The Web Key Directory

Werner Koch

March 2019

Outline

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.

Verifiying 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

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:

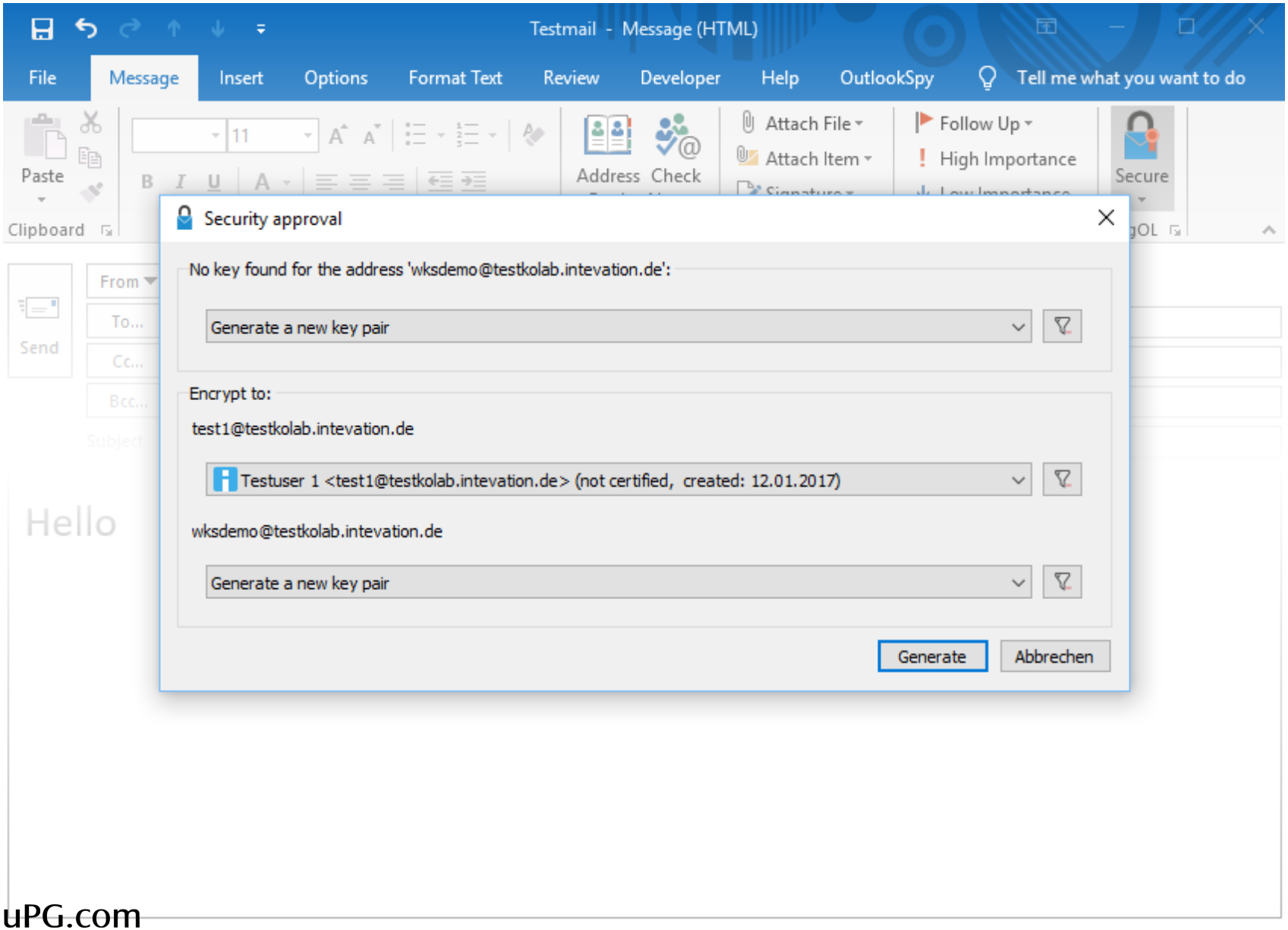
```
https://openpgpkey.gelnhausen.de/
        .well-known/openpgpkey/gelnhausen.de/
        hu/z3167nq86rsd9mbm7k5z6swimpetrxwp?l=philipp.reis
```

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

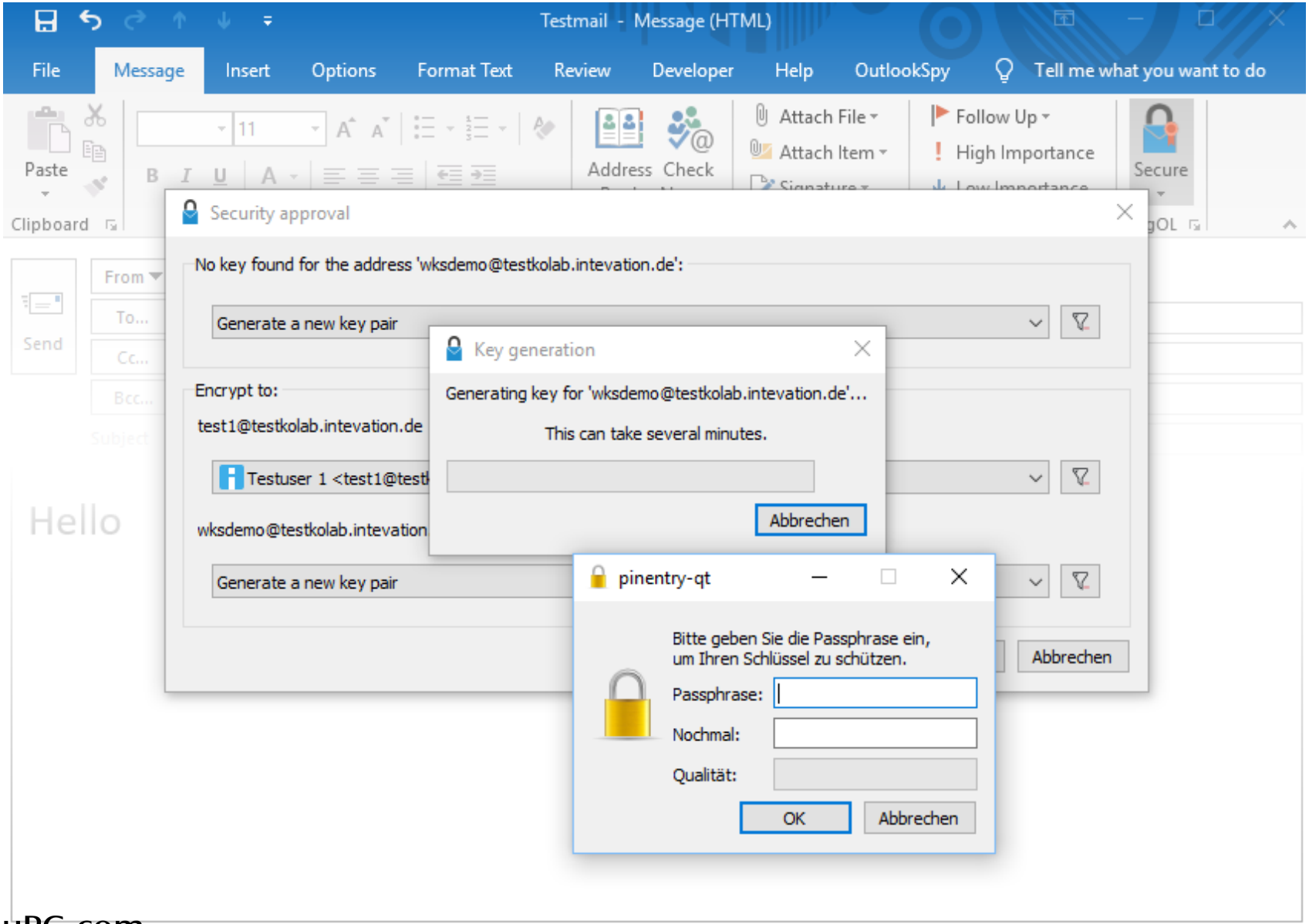
```
https://gelnhausen.de/
        .well-known/openpgpkey/
        hu/z3167nq86rsd9mbm7k5z6swimpetrxwp?l=philipp.reis
```

Outline

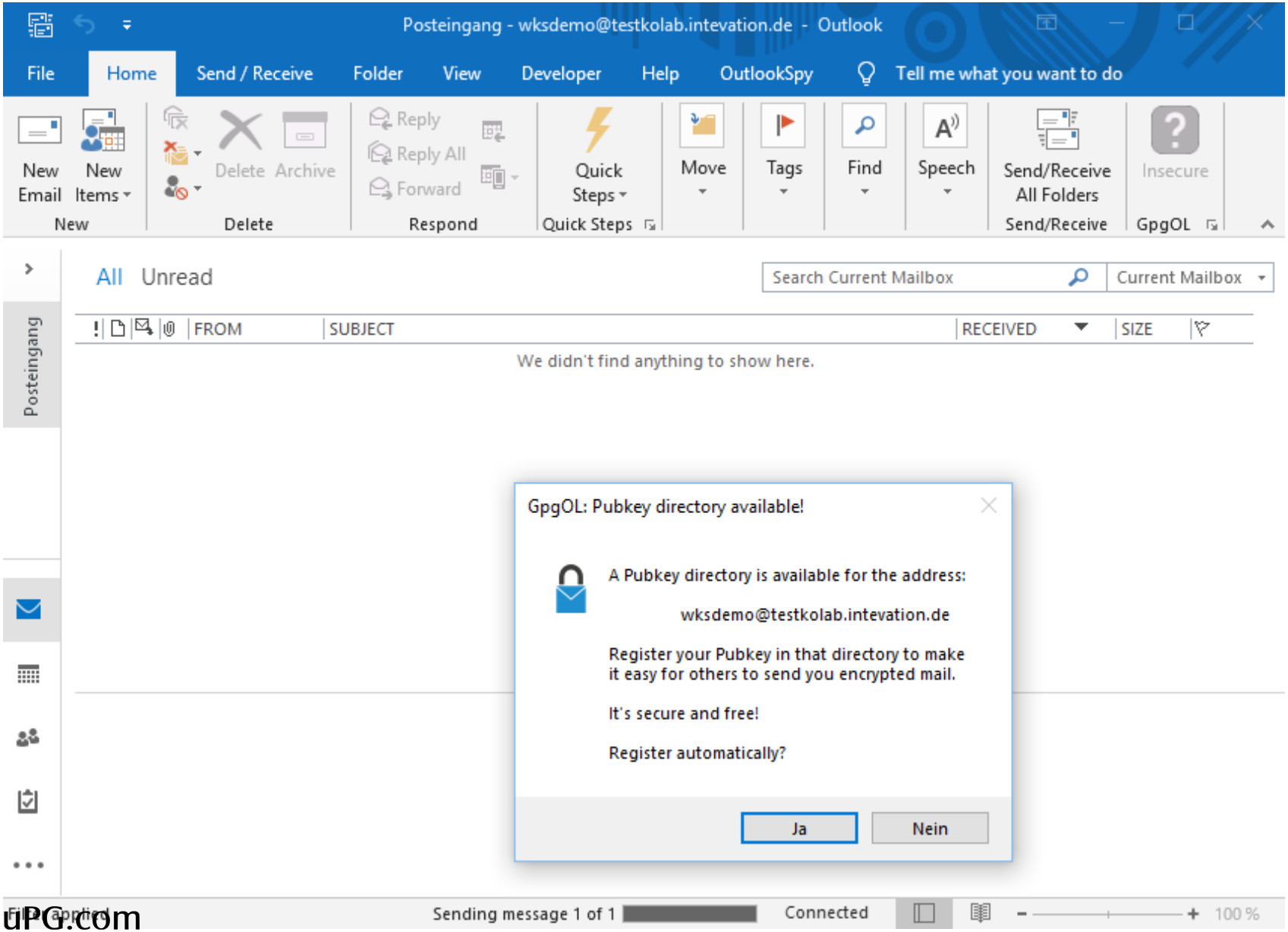
Key generation (1)



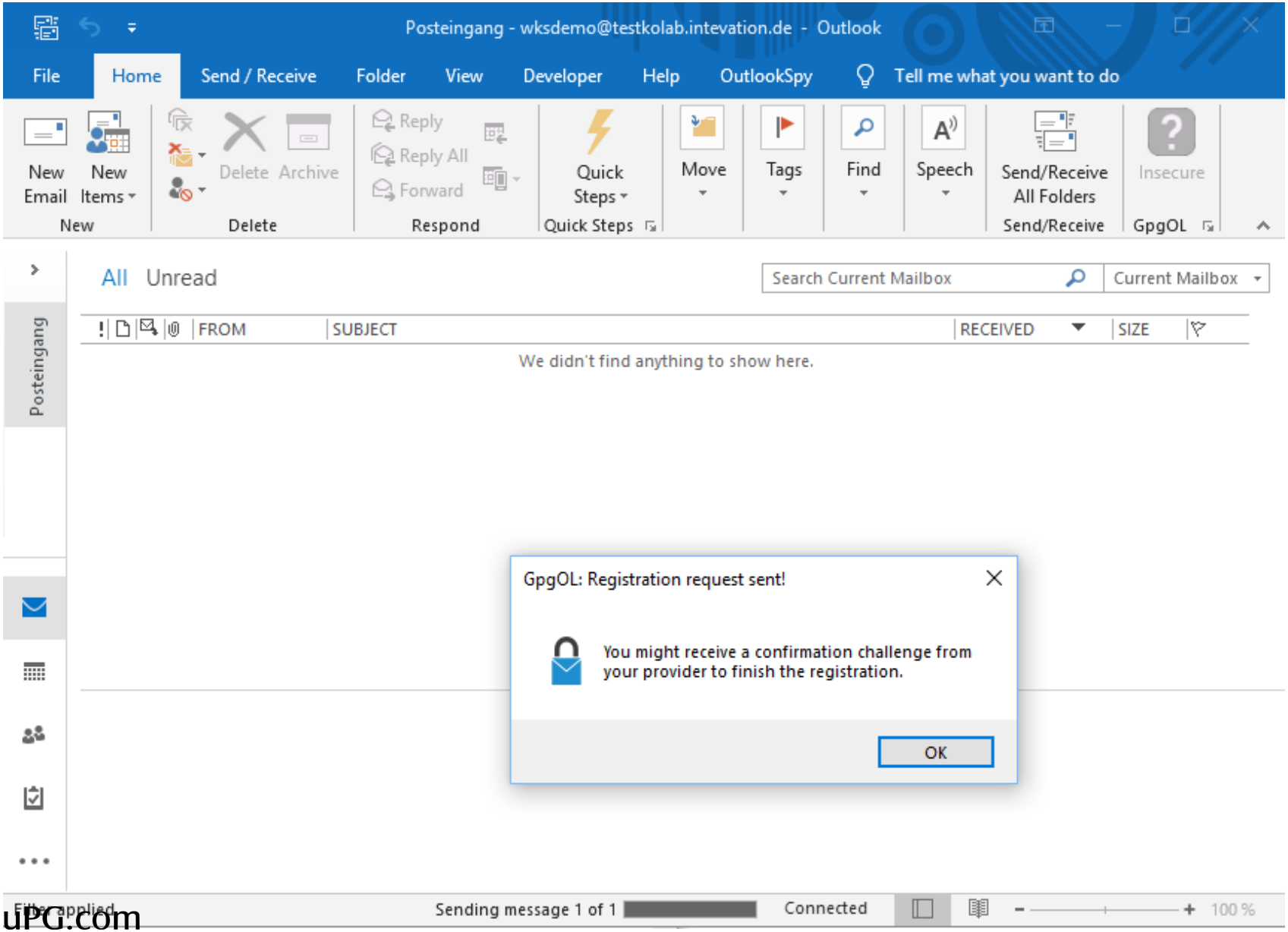
Key generation (2)



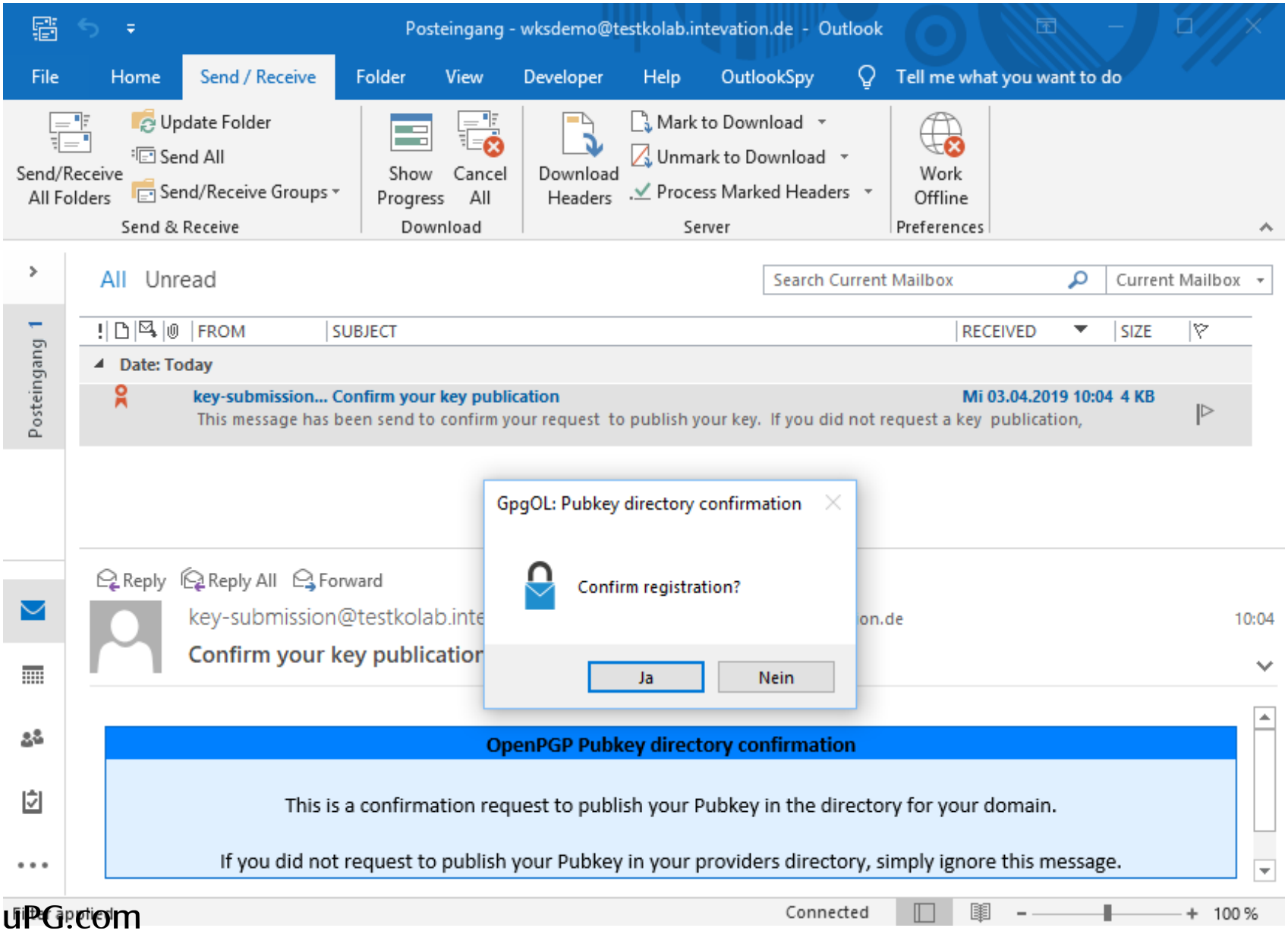
Key enrollment (1)



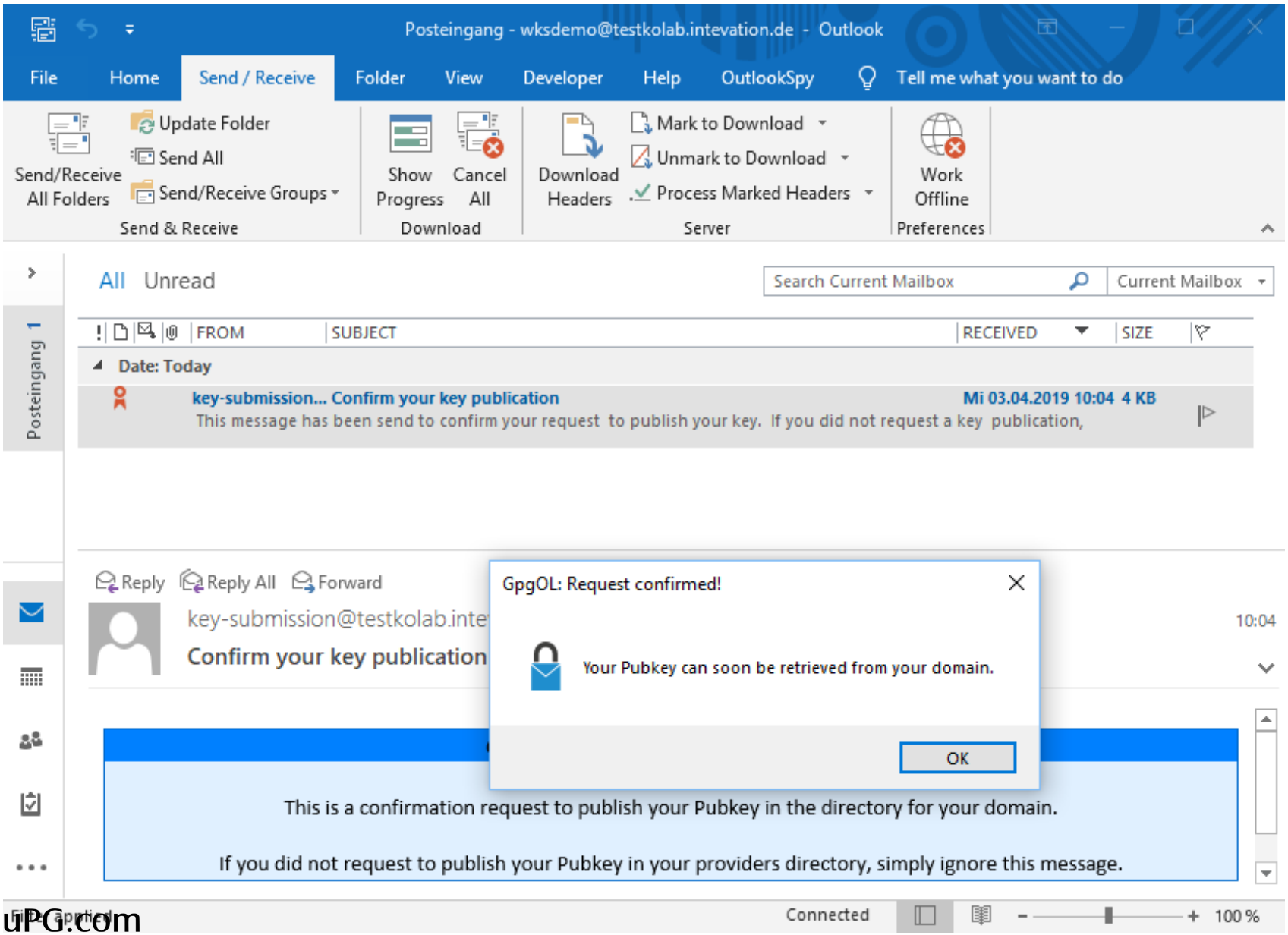
Key enrollment (2)



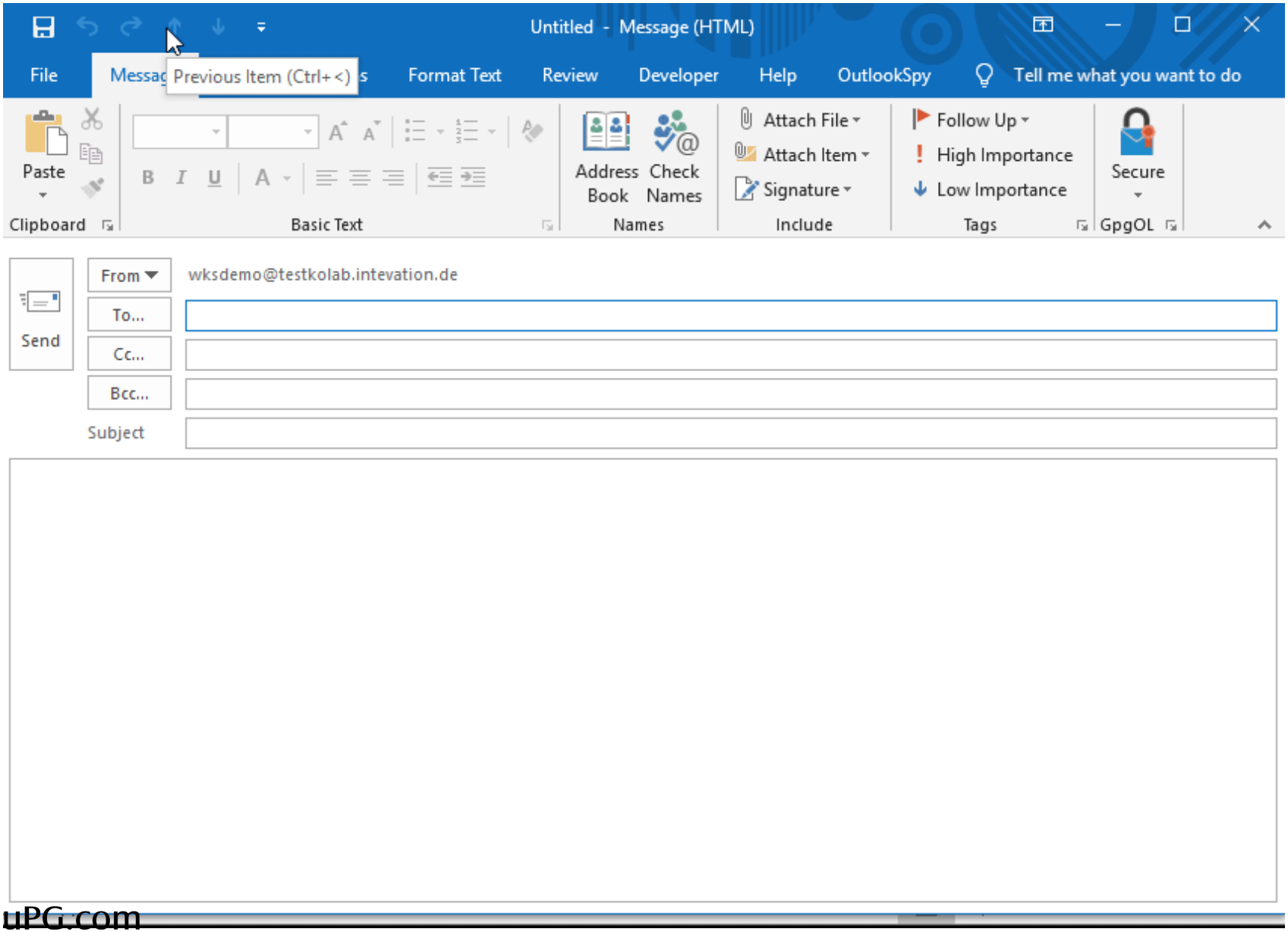
Key enrollment (3)



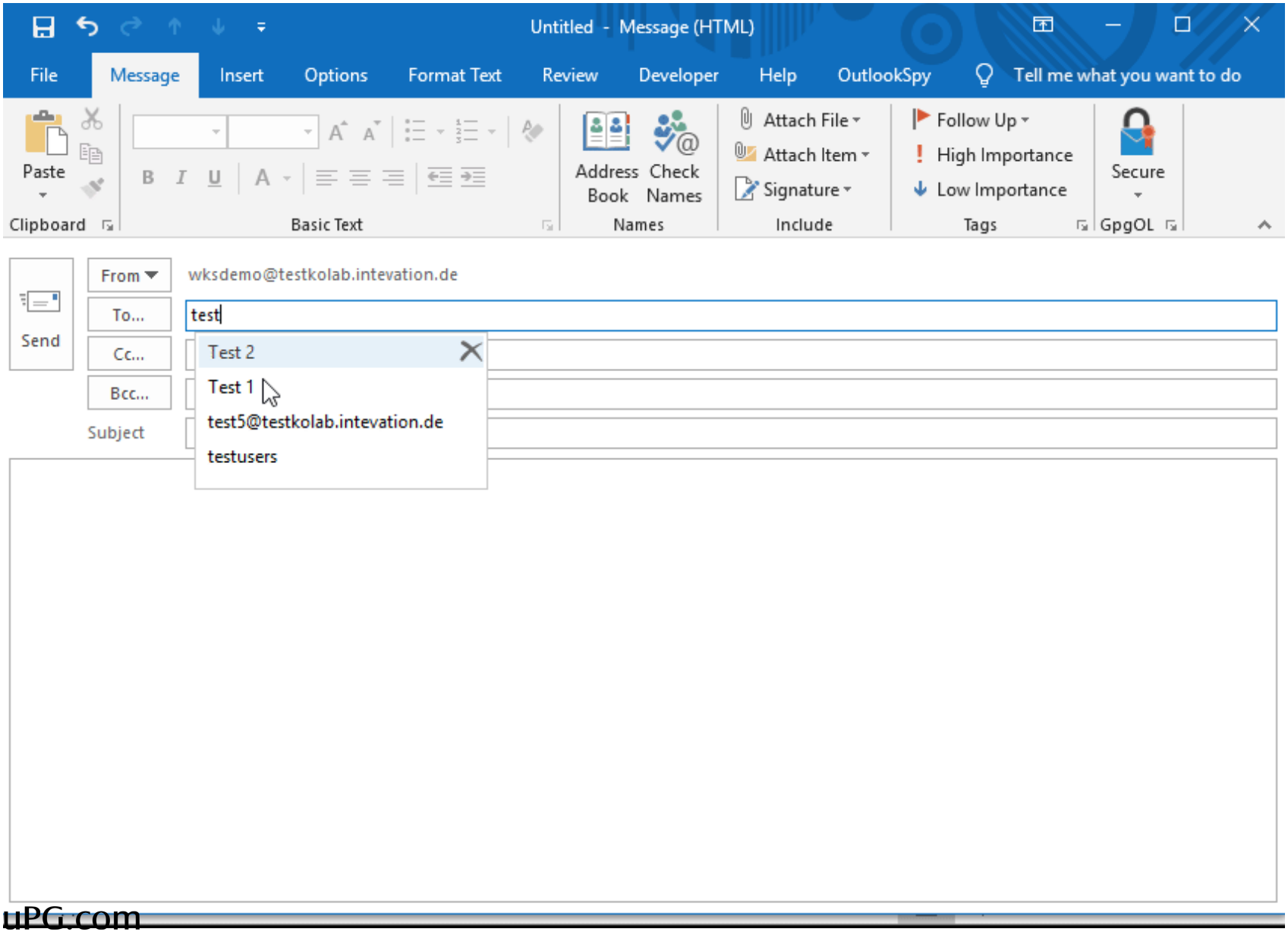
Key enrollment (4)



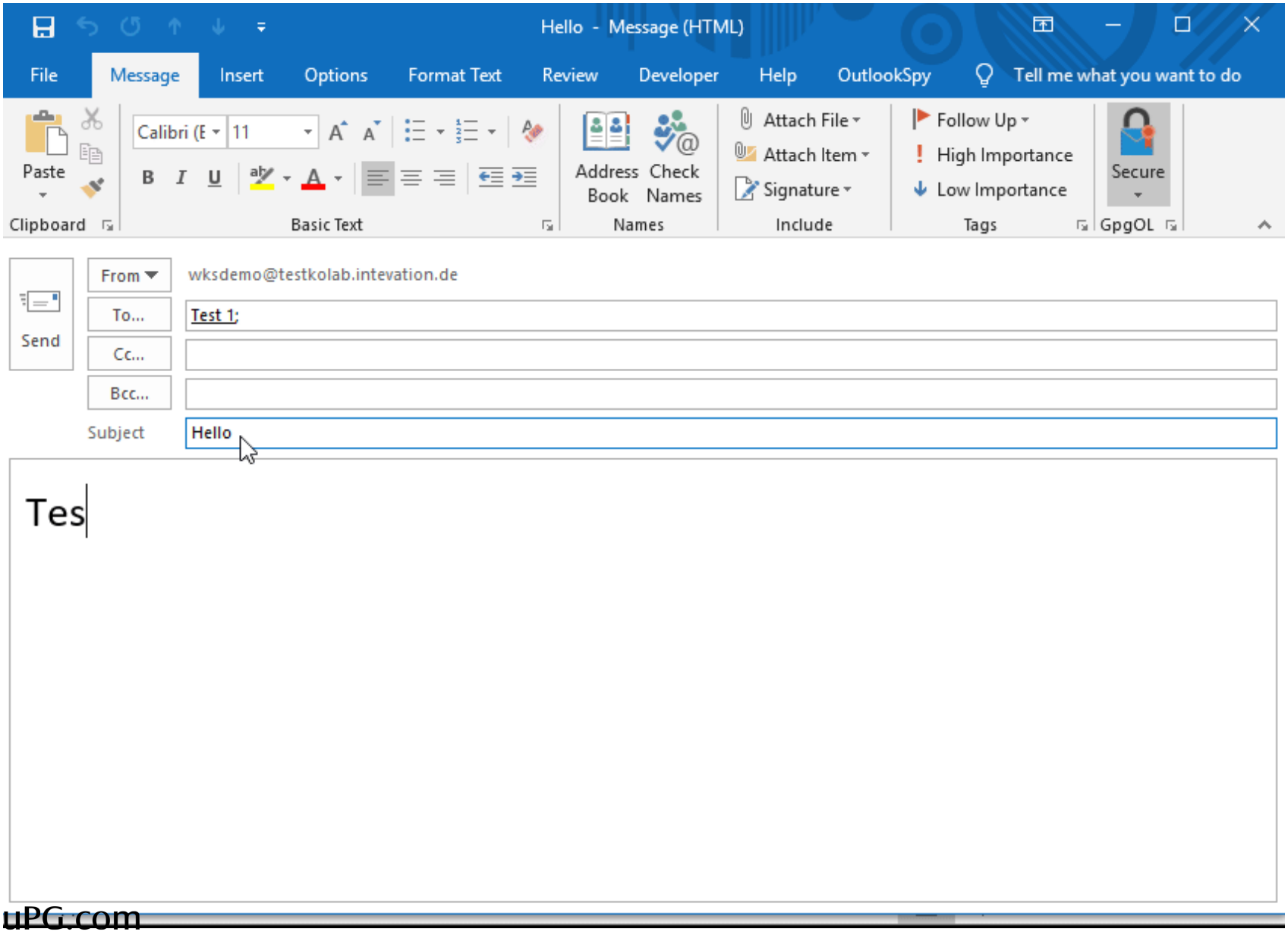
Send mail (1)


Untitled - Message (HTML)
File
Previous Item (Ctrl+<)
Format Text
Review
Developer
Help
OutlookSpy
Tell me what you want to do
Paste
Clipboard
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Follow Up
High Importance
Low Importance
Tags
Secure
GpgOL
Send
From
wksdemo@testkolab.intevation.de
To...
Cc...
Bcc...
Subject

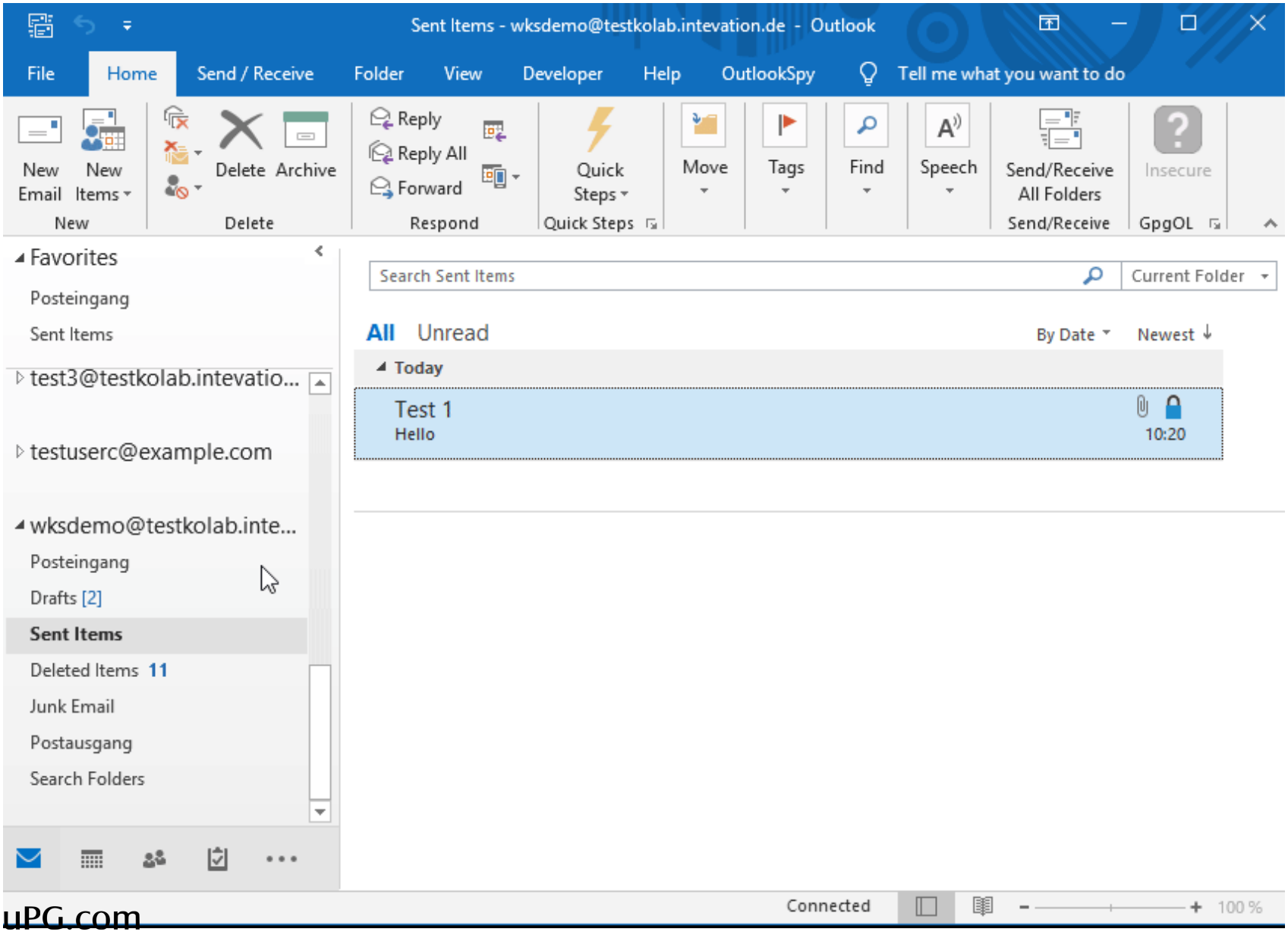
Send mail (2)


Untitled - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Developer
Help
OutlookSpy
Tell me what you want to do
Paste
Clipboard
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Follow Up
High Importance
Low Importance
Tags
Secure
GpgOL
Send
From
wksdemo@testkolab.intevation.de
To...
test
Cc...
Bcc...
Subject
Test 2
Test 1
test5@testkolab.intevation.de
testusers

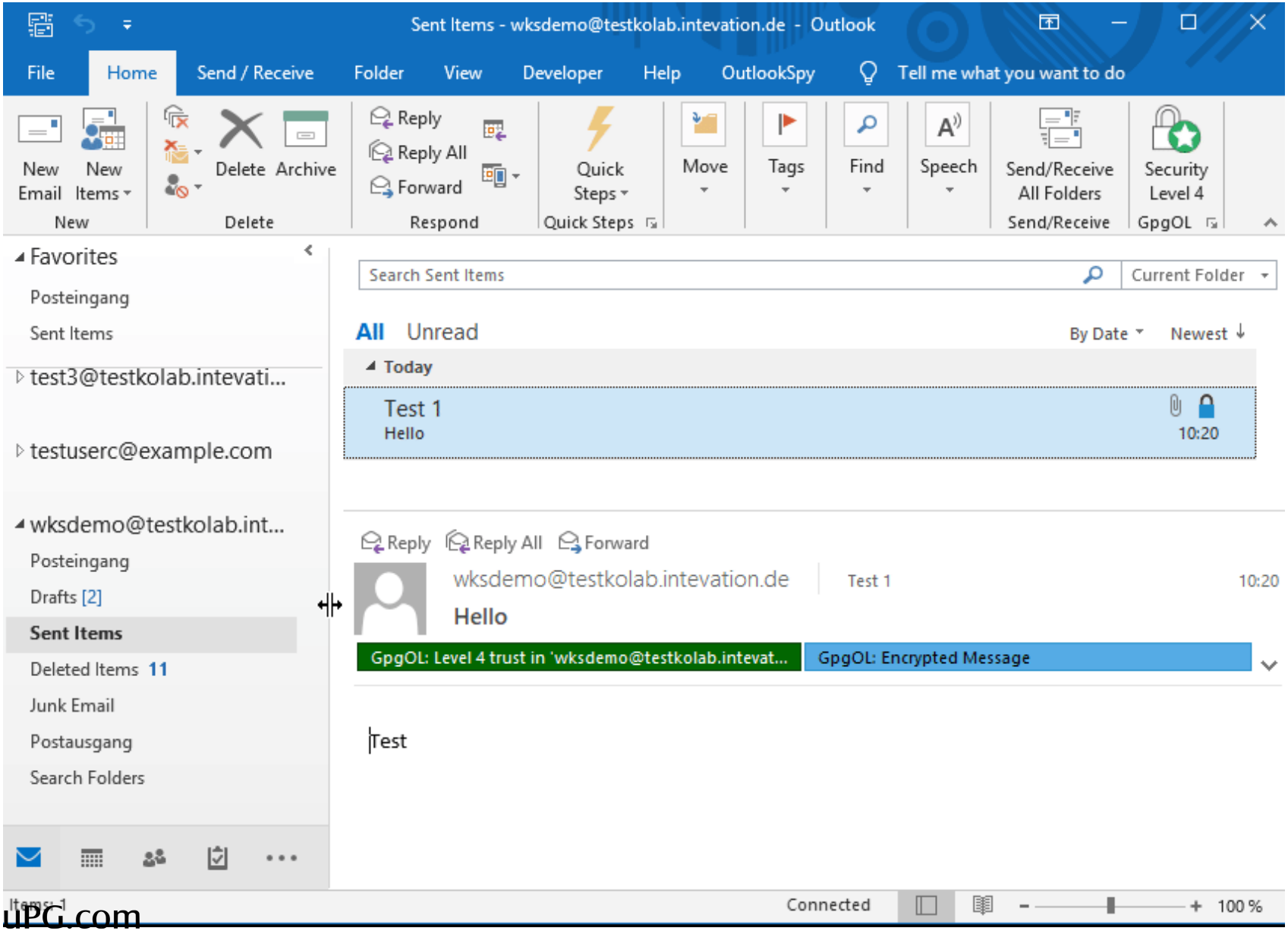
Send mail (3)


Hello - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Developer
Help
OutlookSpy
Tell me what you want to do
Paste
Clipboard
Calibri (E
11
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Follow Up
High Importance
Low Importance
Tags
Secure
GpgOL
Send
From
wksdemo@testkolab.intevation.de
To...
Test 1;
Cc...
Bcc...
Subject
Hello
Tes

Receive mail (1)



Receive mail (1)



Outline

Client Support

- GnuPG (Unix, Windows) uses WKD by default sinse 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