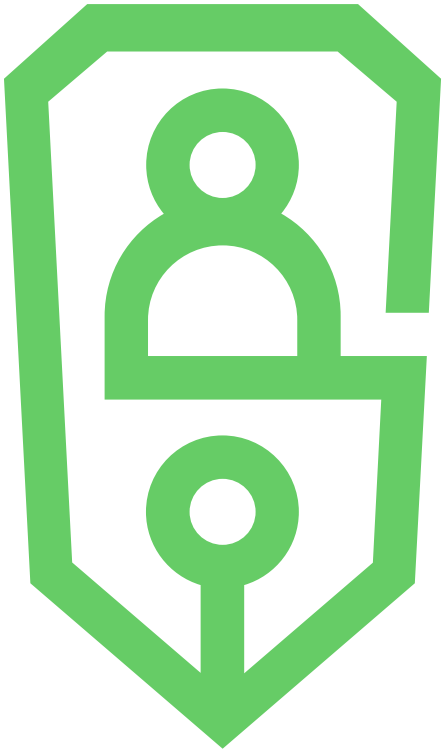

Stateless OpenPGP

IETF 121

What is **sop**?

- Stateless command-line interface to OpenPGP
- Multiple implementations (no “canonical” one)
- Basis for OpenPGP Interoperability Test
- Interface focuses on application-layer functionality
- Implementer chooses appropriate wire format

New subcommands in draft-11...

- **`sop certify-userid`**
  - similar to **`sop sign`**, but with certificates
- **`sop verify-userid`**
  - similar to **`sop inline-verify`**, but with certificates

...New subcommands in draft-11

- **`sop update-key`**
  - Keep a TSK “current” (*what does this mean?*)
- **`sop merge-certs`**
  - Coalesce different variants of a certificate around their shared primary key

Other changes in draft -11

- Replace RFC 4880 with RFC 9580
- Uniform **`--debug`** option
- Set aside **`UNSPECIFIED_FAILURE`**
- JSON output for tail of **`VERIFICATIONS`** lines

Pending Questions

- Predefined profile names? **`security`**, **`performance`**, **`compatibility`**
- **`sop verify`**: Change default of **`--not-before`** from “beginning of time” to “5 years ago”?
- Requirements for digest algorithm when signing with multiple keys?

Seeking recommendations

- What is wrong about the current interface?
- Preserve (and plan for) backward compatibility
- Keep application layer in mind
- Be testable
- Keep it simple
- Strong opinions about *mechanism* belong in your implementation, not in the spec