

Hole-Free Validity

draft-gallagher-openpgp-validity (to be)

Andrew Gallagher

OpenPGP @ IETF interim September 2026

Proposal

draft-gallagher-openpgp-validity (to be)

- Revert to original, singular interpretation of “Signature Creation Time”
 - Intent derived from contemporary discussion omitted from final RFCs
- Use (sub)key creation time field as “not before”
- Permits cleanup of old self-signatures

Implementation Status

draft-gallagher-openpgp-validity (to be)

- Hockeypuck only keeps most recent SLH-DSA selfsig over each packet
 - Third-party certifications not affected (but see 1pa3pc)
 - Revocations not affected

Outstanding decisions

draft-gallagher-openpgp-validity (to be)

- Keep revocation out of scope (-> draft-certificates)?
- Adoption?

Further Information

draft-gallagher-openpgp-validity (to be)

- Editor's copy (I-D pending): <https://openpgp-validity-973f0f.gitlab.io/>
- Repo: <https://gitlab.com/andrewgdotcom/openpgp-validity>
- Early draft of RFC2440: <https://mailarchive.ietf.org/arch/msg/openpgp/Tn719mdl1b14iEEizW7CDiVaYsks/> section 5.1.3