Automatic forwarding and distribution lists
Why?

Transform a ciphertext to another recipient automatically on a server, preserving E2EE

- Temporary automatic forwarding (e.g. when out of office)
- Server-based distribution lists
- Scalable and computationally cheap
How?

- Based on ECDH Curve25519
- Distributes trust between forwarding final recipient and proxy
- Requires implementation changes for the forwarding final recipient only
- Introduces a new key usage flag
Updates

Since the last IETF, we have some updates to the proposal:

- Published draft -00
- **Complete implementation** in OpenPGP.js and GopenPGP
- Deploy in progress for internal E2EE communication
- In the refresh, X25519 and X448 got changed to include PKs, but the draft covers only v4 so far
Adoption?

https://datatracker.ietf.org/doc/draft-wussler-openpgp-forwarding/

Aron Wussler

IETF 117
2023-07-28