Crypto Refresh (RFC 4880bis)

IETF 112 - Online
November, 2021

Paul Wouters
paul.wouters@aiven.io

Table of Contents

Table of Contents 2

History: Bis development stalled 3

History: Restart effort with crypto-refresh in WG 4

Current: Speed up process with design team 5

Design Team work flow 6

Status: draft-ietf-openpgp-crypto-refresh-04 7

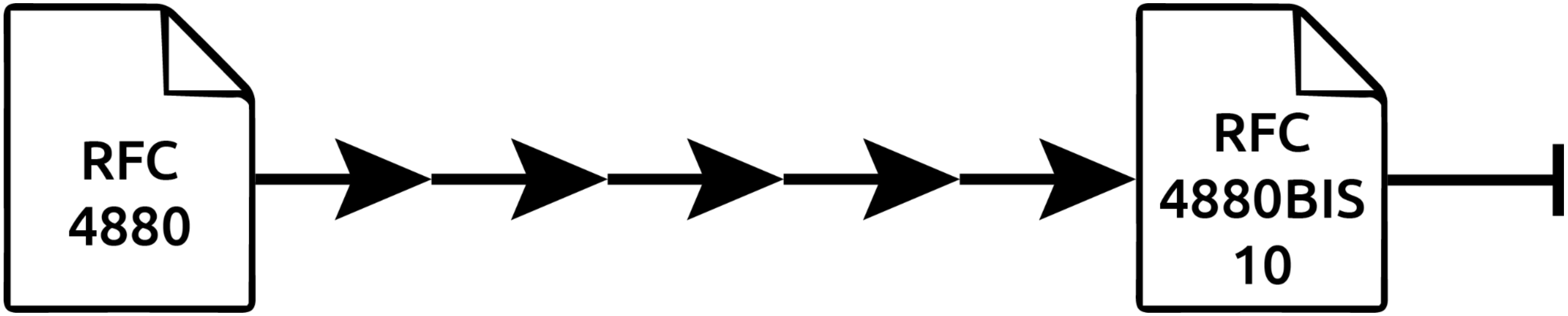
Notable work done: 8

Notable work not done: 9

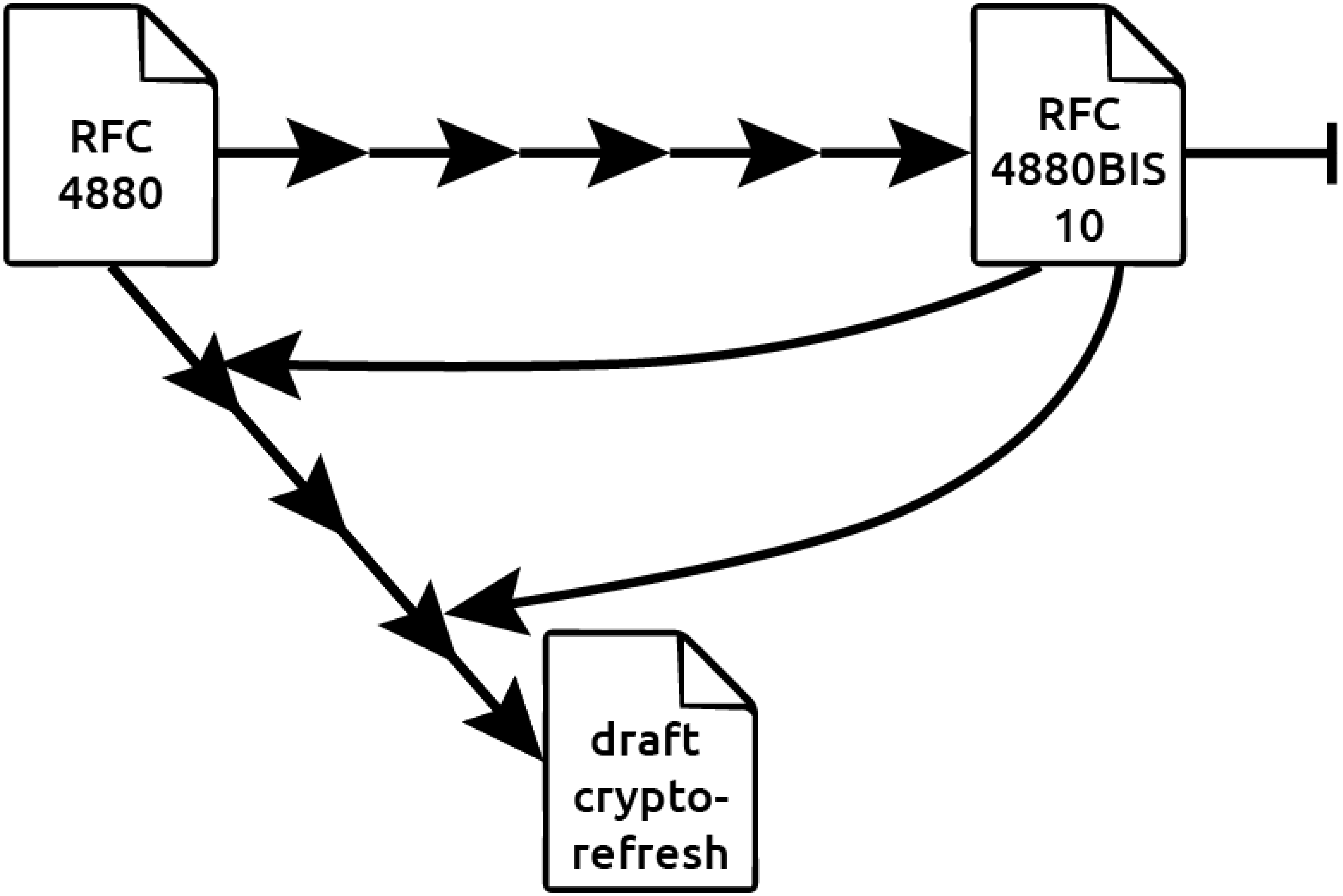
Work done post draft-ietf-openpgp-crypto-refresh-04: 10

Conclusion: We think this process is working 11

History: Bis development stalled



History: Restart effort with crypto-refresh in WG

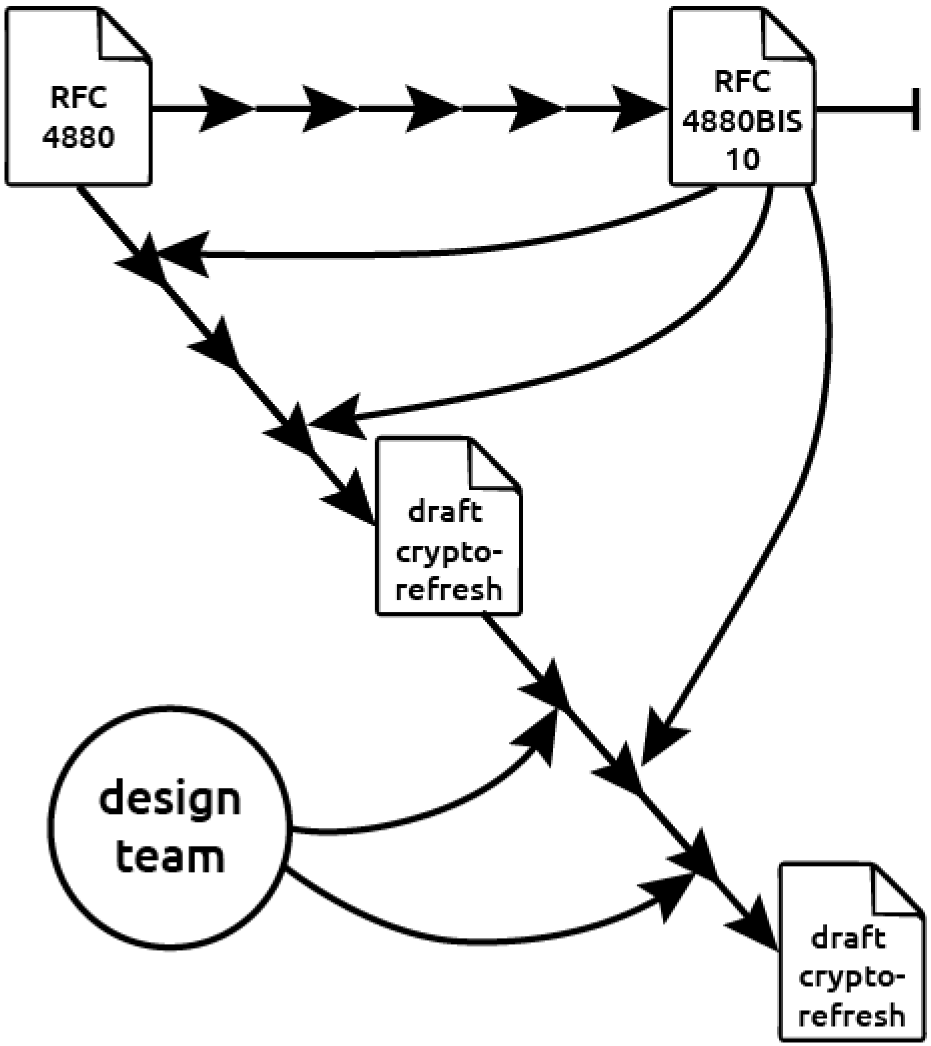


RFC 4880

RFC 4880BIS 10

draft crypto-refresh

Current: Speed up process with design team



Design Team work flow

Weekly meetings, minutes: https://mailarchive.ietf.org/arch/browse/openpgp-dt/
Publish regular updates at: draft-ietf-openpgp-crypto-refresh
Use git for revision control https://gitlab.com/openpgp-wg/rfc4880bis/-/tree/main
gitlab for issue tracking: https://gitlab.com/openpgp-wg/rfc4880bis/-/issues
gitlab for PRs https://gitlab.com/openpgp-wg/rfc4880bis/-/merge_requests
old 4880bis contenthttps://gitlab.com/openpgp-wg/rfc4880bis/-/tree/step-by-step
PRs via topic branches: https://gitlab.com/openpgp-wg/rfc4880bis/-/branches/all
Log of logical commits: https://gitlab.com/openpgp-wg/rfc4880bis/-/commits/main/
Log of logical merged PRs:
https://gitlab.com/openpgp-wg/rfc4880bis/-/merge_requests?scope=all&state=merged

This work does NOT exclude openpgp WG !

Design Team works fully transparently to openpgp WG
Design Team results are input to the openpgp WG
Anything can and should be discussed in the openpgp WG
Everyone is welcome to comment / propose on PRs on our gitlab page!

Status: draft-ietf-openpgp-crypto-refresh-04

- Most of RFC 4880bis merged into crypto-refresh
  - when complete, there is no work left in step-by-step branch
- Some work (marked as "out of charter", can be picked up later after recharter
- Some work drafted, but expecting full openpgp WG discussions (eg MTI)
- Some fairly menial tasks of updates, clarifications, rewrites
- Keep focus on producing RFC 4880bis
- Mark some work as "extra"
  - discuss at the end for inclusion, or
  - suggest to move to separate draft (possibly require re-chartering)
- Continue weekly meetings of Design Team

○

Notable work done:

- AEAD packet defined (and slightly updated)
- AEAD protection of secret key material
- Intended Recipients Subpacket added (signature replay defense)
- SKESKv5 for AEAD only
- RFC 9106 (Argon2) as S2K
- Curve25519
- Curve448: X448 for ECDH, Ed448 for signing
- Improved grammar, structure, tables, language, consistency
- Drop questionable advice about dropping keys.
- etc etc etc (see above links for detailed commits/merged PRs)

Notable work not done:

- Mandatory-to-implement choices (aka "MTI")
- v5 signatures: see active discussion at ISSUE 45
- v5 keys: see different possible proposed changes at (see PR 77 and PR 89)

Work done post draft-ietf-openpgp-crypto-refresh-04:

- Clarify expectations about ECDH secret key material for CFRG curves
- Avoid "NIST curves" as that might be ambiguous when NIST guidance is updated
- Don't pre-process X448 secret keys
- Algorithm-specific fields are "values" not "MPIs"
- Secret key algo-specific data: when usage octet is 253, it also means S2K.
- More explicit guidance on CFRG ECDH wire formats
- Clarify expectations about ECDH secret key material for CFRG

Conclusion: We think this process is working

- Is the working group content with the process ?
- Is the working group content with the progress ?
- Any advice ?
- Comments ?
- Suggestions ?