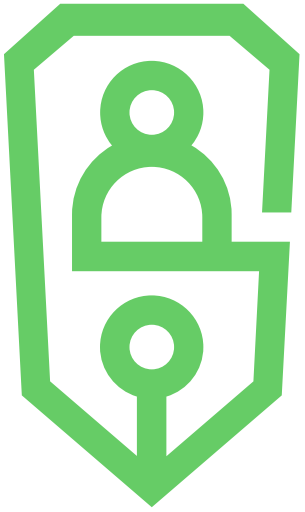


OpenPGP

Replacement Keys for OpenPGP
IETF 120
Vancouver
2024-07-22

draft-gallagher-openpgp-replacement-keys

- Discussed in 2024 OpenPGP e-mail summit
- Use case: automated “transition statements”
- New algorithms, new versions, other reasons?
- Safety / Complexity?

Automated Use by Relying Party

- Certificates are ***equivalent*** to each other
- One certificate is “Preferred”, other(s) are “Fallback”
- Updating known certificate should be enough to be able to look up its related “Preferred” certificate
- Avoid computational DoS
- Avoid network privacy leak (“web bug”)

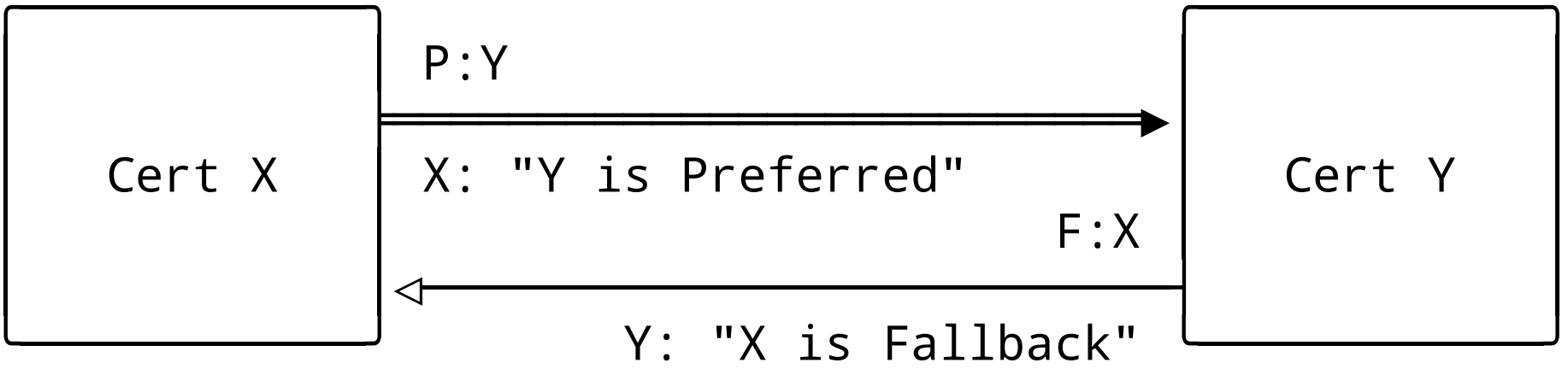
Goals

- “Fallback” certificate can be expired, soft revoked, or still active
- Relationship is directional, but…
- …Assertion of relationship should be made in both directions
- Minimize size of wire format

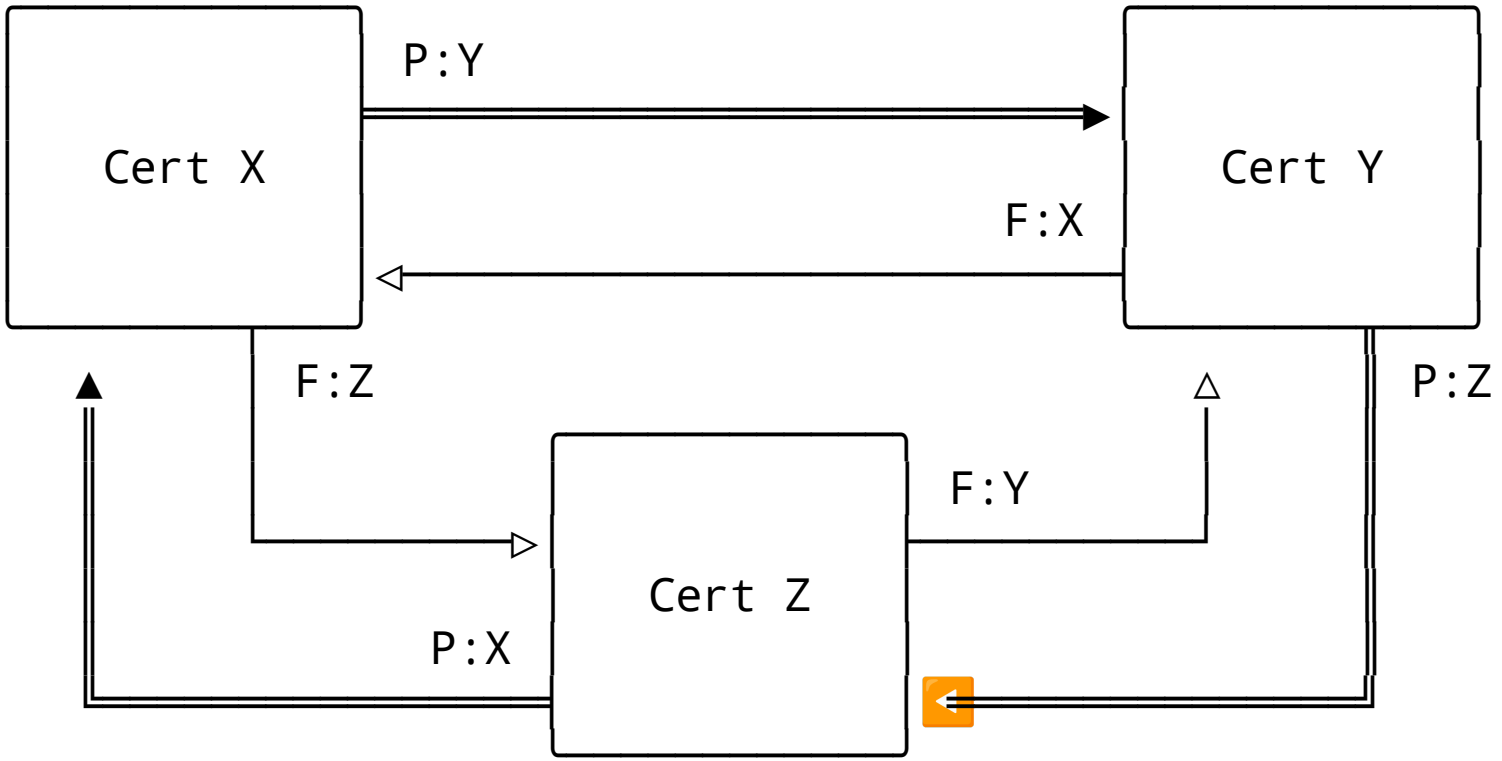
Observations

- Relates primary key to primary key
- Lives in Direct Key Signature or Soft Revocation
- Similar to signing-capable subkey (cross-sig required)

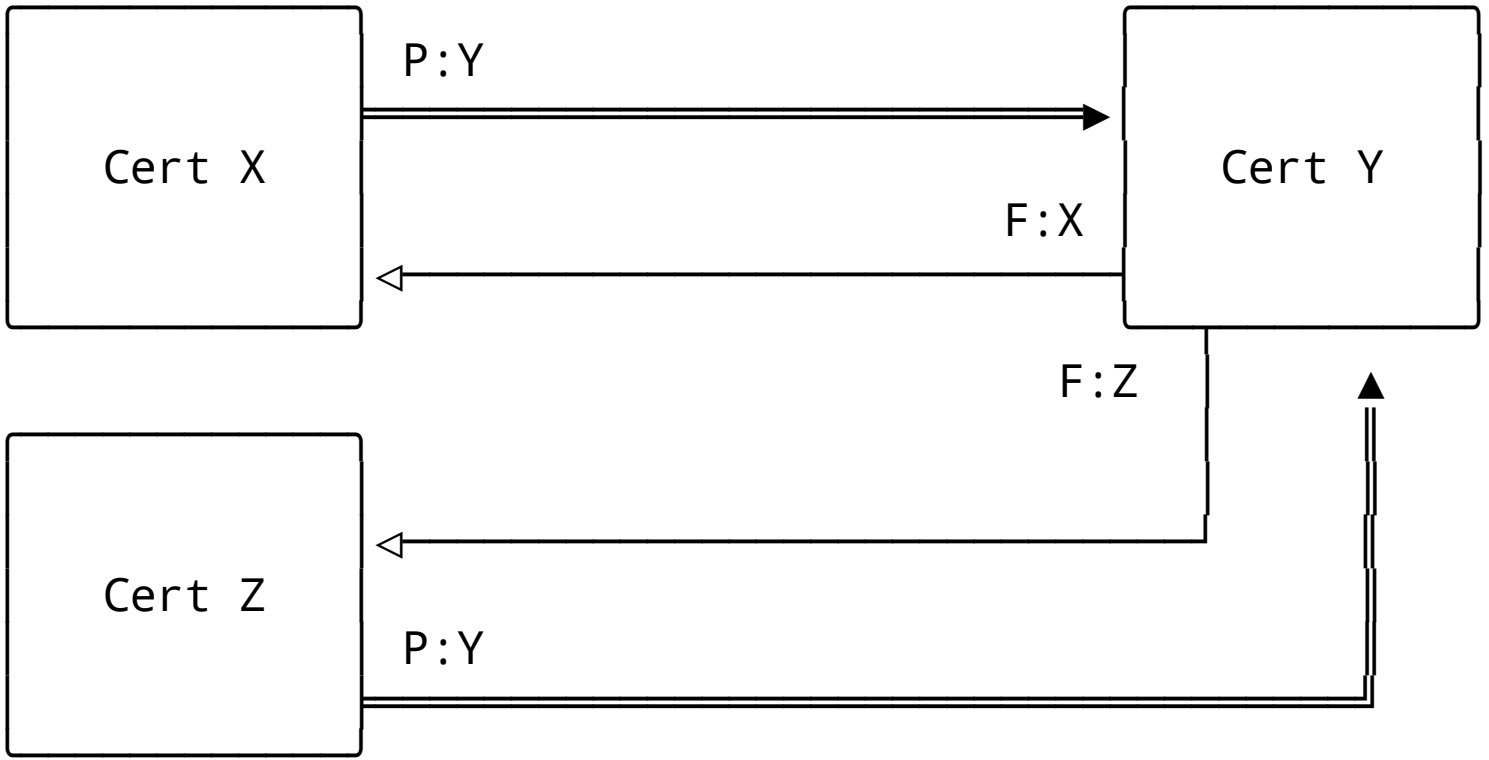
Basic model



⚠️ Loops! ⚠️



One Preferred *or* Many Fallbacks



How to point to a certificate?

- Primary Key Fingerprint
  - Fixed digest algorithm per version
  - Possibly weaker than signature hash
  - Network lookup
- Primary Key “Imprint” via Signature Hash
  - Same strength as signature
  - No network lookup
- Current answer: use both?

Wrinkles

- Web of Trust calculations should not double-count certifications from an equivalence group
- Equivalence groups might change over time (is historical evaluation OK?)
- Transitivity across > 2 certs depends on Relying Party understanding Preferred primary key

Give Feedback!

- Andrew will post draft-ietf- soon
- Review and give feedback!
- Do we need a SOP interface to make equivalence group?
  - To test for equivalence?
- Try to implement!