A Simple Solution to Key Discovery

Werner Koch

OpenPGP.conf
Cologne
September 8, 2016

Outline

Road Blockers for OpenPGP Adoption

A Solution for Key Discovery

Wrapping Up

Support in MUAs

- Solved for all free software MUAs. ✓
- Solved for most proprietary MUAs. ✓
- Soon to be solved for Outlook. ✓
- Web-mailers are problematic.
  - Solutions are on the way.

Meta Data Protection Needed?

- No way to do this with standard mail.
  - RFC-822 will stay with us.
- New transports need a working anti-spam solution.
  - Will that ever be possible?
  - Without high ecological costs.
- Meta data is often useful.
  - Depends on the threat model.
- Political solutions required !

Key Discovery

- Keyservers can't map a mail address to a key.
  - Only the mail provider can do that.
  - Mail addresses are not under the user's authority.
- Keyserver are decentralized; this is a Good Thing™.
- Verifying keyservers harm the PGP system.
  - They need to be under a single authority.
  - The return of the X.500 dilemma.
- Provider provides the key. ✓

Key Validation

- The Web-of-Trust is a geek's instrument.
  - Hard to explain.
  - Global social graph.
  - It does not scale.
- The Trust On First Use paradigm is better.
  - Local. ✓
  - Keeps the PGP properties. ✓

Outline

Road Blockers for OpenPGP Adoption

A Solution for Key Discovery

Wrapping Up

DANE (RFC-7929)

- DNSSEC for key lookup.
- Distributed database.
- Experimental RFC.
- Support in GnuPG..

Problems:

- No encryption.
- Client DNSSEC is virtually impossible.
- Adding resources to the DNS is not easy.
- Requires collaboration of the mail provider.

Web Key Directory

- HTTPS for key lookup.
- Using a well-known URL
- Easy to deploy.
- Encrypted access.
- Support in GnuPG.

Problems:

- Not distributed, but decentralized.
- TLS access required.
  - Should be standard today.
- Requires collaboration of the mail provider.

What Both Cannot Do

- They assume trustworthy mail providers.
- No protection against customized answers.
- No easy offline communication.
- No specification for a key publication.

Shall only be used for initial key discovery.

Web Key Service

- Supporting protocol for WKD and DANE.
- Entirely based on mail exchange.
- Can work offline (air-gap).
- Server and client are part of GnuPG.
    - Mailers should be enhanced.

WKS Standard Protocol

- Client reads address and policy for the domain.
- Client sends key encrypted to that address.
- Server receives key; sends encrypted nonce.
- Client decrypts the nonce; sends it back to the server.
- Server checks the received nonce and publishes the key.
- Server sends a welcome message.

WKS Variant “auth-submit”

- Iff the Server has authenticated the sender,
- the Server may publish the key directly.

Why:

- Only small client modifications.
- But more fragile and difficult to set up correctly.
- Only for large providers, no aliases, etc.

Improving WKS

Now: Enc(nonce)
Then: Sign(text, Enc(nonce))

- Easy verification: Provider key already known.
- Unattended discarding of non-provider mails.
- Detection of WKS messages before encryption.
- No decryption of unknown messages.
- Allows for customized prompt.

Future WKD/WKS improvements

- Client DB of pending requests.
- DNS based WKS (submitter-address, policy).
- Key retrieval by mail.
- Several keys per address:
  - Revocation of old key.
  - Offline key rollover (forward secrecy).
- Support for CONIKS once that is matured.

Outline

Road Blockers for OpenPGP Adoption

A Solution for Key Discovery

Wrapping Up

What Needs To Be Done

- Convince mail providers to install either WKD or DANE along with the Web Key Service for easy key publication.
- Add support to clients.

Summary

- Web Key Directory finds the right key.
- Web Key Service does the key publishing.
- Malicious provider detection to be added later.

Thanks for attending OpenPGP.conf

https://openpgp-conf.org/2016/openpgp-2016-simple-key-discovery.pdf

Summary

- Web Key Directory finds the right key.
- Web Key Service does the key publishing.
- Malicious provider detection to be added later.

Thanks for attending OpenPGP.conf

https://openpgp-conf.org/2016/openpgp-2016-simple-key-discovery.pdf

Summary

- Web Key Directory finds the right key.
- Web Key Service does the key publishing.
- Malicious provider detection to be added later.

Thanks for attending OpenPGP.conf

https://openpgp-conf.org/2016/openpgp-2016-simple-key-discovery.pdf

Summary

- Web Key Directory finds the right key.
- Web Key Service does the key publishing.
- Malicious provider detection to be added later.

Thanks for attending OpenPGP.conf

https://openpgp-conf.org/2016/openpgp-2016-simple-key-discovery.pdf