

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 keyserver

Verifying keyserver 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@gelnhhausen.de would be made accessible under an URL like:

```
https://gelnhhausen.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 workspace
 - 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)

The screenshot shows the Outlook interface with a "Security approval" dialog box open. The dialog box has a title bar with a lock icon and the text "Security approval". The main content of the dialog is as follows:

- Message: "No key found for the address 'wksdemo@testkolab.intevation.de':"
- Dropdown menu: "Generate a new key pair" with a search icon.
- Section: "Encrypt to:"
- Text: "test1@testkolab.intevation.de"
- Dropdown menu: "Testuser 1 <test1@testkolab.intevation.de> (not certified, created: 12.01.2017)" with a search icon.
- Text: "wksdemo@testkolab.intevation.de"
- Dropdown menu: "Generate a new key pair" with a search icon.
- Buttons: "Generate" and "Abbrechen".

The background shows the Outlook ribbon with tabs for File, Message, Insert, Options, Format Text, Review, Developer, Help, and OutlookSpy. The ribbon includes options like Attach File, Follow Up, High Importance, and Secure. The message body is partially visible, showing "Hello".

Key generation (2)

The screenshot shows the Outlook interface with a message titled "Testmail - Message (HTML)". The message content includes "Hello" and several recipients: "test1@testkolab.intevation.de", "Testuser 1 <test1@testkolab.intevation.de>", and "wksdemo@testkolab.intevation.de".


Three dialog boxes are overlaid on the message:

- Security approval**: A dialog box with a lock icon and the text "No key found for the address 'wksdemo@testkolab.intevation.de:'". It contains a "Generate a new key pair" button.
- Key generation**: A dialog box with a lock icon and the text "Generating key for 'wksdemo@testkolab.intevation.de'... This can take several minutes." It has an "Abbrechen" button.
- pinentry-qt**: A dialog box with a lock icon and the text "Bitte geben Sie die Passphrase ein, um Ihren Schlüssel zu schützen." It contains three input fields labeled "Passphrase:", "Nochmal:", and "Qualität:", and "OK" and "Abbrechen" buttons.

Key enrollment (1)

The screenshot shows the Outlook interface with the 'Home' ribbon selected. The main pane displays 'All Unread' and a search bar. A dialog box titled 'GpgOL: Pubkey directory available!' is overlaid on the interface. The dialog contains the following text:

GpgOL: Pubkey directory available!

 A Pubkey directory is available for the address:
wksdemo@testkolab.intevation.de

Register your Pubkey in that directory to make it easy for others to send you encrypted mail.

It's secure and free!

Register automatically?

Buttons:

The Outlook status bar at the bottom shows 'Sending message 1 of 1', 'Connected', and a zoom level of '100%'.

Key enrollment (2)

The screenshot shows the Microsoft Outlook interface. The title bar indicates the account is "Posteingang - wksdemo@testkolab.intevation.de - Outlook". The ribbon is set to "Home". The main pane shows "All Unread" with a search bar and a message list header containing "FROM" and "SUBJECT". A message is not visible, with the text "We didn't find anything to show here." below the header.

A dialog box titled "GpgOL: Registration request sent!" is displayed in the foreground. It contains a lock icon and the text: "You might receive a confirmation challenge from your provider to finish the registration." An "OK" button is located at the bottom right of the dialog.

At the bottom of the Outlook window, the status bar shows "Sending message 1 of 1", "Connected", and a zoom level of "100%".

Key enrollment (3)

The screenshot shows the Outlook interface with the 'Send / Receive' tab selected. The ribbon includes options like 'Update Folder', 'Send All', 'Send/Receive All Folders', 'Send/Receive Groups', 'Send & Receive', 'Show Progress', 'Cancel All', 'Download', 'Download Headers', 'Mark to Download', 'Unmark to Download', 'Process Marked Headers', 'Server', 'Work Offline', and 'Preferences'. The main pane shows an email titled 'key-submission... Confirm your key publication' from 'key-submission@testkolab.intevation.de' received on 'Mi 03.04.2019 10:04' (4 KB). The email content reads: 'This message has been send to confirm your request to publish your key. If you did not request a key publication,'.

A dialog box titled 'GpgOL: Pubkey directory confirmation' is overlaid on the email. It asks 'Confirm registration?' with 'Ja' and 'Nein' buttons.

Below the dialog, a blue banner reads 'OpenPGP Pubkey directory confirmation'. The text below the banner states: '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.'

The bottom of the Outlook window shows 'Connected' and a volume icon set to 100%.

Key enrollment (4)

The screenshot shows the Outlook interface for the account 'Posteingang - wksdemo@testkolab.intevation.de'. The ribbon is set to 'Send / Receive'. A message titled 'key-submission... Confirm your key publication' is selected, with a subject line 'Confirm your key publication'. The message content reads: 'This message has been send to confirm your request to publish your key. If you did not request a key publication, ...'.

A dialog box titled 'GpgOL: Request confirmed!' is overlaid on the message. It contains a lock icon and the text: 'Your Pubkey can soon be retrieved from your domain.' with an 'OK' button.

Below the dialog box, the message body text is visible: '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.'

The bottom of the screenshot shows the system tray with 'Connected' status and a volume icon.

Send mail (1)

Untitled - Message (HTML)

File Message Previous Item (Ctrl+<) s Format Text Review Developer Help OutlookSpy Tell me what you want to do

Paste

Clipboard Basic Text

Names Address Book Check Names

Include Attach File Attach Item Signature

Tags Follow Up High Importance Low Importance

GpgOL Secure

Send

From wksdemo@testkolab.intevation.de

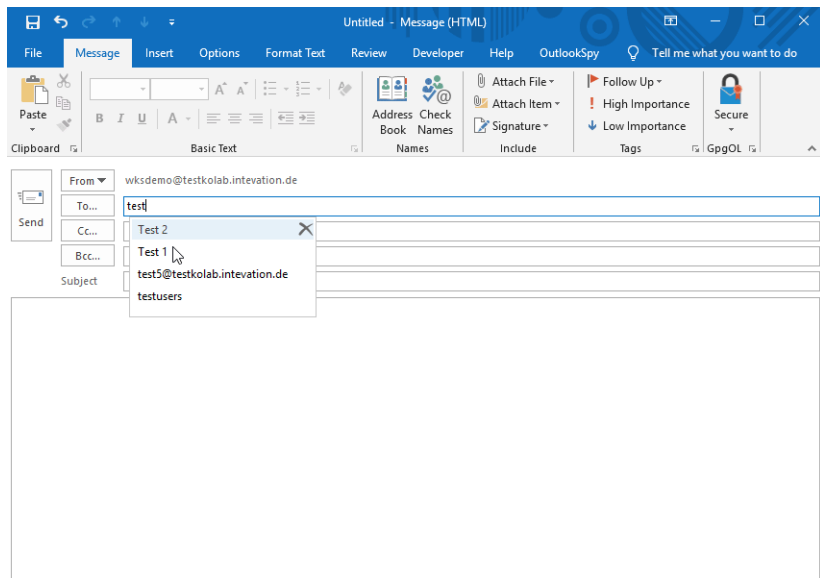
To...

Cc...

Bcc...

Subject

Send mail (2)



The screenshot shows the 'Send Mail' dialog box in Microsoft Outlook. The window title is 'Untitled - Message (HTML)'. The ribbon includes 'File', 'Message', 'Insert', 'Options', 'Format Text', 'Review', 'Developer', 'Help', 'OutlookSpy', and 'Tell me what you want to do'. The 'Message' ribbon is active, showing options for 'Basic Text', 'Names', 'Include', 'Tags', and 'GpgOL'. The 'Send' button is visible on the left. The 'From' field is 'wksdemo@testkolab.intevation.de'. The 'To' field contains 'test|', and a dropdown menu is open showing 'Test 2', 'Test 1', 'test5@testkolab.intevation.de', and 'testusers'. The 'Cc' and 'Bcc' fields are empty. The 'Subject' field is empty. The main body of the message is a large empty text area.

Send mail (3)

Microsoft Outlook interface showing an email composition window titled "Hello - Message (HTML)". The ribbon includes "File", "Message", "Insert", "Options", "Format Text", "Review", "Developer", "Help", "OutlookSpy", and "Tell me what you want to do". The "Message" tab is active, showing options like "Paste", "Basic Text", "Names", "Include", "Tags", and "GpgOL".

The email fields are:

- From: wksdemo@testkolab.intevation.de
- To: Test 1
- Cc:
- Bcc:
- Subject: Hello

The main body of the email contains the text "Tes|".

Receive mail (1)

Sent Items - wksdemo@testkolab.intevation.de - Outlook

File Home Send / Receive Folder View Developer Help OutlookSpy Tell me what you want to do

New Email New Items Delete Archive Reply Reply All Forward Respond Quick Steps Move Tags Find Speech Send/Receive All Folders Send/Receive Insecure GpgOL

Search Sent Items Current Folder

All Unread By Date Newest

Today

Test 1
Hello 10:20

Receive mail (1)

The screenshot shows the Microsoft Outlook interface. The title bar indicates the current folder is 'Sent Items - wksdemo@testkolab.intevation.de - Outlook'. The ribbon is set to 'Home', and the 'Send / Receive' tab is active. The ribbon contains various actions such as 'New Email', 'Delete', 'Reply', 'Forward', 'Quick Steps', 'Move', 'Tags', 'Find', 'Speech', 'Send/Receive All Folders', and 'Security Level 4 GpgOL'. The left-hand navigation pane shows the 'Sent Items' folder selected under the 'wksdemo@testkolab.int...' account. The main pane displays a search bar for 'Sent Items' and a list of messages. The selected message, 'Test 1', is highlighted in blue and shows a subject of 'Hello' and a time of 10:20. Below the message header, there are actions for 'Reply', 'Reply All', and 'Forward'. The sender is identified as 'wksdemo@testkolab.intevation.de'. A green bar indicates 'GpgOL: Level 4 trust in 'wksdemo@testkolab.intevat...'' and a blue bar indicates 'GpgOL: Encrypted Message'. The body of the email contains the text '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