Reportback from OpenPGP E-mail Summit

Patrick Brunschwig

2024-07-12

IETF-120

Target Audience / Participants

- **Email Clients & Plugins**

  Proton, Thunderbird, R2Mail2, Enigmail, Delta Chat, Planck (former pEp)
  Kontact, Mailvelope

- **OpenPGP Implementations / Libraries**

  Sequoia PGP, OpenPGP.js, rPGP, GopenPGP, RNP

- **Key Servers**

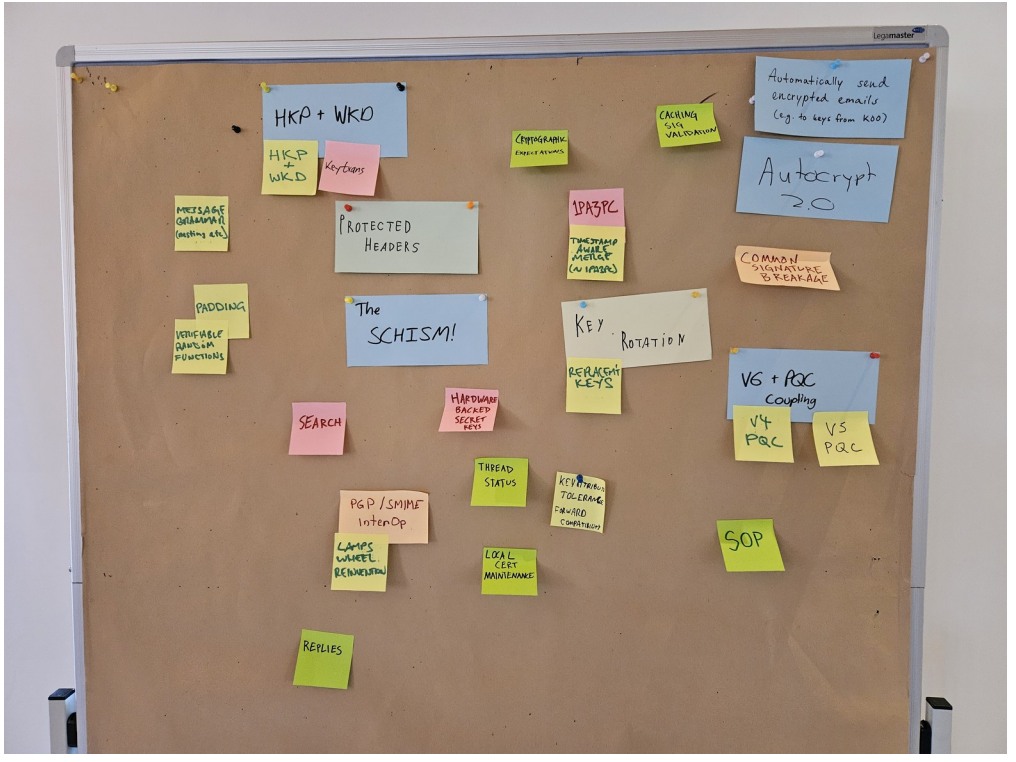
  Hockeypuck, Hagrid (keys.openpgp.org)

- **Standardization folks**

  (OpenPGP v6, PQC, LAMPS, Autocrypt, ...)

Event Organization

- 8th Summit since 2015
- Unconference Style – agenda driven by participants
- Plenary Sessions with topics of general interest
- Social part with joint dinners



Topics Discussed

- What happened / successes since last summit
- The Schism
- PQC in OpenPGP v4
- Header Protection
- Forward Compatibility (how to deal with things that aren’t specified yet)
- HKP & WKD
- Key Distribution Methods
- Migration to OpenPGP v6
- Automatic encryption to published keys
- How to initiate work on Autocrypt 2.0

Deep Dive: Certificate Migration from v4 to v6

Challenge: we want to migrate to v6 as fast possible, but ...

- Existing v4 implementations can't handle v6 keys → users who want to use v6 will need to manage both v4 and v6 keys
- Migration should be transparent, or at least easy for non-expert users
- Interop issues in group communications must be avoided

Ideas Discussed

- Link the v4 cert to the v6 cert (& vice versa); ideally present them like a pair
- Links are directed and can be revoked (by either key)
- Links are discoverable in both directions
- Disallow chains/trees for simplicity
- Solution should also be re-usable for v6 → PQC migration