Keylists

Simplifying PGP public key discovery and management for larger organizations

draft-mccain-keylist-04

miles@rmrm.io | micah.lee@theintercept.com | nat@natwelch.com

Problem Statement

- Organizations need to keep their (potentially tech-illiterate) employees’ internal keystores up to date across all devices.

- Keys are frequently added or updated, and not all keys’ identities correspond with a single controlled domain.

  (Some are **@gmail.com**; some are **@mit.edu**; others are **@theintercept.com**)

“One of the main purposes of keylists is to reduce the amount of work required to ensure that everyone in an organization (or anyone who wishes to communicate with members of that organization) has the correct public key for everyone else.”

— **Micah Lee,** in an email to the openpgp mailing list

Our Solution

- Organizations publish a list of public key fingerprints in the form of a PGP-signed **keylist**.

- Subscribers to that keylist refresh and/or import all the keys in the keylist at a user-defined interval.

→ **Users automatically have the latest version of their colleagues' public keys.**

```
{
  "metadata": {
    "signature_uri": "https://www.example.com/keylist.json.asc",
    "comment": "This is an example of a keylist file"
  },
  "keys": [
    {
      "fingerprint": "927F419D7EC82C2F149C1BD1403C2657CD994F73",
      "name": "Micah Lee",
      "email": "micah.lee@theintercept.com",
      "comment": "Each key can have a comment"
    },
    {
      "fingerprint": "1326CB162C6921BF085F8459F3C78280DDBF52A1",
      "name": "R. Miles McCain",
      "email": "0@rmrm.io"
    },
    {
      "fingerprint": "E0BE0804CF04A65C1FC64CC4CAD802E066046C02",
      "name": "Nat Welch",
      "email": "nat.welch@firstlook.org"
    }
  ]
}
```

An example keylist (from draft-mccain-keylist-04)

Why an Internet Standard?

The PGP ecosystem is diverse. We want **cross-compatibility between clients.**

Why Not ________?

WKD, X.509 PKI, etc: we don’t manage the keys themselves; we just point to them.

GnuPG Keyrings: all above, and not cross-compatible (not an Internet Standard)

Because keylists only *point* to keys, key owners retain the ability to push pubkey updates without updating the keylist.

Implementation Status

GPG Sync is an open-source tool that implements this Internet-Draft.

It is in active use by First Look Media, The Intercept, and the Freedom of the Press Foundation.

Further Development

- Consider a **./well-known** location
- Consider additional keylist functionality
- Better analyze security implications
- Perform general draft improvements
- Achieve wider adoption by PGP tools