The Web Key Directory

Werner Koch

March 2019
Outline

Problem

Solution

Examples

Availability
Key discovery

“How to find a key for mail address”

▶ Keyservers are decentralized; this is a Good Thing™.

but:

▶ Keyservers don’t work — they can’t map an address to a key.
▶ Mail addresses are not under the user’ authority like their keys are.
▶ Mail providers can map their addresses to a key.

thus:

▶ Mail providers should distribute the public keys.
### Verifying keyservers

Verifying keyservers harm the PGP ecosystem:

- They need to be under a single authority.
- It is the return of the X.500 dilemma.
Key validation

The Web-of-Trust is a geek’s instrument:

- Hard to explain.
- Travel required.
- Global social graph.
- It does not scale.

The Trust On First Use (TOFU) paradigm is better:

- Easy to explain. ✓
- Local. ✓
- Keeps the PGP properties. ✓
Key validation

The Web-of-Trust is a geek’s instrument:

- Hard to explain.
- Travel required.
- Global social graph.
- It does not scale.

The Trust On First Use (TOFU) paradigm is better:

- Easy to explain. ✓
- Local. ✓
- Keeps the PGP properties. ✓
Outline

Problem
Solution
Examples
Availability
Web Key Directory

Straightforward Web based method:
A key for philipp.reis@gelnhausen.de would be made accessible under an URL like:

https://gelnhausen.de/.well-known/openpgpkey/philipp.reis

For various practical reasons the URL is a bit more complicated as explained on the next slide.

- TLS secured
- Web domain == Mail domain
Design goals

- Implementable using static web pages
  - Can be prepared locally and uploaded to the webspace
  - Low resource usage
- Exact mail address must be known for lookup
- Shared server for several mail domains possible
- Simple mail based key upload system
  - Allows mail clients to create a key and upload it.
  - Challenge/Response or authenticated upload.
Static web pages

- Mail addresses may include characters which are not allowed in a file name (e.g. `/` on Unix).
- Mail addresses may be longer than the maximum size of a file name

What we do:

- We use a base-32 encoded hash of the UTF-8 representation of the mail address.

philipp.reis  ->  z3167nq86rsd9mbm7k5z6swimpetrxwp
wk            ->  nq6t9teux7edsnwdksswydu4o9i5es3f
Use of one server for multiple domains

- DNS SRV records would be the Right Thing™.
- Web browsers have no feature to resolve SRV records. Thus we can’t use it.
- A fixed well known sub-domain is now used instead of SRV records.
- A fallback to the direct domain lookup is supported.
Example URLs

This is the final canonical lookup URL:

https://openpgpkey.gelnhausen.de/
  .well-known/openpgpkey/gelnhausen.de/
  hu/z3167nq86rsd9mbm7k5z6swimpetrxwp?l=philipp.reis

The fallback to the non-subdomain format should be implemented by clients:

https://gelnhausen.de/
  .well-known/openpgpkey/
  hu/z3167nq86rsd9mbm7k5z6swimpetrxwp?l=philipp.reis
Outline

Problem

Solution

Examples

Availability
Key generation (1)
Key generation (2)
Key enrollment (1)
Key enrollment (2)

GpgOL: Registration request sent!

You might receive a confirmation challenge from your provider to finish the registration.

OK
Key enrollment (3)

Posteingang - wksdemo@testkolab.intevation.de - Outlook

All Unread

Date: Today

key-submission... Confirm your key publication
This message has been send to confirm your request to publish your key. If you did not request a key publication,

GpgOL: Pubkey directory confirmation
Confirm registration?

Ja Nein

OpenPGP Pubkey directory confirmation
This is a confirmation request to publish your Pubkey in the directory for your domain.
If you did not request to publish your Pubkey in your providers directory, simply ignore this message.
Key enrollment (4)

Problem
Solution
Examples
Availability

Send/Receive
Update Folder
Send All
Send/Receive Groups
Send & Receive

Folder
View
Developer
Help
OutlookSpy
Tell me what you want to do

Work Offline
Preferences

All
Unread

Search Current Mailbox
Current Mailbox

Date: Today
key-submission... Confirm your key publication
This message has been send to confirm your request to publish your key. If you did not request a key publication,

GpgOL: Request confirmed!

Your Pubkey can soon be retrieved from your domain.

This is a confirmation request to publish your Pubkey in the directory for your domain.
If you did not request to publish your Pubkey in your providers directory, simply ignore this message.
Send mail (1)
Send mail (2)
Send mail (3)

Hello - Message (HTML)

From: wksdemo@testkolab.intevation.de
To: Test 1
CC:
BCC:
Subject: Hello

Test

GnuPG.com
Receive mail (1)
Receive mail (1)

Test 1
Hello

Test
Outline

Problem
Solution
Examples
Availability
Client Support

- GnuPG (Unix, Windows) uses WKD by default since summer 2017. It also comes with helper tools for easy key enrollment.
- Kmail has full support
- GpgOL (OpenPGP and S/MIME Outlook plugin) has full support
- Enigmail has full support.
- OpenPGP.js has lookup support
- OpenKeychain (Java) has lookup support.
Some providers

- Posteo
- Protonmail
- Several smaller organizations (e.g. kernel.org)
Pitfalls

- Wildcard sub-domains require special treatment for the openpgpkey sub-domain.
- CORS header needs to be set on the server so that Javascript can download the key.
- At least an empty policy file needs to be available so that clients can detect support for the Web Key Directory.
- Redirect works but is subject to CSRF mitigation
Conclusion

A Web Key Directory is
▶ ... easy to use
▶ ... easy to provide
▶ ... easy to maintain
▶ ... solves the UI problem of finding a key.

https://wiki.gnupg.org/WKD

Thanks for your attention
Conclusion

A Web Key Directory is

▶ ... easy to use
▶ ... easy to provide
▶ ... easy to maintain
▶ ... solves the UI problem of finding a key.

https://wiki.gnupg.org/WKD

Thanks for your attention