Hole-Free Validity

Andrew Gallagher

OpenPGP @ IETF 126 July 2026

Problem History

Hole-Free Validity

- “Signature Creation Time” subpacket is overloaded:
  - Indicates which signature is the “most recent”
  - Many modern implementations also interpret it as “not before”
- Originally, key/subkey creation time field indicated “not before”
  - Early drafts of RFC2440 and older implementations are clear, RFC is not
- Interop test suite added the overloaded interpretation as an expectation
  - Gamification ensured compliance

Implications

Hole-Free Validity

- Old self-signatures cannot be cleaned up
- Genuine historical signatures become unverifiable
- Certificate sizes grow over time without limit
  - SLH-DSA signature packets are HUGE (up to 30 kB EACH)

Solution

Hole-Free Validity

- Revert to original, singular interpretation of “Signature Creation Time”
- Use (sub)key creation time field as “not before”
- Agree to clean up old SLH-DSA selfsigs from start
  - Other self-sigs can be grandfathered

Further Information

Hole-Free Validity

- Draft: https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-certificates-00#name-time-evolution-of-signature
- Repo: https://gitlab.com/andrewgdotcom/openpgp-certificates
- Early draft of RFC2440: https://mailarchive.ietf.org/arch/msg/openpgp/Tn719mdlb14iEEizW7CDiVaYsks/ section 5.1.3