



# **Exchanging Microsoft: Implementing 27+ MS Exchange Protocols & APIs in OSS with grommunio**

**Jan Engelhardt, Lead Software Architect**

# MAPI

## Messaging Application Programming Interface

...it's a slightly ambiguous term.  
Used for:

- Concepts and the data model
  - Programming interfaces
- Network protocols on the wire



# Leading MAPI Products

Microsoft Exchange  
Exchange Online

# Microsoft Exchange Protocols & Specifications

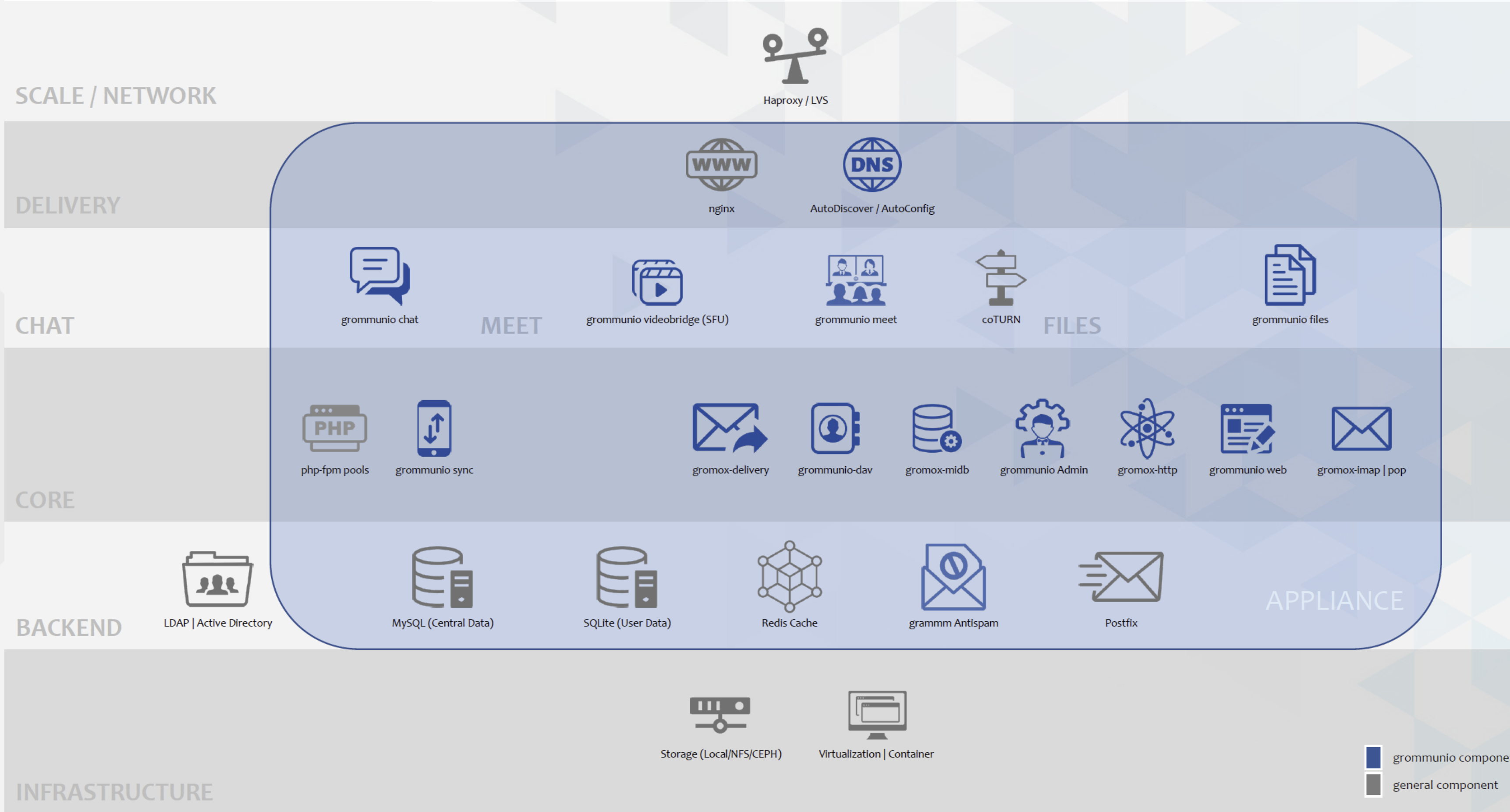
The specifications are quite vast.

<https://learn.microsoft.com/en-us/openspecs/protocols/ms-protocols/olsp/>

132+ documents, 8400+ pages.

And that is on top of the Internet Mail protocols (i.e. RFC 5322, 5545, etc.) that need to be supported anyway.

## grommunio component architecture





# Leading Open Source Project



**gromox by grommunio**



### **EX/MAPI related:**

- OXCDATA
- OXDSCLI
- OXCFOLD
- OXCFXICS
- OXCICAL
- OXCMAIL
- OXCMAPIHTTP
- OXCMSG
- OXCNOTIF
- OXNSPI
- OXCPerm
- OXCPRPT
- OXCROPS
- OXCRPC
- OXCSTOR
- OXCTABL
- OXMSG
- OXOABK
- OXOABKT
- OXOCAL
- OXOCNTC
- OXODLGT
- OXOMSG
- OXORULE
- OXOSFLD
- OXOSMIME
- OXPROPS
- OXTNEF
- OXVCARD
- OXABREF
- OXOCFG
- OXRTFCP
- OXWAVLS
- OXWOOF
- OXWSCDATA
- OXWSCONT
- OXWSCORE
- OXWSFOLD
- OXWSMSG
- OXODLGT
- OXWSMTGS
- OXWSPOST

# Protocols and formats in gromox

- OXWSRSLNM
- OXWSSYNC
- OXWSTASK
- PST
- CFB
- RCPE
- RPCH
- DCERPC/C706

# Tools for protocol analysis: MAPI/ROP

## Decoding

- SSL intercept, decrypt, parse with Fiddler / Wireshark
- confer/compare with specs to validate
- write marshalling code

## Clients

- MFCMAPI
- Outlook





Progress Telerik Fiddler Classic

File Edit Rules Tools View Help

WinConfig | Replay | Go | Stream | Decode | Keep: All sessions | Any Process | Find | Save | Browse | Clear Cache | TextWizard | Tearoff

#	R...	P..	Host	URL	Body	Ca
18	2...	H..	srv-exchange-...	/...	415	pri
19	2...	H..	srv-exchange-...	/...	416	pri
20	2...	H..	srv-exchange-...	/...	274	pri
21	2...	H..	srv-exchange-...	/...	512	pri
22	2...	H..	srv-exchange-...	/...	512	pri
23	2...	H..	srv-exchange-...	/...	295	pri
24	2...	H..	srv-exchange-...	/...	274	pri
25	2...	H..	srv-exchange-...	/...	161	pri
26	2...	H..	srv-exchange-...	/...	123	pri
27	2...	H..	srv-exchange-...	/...	295	pri
28	2...	H..	srv-exchange-...	/...	123	pri
29	2...	H..	srv-exchange-...	/...	167	pri
30	2...	H..	srv-exchange-...	/...	295	pri
31	2...	H..	srv-exchange-...	/...	137	pri
32	2...	H..	srv-exchange-...	/...	295	pri
33	2...	H..	srv-exchange-...	/...	124	pri
34	2...	H..	Tunnel to s...		660	
35	2...	H..	srv-exchange-...	/...	123	pri
36	2...	H..	srv-exchange-...	/...	279	pri
37	2...	H..	srv-exchange-...	/...	123	pri
38	2...	H..	srv-exchange-...	/...	180	pri
39	2...	H..	srv-exchange-...	/...	291	pri
40	2...	H..	Tunnel to s...		660	
41	4...	H..	srv-exchange-...	/...	0	
42	2...	H..	srv-exchange-...	/...	415	pri
43	2...	H..	srv-exchange-...	/...	1,227	pri
44	2...	H..	srv-exchange-...	/...	137	pri
45	2...	H..	srv-exchange-...	/...	294	pri
46	2...	H..	srv-exchange-...	/...	168	pri
47	2...	H..	srv-exchange-...	/...	177	pri
48	2...	H..	srv-exchange-...	/...	160	pri
49	2...	H..	srv-exchange-...	/...	160	pri
50	2...	H..	srv-exchange-...	/...	237	pri
51	2...	H..	srv-exchange-...	/...	189	pri

FiddlerScript | Log | Filters | Timeline

Get Started | Statistics | Inspectors | AutoResponder | Composer | Fiddler Orchestra Beta

Headers | TextView | SyntaxView | WebForms | HexView | MAPI | Auth | Cookies | Raw | JSON | XML

```
Origin:BOOKMARK_CURRENT
RowCount:1
WantRowMovedCount:False
-RopQueryRowsRequest
  -RopId:RopQueryRows
  -LogonId:1
  -InputHandleIndex:0
  -QueryRowsFlags:Advance
  -ForwardRead:True
  -RowCount:50
  -ServerObjectHandleTable:[16777221]
MaxRopOut:32775
AuxiliaryBufferSize:16
-AuxiliaryBuffer
  -RPCHEADEREXT
    -Version:0
    -Flags>Last
```

Response body is encoded. Click to decode.

Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | MAPI | Auth | Caching

Cookies | Raw | JSON | XML

```
RowCount:19
-RowData
  -PropertyRow
    -Flag:0
    -ValueArray
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyValue
      -PropertyRow
      -PropertyRow
      -PropertyRow
```

50 52 4F 43 45 53 53 49 4E 47 0D  
0A 44 4F 4E 45 0D 0A 58 2D 53 74  
61 72 74 54 69 6D 65 3A 20 46 72  
69 2C 20 30 32 20 46 65 62 20 32  
30 32 34 20 32 32 3A 31 37 3A 34  
30 20 47 4D 54 0D 0A 58 2D 45 6C  
61 70 73 65 64 54 69 6D 65 3A 20  
37 0D 0A 0D 0A 00 00 00 00 00 00  
00 00 00 00 00 00 59 04 00 00 00  
19 0A 18 00 00 00 00 00 00 01 00  
00 00 15 00 00 00 00 00 02 13 00  
00 01 00 00 00 00 00 01 0C 01 00  
00 00 0A DB 67 DE 01 00 00 00 0A  
DB 67 DE 00 00 00 00 01 00 00 00  
49 00 50 00 4D 00 2E 00 43 00 6F  
00 6E 00 66 00 69 00 67 00 75 00  
72 00 61 00 74 00 69 00 6F 00 6E  
00 2E 00 41 00 75 00 74 00 6F 00  
63 00 6F 00 6D 00 70 00 6C 00 65

Capturing | All Processes | 1 / 411 | https:// /mapi/emsmdb/?MailboxId=31d04b5e-e070-43a1-82a3-afdb25c658fc@gr

# Pinpointing issues

- User actions often entail multiple remote procedure calls.
- Request logging at e.g. the HTTP, DCERPC or ROP layers can help narrow down logic issues - (e.g. when packet framing is right but the content is not as expected)

```
[1/5] rop_dispatch(ropGetContentsTable) EC=ecSuccess RS=ecSuccess
[2/5] rop_dispatch(ropSetColumns) EC=ecSuccess RS=ecSuccess
[3/5] rop_dispatch(ropSortTable) EC=ecSuccess RS=ecSuccess
[4/5] rop_dispatch(ropSeekRow) EC=ecSuccess RS=ecSuccess
[5/5] rop_dispatch(ropFindRow) EC=ecSuccess RS=ecSuccess
Entering nsp_interface_get_specialtable: {container=0h record=0h delta=0 fpos=0/50}
Leaving nsp_interface_get_specialtable: {container=0h record=0h delta=0 fpos=0/50} {#outrows=2}
#0 (6 props)
#0 ~@~@~@~@dc^a7^c8^c0B^P^Z^b4^b9^H^@+/~e1^82^A^@~@~@~@A^@~@/~@
#1 (6 props)
#1 ~@~@~@~@dc^a7^c8^c0B^P^Z^b4^b9^H^@+/~e1^82^A^@~@~@~@A^@~@/~@/guid=81000003-0003-0000
6-e525584~@
[1/4] rop_dispatch(ropFindRow) EC=ecSuccess RS=ecNotFound
[1/5] rop_dispatch(ropFindRow) EC=ecSuccess RS=ecNotFound
^C[1/5] rop_dispatch(ropFindRow) EC=ecSuccess RS=ecNotFound
```

# Tools for protocol analysis: EWS

- observe Outlook etc. sending EWS requests (let gromox dump the XML)
- replay requests to an Exchange Server
- confer/compare with the specifications
- make Gromox respond to the EWS request

## **Clients**

- Outlook for Mac
- MacMail
- Evolution (partially)
- Postman / curl



- Menu
  - New Import
  - POST https://srv-exchange-01
  - POST https://srv-exchange-01
  - POST {{EWS\_URL}}
  - +
  - ...
- October 30
- POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
- October 26
- POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
  - POST {{EWS\_URL}}
- July 27
- POST {{EWS\_URL}}

HTTP {{EWS\_URL}}

POST {{EWS\_URL}} Send

Params Authorization Headers (9) Body Pre-request Script Tests Settings Cookies Beautify

none form-data x-www-form-urlencoded raw binary XML

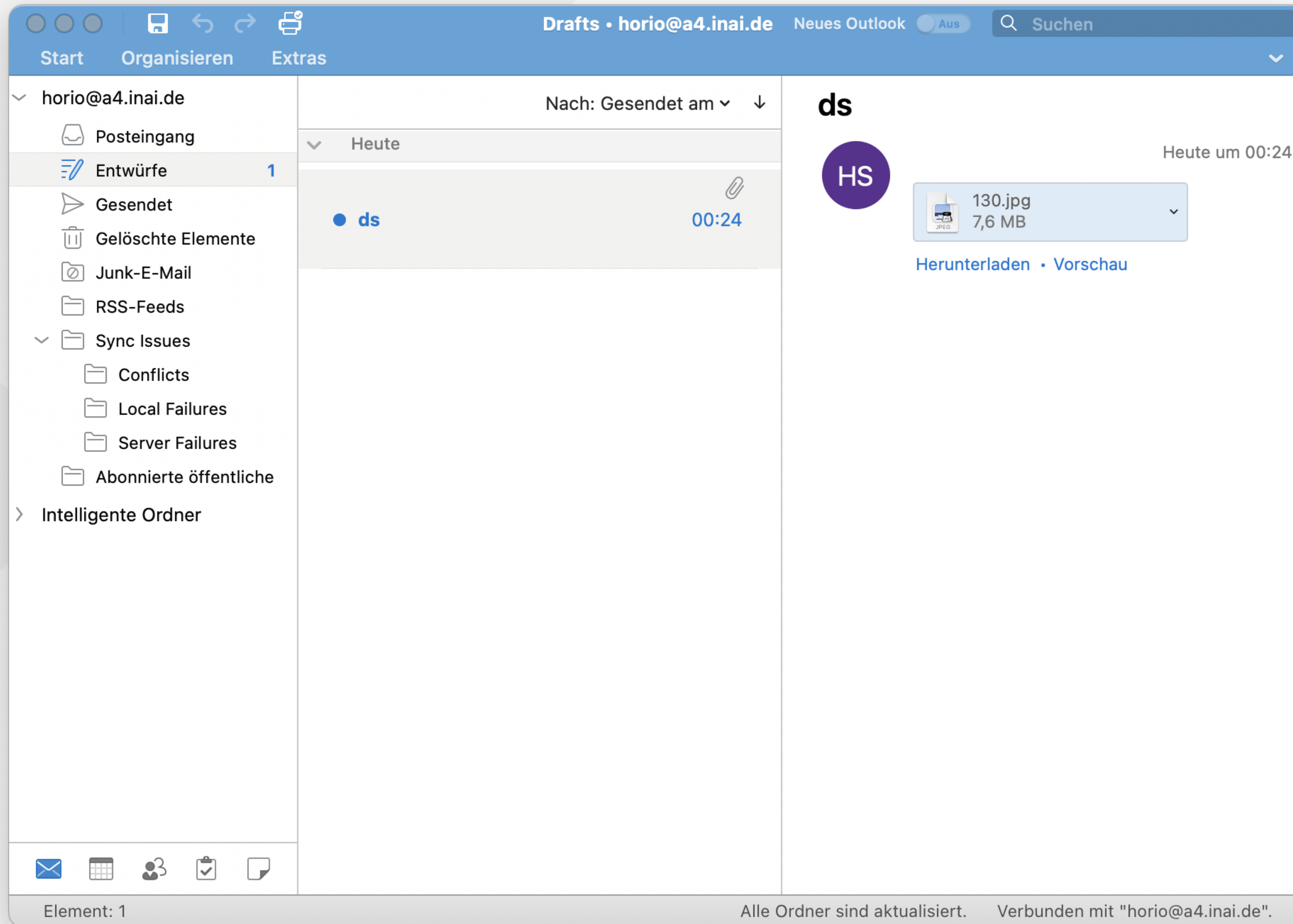
```
1 <?xml version="1.0" encoding="UTF-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
2   <soap:Header>
3     <t:RequestServerVersion Version="Exchange2013"/>
4     <t:MailboxCulture>en-US</t:MailboxCulture>
5     <t:TimeZoneContext>
6       <t:TimeZoneDefinition Id="E. South America Standard Time"/>
7     </t:TimeZoneContext>
8   </soap:Header>
9   <soap:Body>
10    <GetItem xmlns="http://schemas.microsoft.com/exchange/services/2006/messages">
11      <ItemShape>
12        <t:BaseShape>IdOnly</t:BaseShape>
13        <t:BodyType>HTML</t:BodyType>
14        <t:AdditionalProperties>
15          <t:FieldURI FieldURI="item:Sensitivity"/>

```

Body Cookies Headers Test Results Status: 200 OK Time: 161 ms Size: 4.56 KB Save Response

Pretty Raw Preview Visualize Text

1



The screenshot shows the Microsoft Outlook interface for the account **horio@a4.inai.de**. The window title is **Drafts • horio@a4.inai.de**. The interface is divided into three main sections:

- Left Navigation Pane:** Shows the folder structure for the account. The **Entwürfe** (Drafts) folder is selected and contains 1 item. Other folders include Posteingang, Gesendet, Gelöschte Elemente, Junk-E-Mail, RSS-Feeds, Sync Issues (with sub-folders for Conflicts, Local Failures, and Server Failures), Abonnierte öffentliche, and Intelligente Ordner.
- Center Pane:** Displays a list of drafts. The selected draft is from **ds**, sent on **00:24** today. A paperclip icon indicates an attachment.
- Right Pane:** Shows the details of the selected draft. The sender is **ds**. The draft is dated **Heute um 00:24**. It contains one attachment: **130.jpg** (7,6 MB). Below the attachment, there are links for **Herunterladen** (Download) and **Vorschau** (Preview).

At the bottom of the window, there is a status bar with the following information:

- Left: **Element: 1**
- Center: **Alle Ordner sind aktualisiert.**
- Right: **Verbunden mit "horio@a4.inai.de".**

+

Tag
Woche
Monat
Jahr

Suchen

## Februar 2024

<
Heute
>

Mo	Di	Mi	Do	Fr	Sa	So
29	30	31	1	2	3	4
5	Something to...	6	7	8	10	11
Rosenmontag	Faschingsdie...	12	13	14	17	18
19	20	21	22	23	24	25
26	27	28	29	1. März	2	3
4	5	6	7	8	9	10

<
Februar 2024
>

Mo	Di	Mi	Do	Fr	Sa	So
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	1	2	3
4	5	6	7	8	9	10

**Something to remember**

Standort oder Videoanruf hinzufügen

06.02.2024

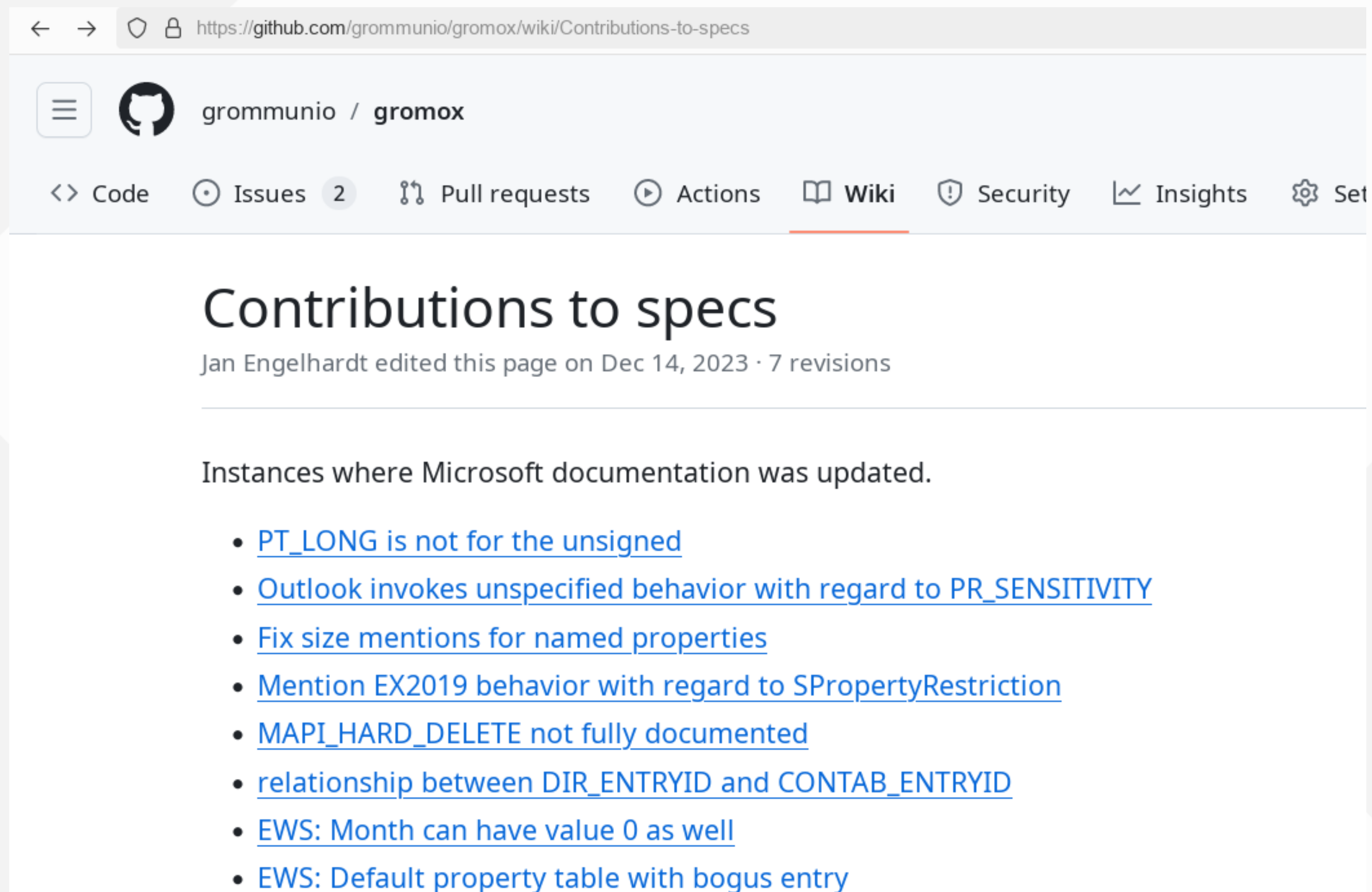
Personen einladen

This is a note

Anhang hinzufügen ...

# Fixing specification errors

<https://github.com/grommunio/gromox/wiki/Contributions-to-specs>



The screenshot shows a web browser displaying a GitHub Wiki page. The address bar shows the URL <https://github.com/grommunio/gromox/wiki/Contributions-to-specs>. The page header includes the GitHub logo, the repository name 'grommunio / gromox', and navigation tabs for Code, Issues (with a '2' badge), Pull requests, Actions, Wiki (which is selected and underlined), Security, Insights, and Settings. The main content area has the title 'Contributions to specs' and a subtitle 'Jan Engelhardt edited this page on Dec 14, 2023 · 7 revisions'. Below this, there is a section titled 'Instances where Microsoft documentation was updated.' followed by a bulleted list of links to specific specification errors.

Contributions to specs

Jan Engelhardt edited this page on Dec 14, 2023 · 7 revisions

Instances where Microsoft documentation was updated.

- [PT\\_LONG is not for the unsigned](#)
- [Outlook invokes unspecified behavior with regard to PR\\_SENSITIVITY](#)
- [Fix size mentions for named properties](#)
- [Mention EX2019 behavior with regard to SPropertyRestriction](#)
- [MAPI\\_HARD\\_DELETE not fully documented](#)
- [relationship between DIR\\_ENTRYID and CONTAB\\_ENTRYID](#)
- [EWS: Month can have value 0 as well](#)
- [EWS: Default property table with bogus entry](#)



C++17

PHP8

MAPI/HTTP

Message Information Store (w/SQLite)

DCE/RPC

EAS

EWS



NSP

Web

Zcore (PHP-MAPI Bridge)

EMS MDB

CalDAV

POP3

Autodiscover

Autoconfig

IMAP

CardDAV



# Future of gromox

- Better parallelization of accessing one and the same message store
- improved support for Internet Mail specs
- Graph API (See <https://github.com/grommunio/grommunio-next>)
- Continuing reporting spec errors/omissions (8400+ pages are not always right or complete)



Thanks!

Questions?