E-Mail

Hässlich, aber es funktioniert

@leyrer

Email ist immer noch super und unsere letzte, beste Hoffnung auf systemübergreifende Kommunikation.

– @leyrer

@MacLemon

Email ist irreparabel kaputt.

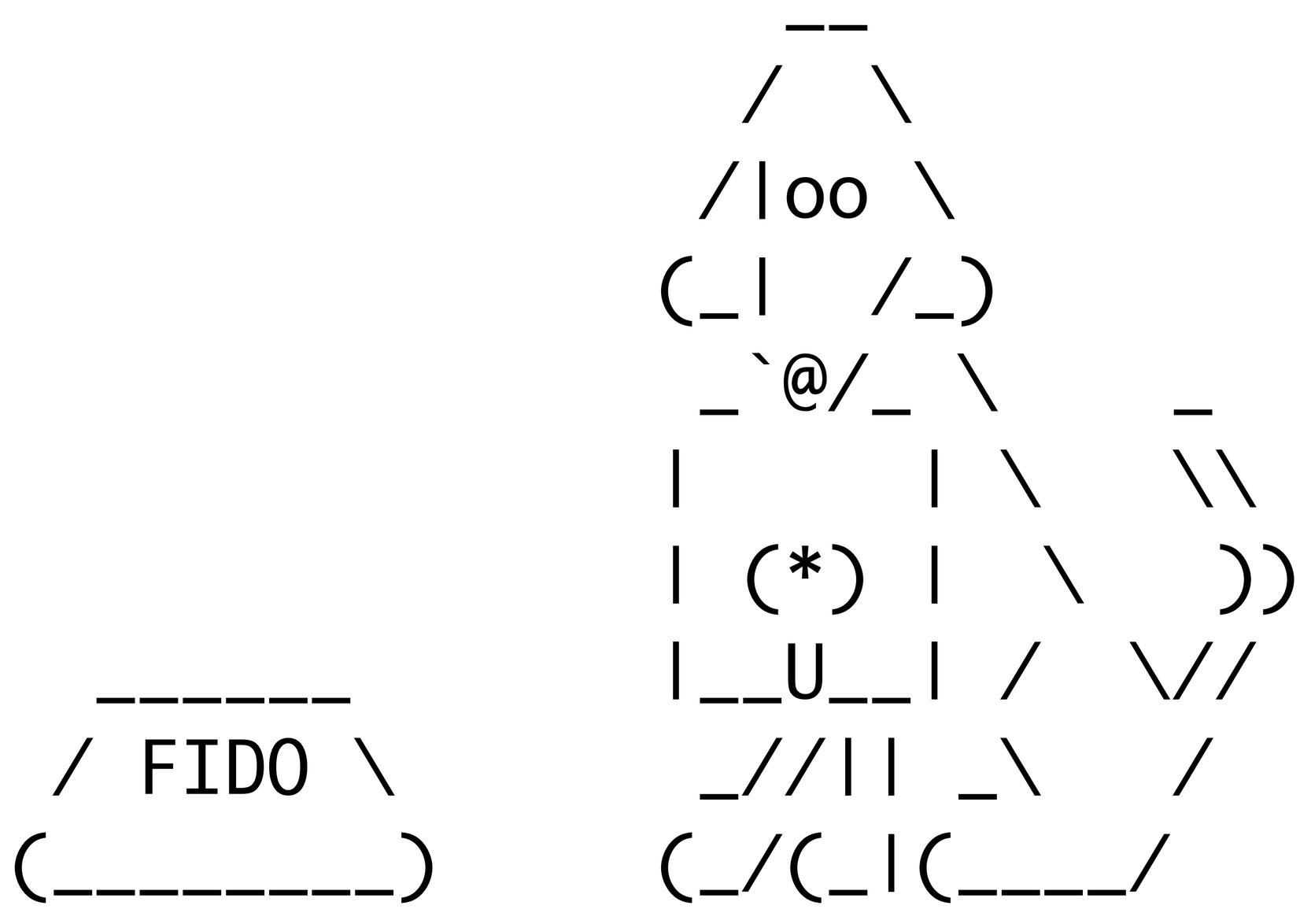
– @MacLemon

Abgrenzung

UUCP

X.25

X.400


FIDO

Telefaximile

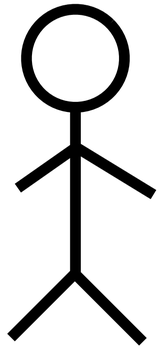
Internet Email

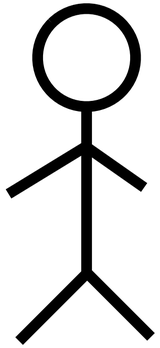
Fragen?

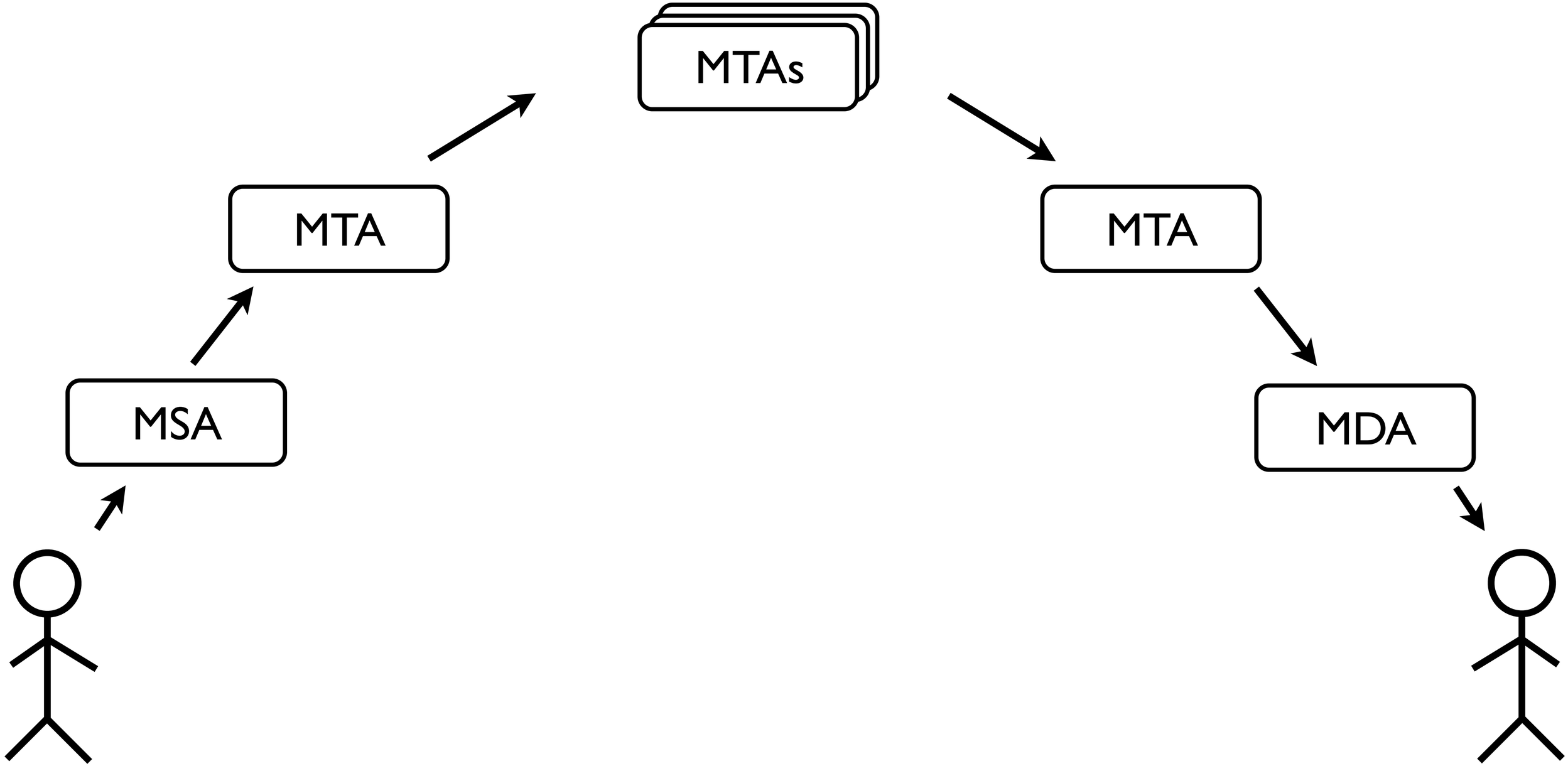
Wer verwendet noch Email?

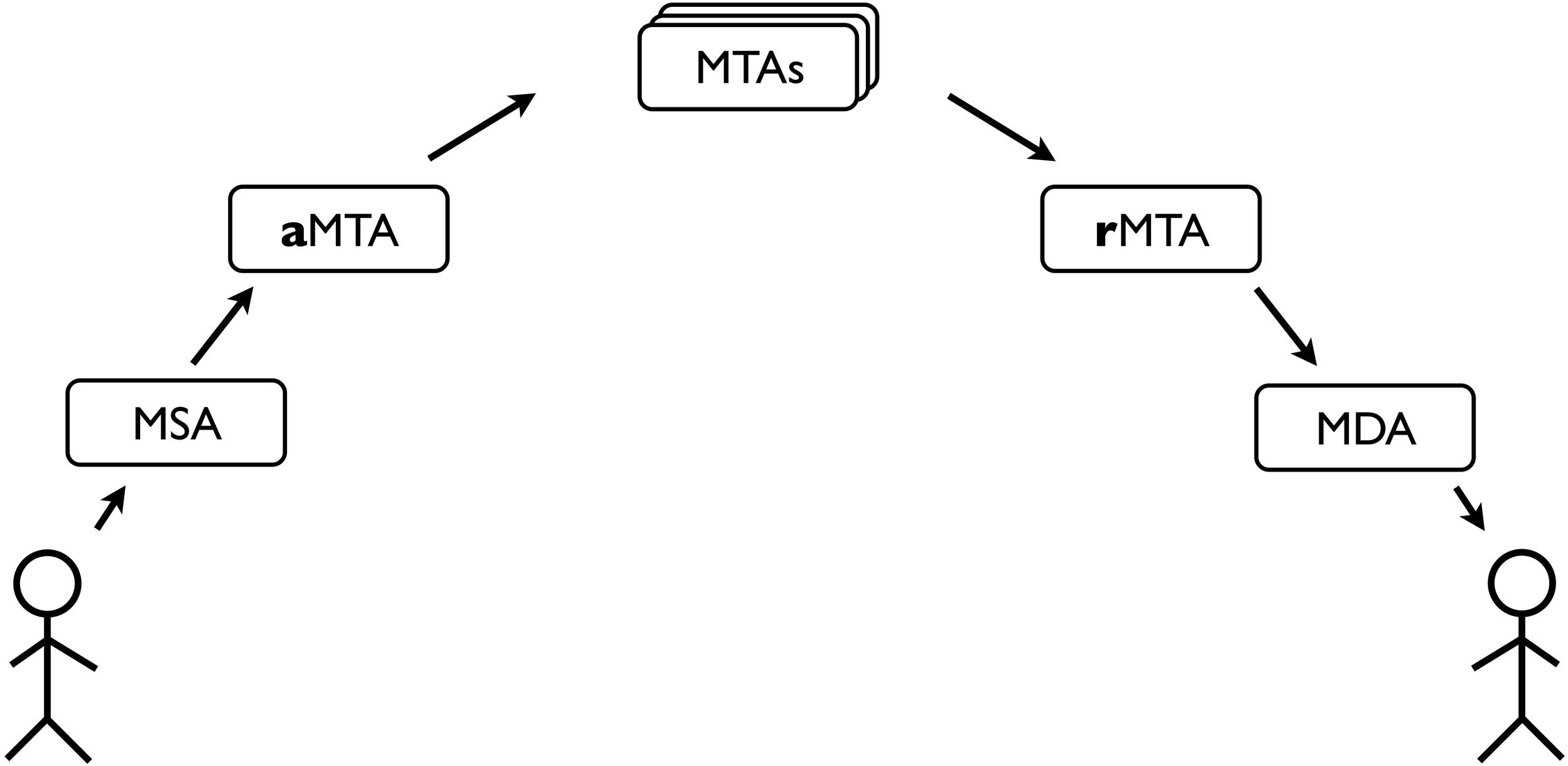
0. Akt

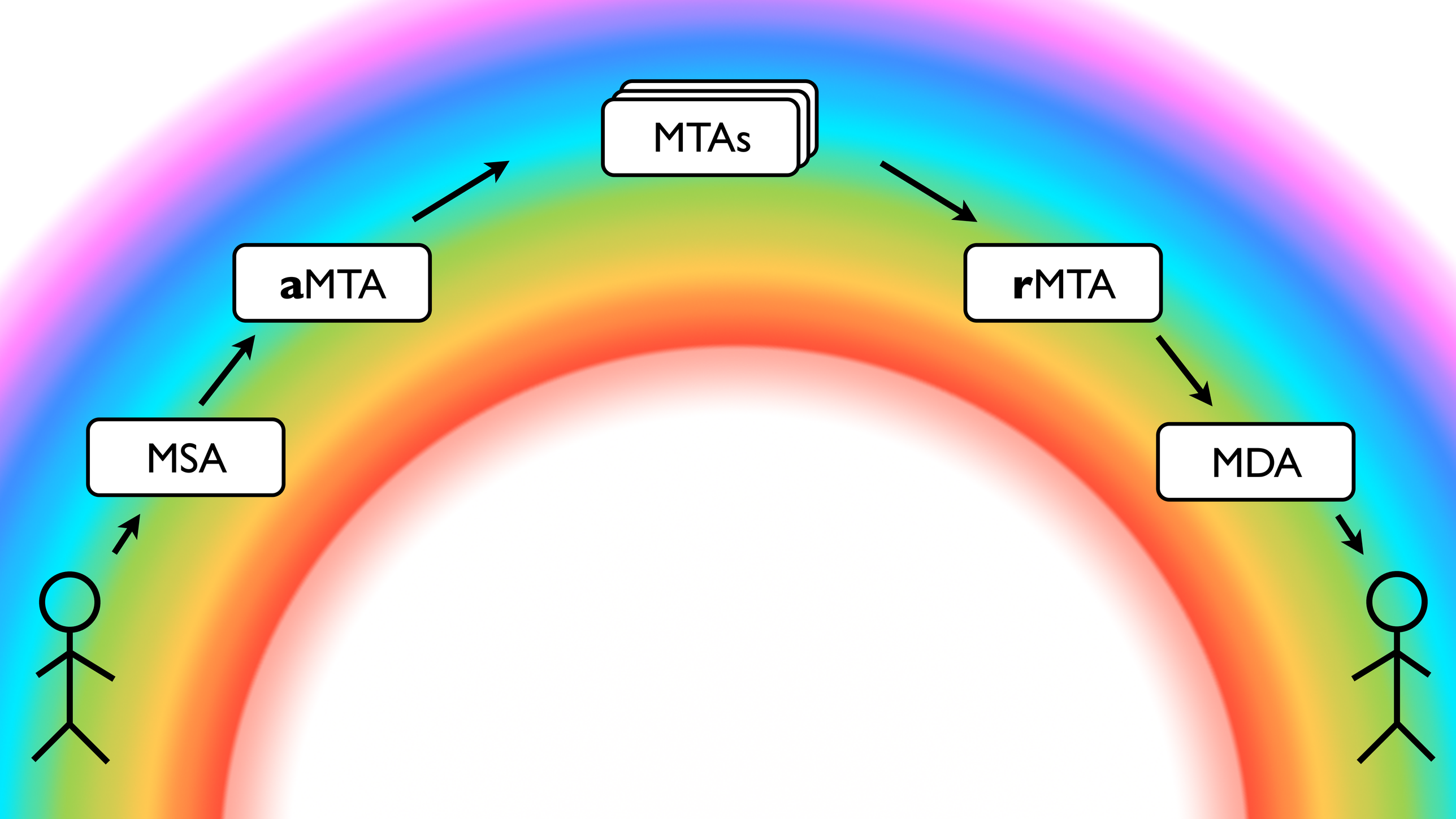
Wie funktioniert Email eigentlich?

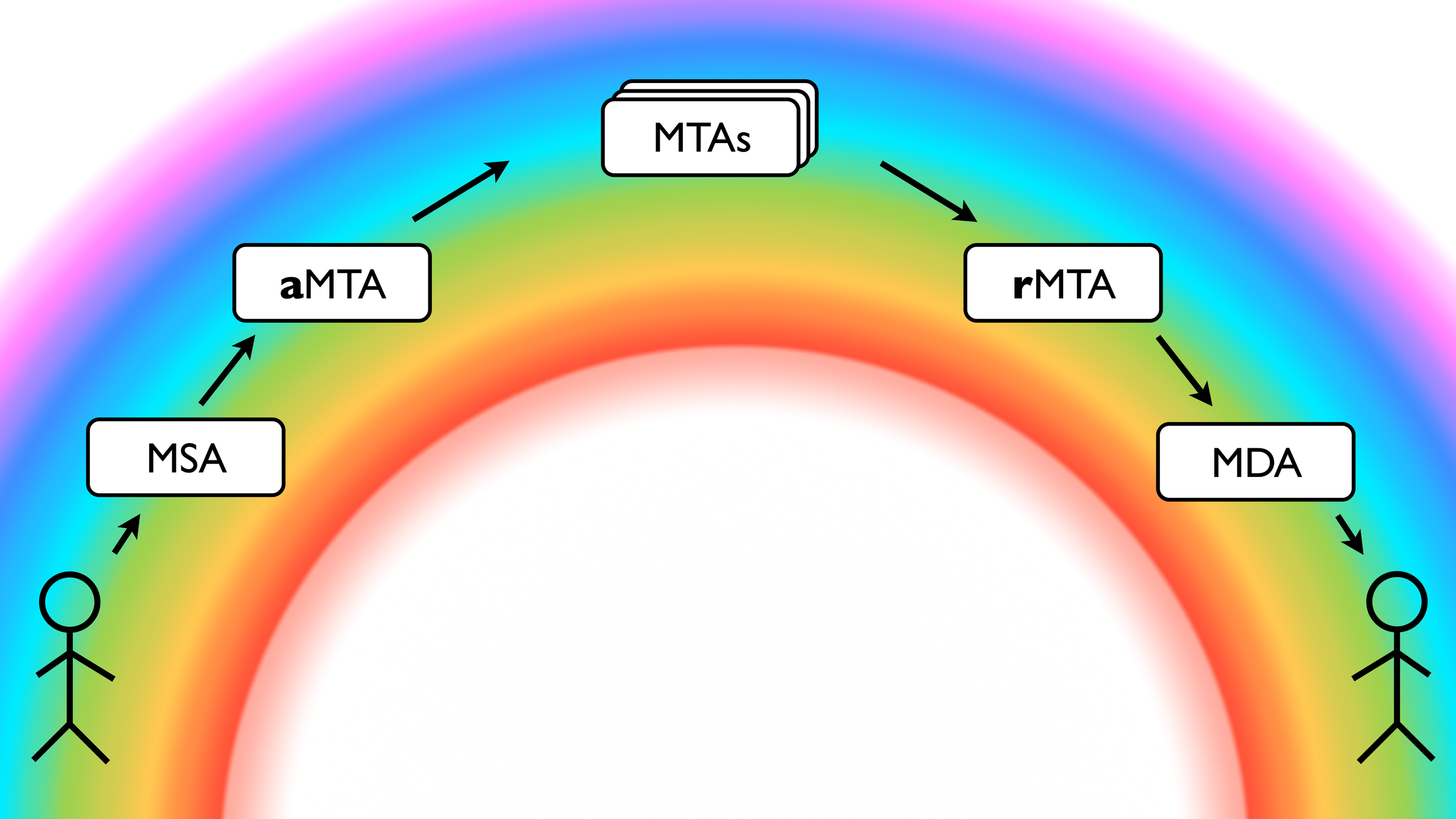





MTAs
MTA
MTA
MSA
MDA


MTAs
aMTA
rMTA
MSA
MDA


MTAs
aMTA
rMTA
MSA
MDA


MTAs
aMTA
rMTA
MSA
MDA

Envelope Header

Here's to the crazy ones. The misfits. The rebels. The troublemakers. The round pegs in the
square holes. The ones who see things differently. They're not fond of rules. And they have
no respect for the status quo. You can praise them, disagree with them, quote them, disbelieve
them, glorify or vilify them. About the only thing you can't do is ignore them. Because they
change things. They invent. They imagine. They heal. They explore. They create. They
inspire. They push the human race forward. Maybe they have to be crazy. How else can you

```
-----BEGIN PGP MESSAGE-----

hQEOA3MJaelH4lKFEAQAgbu3aFbD5z5pQEz
GxaoobXQNetKarRmFqG1tXLd2qLAs
pyTCysWxBfE04pPh9hORyWOBm2QPgA3GATm
v6D96VMP8WgdI2q/eeMkIRR10YbaZ
3UomVhcBW6phLSkLsIfnjODxD680ufUH7qB
Aw6mVGuKhUTt22erp6RueVo2ikhcE
ANVSOgtf+aWD/
n9Vr90lEMnL6YjsvVZQvIppgXNTUT0JCbhI
KJ4tAdX9s3HzDiTE
1a5N7aH1FGy/
rHp4YMqy1kJ9F57fj2eJtFylpfA8Z299eNb
mFFMBOYe56fjR4iOM
PIYO42xJajqrnHWJdhQVAwux7W1Yj19ci1K
cO+79SQAv0l4BoXPbIAGsAmaynzNt
gYoF61YteD3IBCJyWBfHg7s
+1QGNsSziB6qjWPSlZCsdQydO3/8K9fGkcR
NYKSqQ
uUiydE/38oBZwJ8Hktbd/
EQTcvwADbaJVPGjosh5nMdk
=87Ir
-----END PGP MESSAGE-----
```

@leyrer

Metalab

1010 Wien

```
-----BEGIN PGP MESSAGE-----

hQEOA3MJaelH4lKFEAQAgbu3aFbD5z5pQEz
GxaoobXQNetKarRmFqG1tXLd2qLAs
pyTCysWxBfE04pPh9hORyWOBm2QPgA3GATm
v6D96VMP8WgdI2q/eeMkIRR10YbaZ
3UomVhcBW6phLSkLsIfnjODxD680ufUH7qB
Aw6mVGuKhUTt22erp6RueVo2ikhcE
ANVSOgtf+aWD/
n9Vr90lEMnL6YjsvVZQvIppgXNTUT0JCbhI
KJ4tAdX9s3HzDiTE
1a5N7aH1FGy/
rHp4YMqy1kJ9F57fj2eJtFylpfA8Z299eNb
mFFMBOYe56fjR4iOM
PIYO42xJajqrnHWJdhQVAwux7W1Yj19ci1K
cO+79SQAv0l4BoXPbIAGsAmaynzNt
gYoF61YteD3IBCJyWBfHg7s
+1QGNsSziB6qjWPSlZCsdQydO3/8K9fGkcR
NYKSqQ
uUiydE/38oBZwJ8Hktbd/
EQTcvwADbaJVPGjosh5nMdk
=87Ir
-----END PGP MESSAGE-----
```

@leyrer

Metalab

1010 Wien

MAIL FROM:<fisch@linuxwochen.at>

RCPT TO:<ei@easterhegg.eu>

/ 0. Akt

1. Akt

Protokolle

<SMTP>

25/TCP

SMTP

MTA → MTA

Open Relay

SMTP

aMUA → MTA

<SUBMISSION>

587/TCP

SUBMISSION

aMUA → MSA

<IMAP4>

993/TCP

143/TCP

IMAP4

MDA → rMUA

<POP3>

995/TCP

110/TCP

POP3

MDA → rMUA

<TLS>
Transport Layer Security

Transportverschlüsselung

TLS 1.3

TLS 1.2

TLS 1.1

TLS 1.0

~~*SSLv3*~~

~~*SSLv2*~~

Mailbox names for common Services, Roles and Functions

Internet Services

Postmaster@ <SMTP>

Hostmaster@ <DNS>

Webmaster@ <HTTP>

Network Operations

Abuse@	Customer Relations
NOC@	Network Operations
Security@	Network Security

Business Related

Info@	Marketing
Marketing@	Marketing
Sales@	Sales
Support@	Customer Service

<DNS>

53/UDP & TCP

<DNS>

MX Record

```
$ host -t MX easterhegg.eu

easterhegg.eu mail is handled by
10 kilbeggan.fourecks.de.
```

Achievement unlocked

Du kannst nun Spam und Phishing Emails empfangen!

/ 1. Akt

2. Akt

<DNS>

53/UDP & TCP

<DNS>

MX Record

easterhegg.eu mail is handled by
10 kilbeggan.fourecks.de.

easterhegg.eu mail is handled by
10 kilbeggan.fourecks.de.

hase@easterhegg.eu

easterhegg.eu **mail is handled by**
10 kilbeggan.fourecks.de.

easterhegg.eu mail is handled by
10 **kilbeggan.fourecks.de.**

easterhegg.eu mail is handled by
10 kilbeggan.fourecks.de.

10
20
23
42
100
1337

10
10
10
23
42
1337

easterhegg.eu mail is handled by
10 **kilbeggan.fourecks.de.**

```
IN MX 10 kilbeggan.fourecks.de.
kilbeggan IN AAAA 2001:DB8::e99
```

```
IN MX 10 kilbeggan.fourecks.de.
kilbeggan IN CNAME kilkenny
```

IN MX 10 2001:DB8::e99

```
IN MX 10 kilbeggan.fourecks.de.
kilbeggan IN AAAA 2001:DB8::e99
kilbeggan IN A 88.198.54.132
```

```
IN MX 10 kilbeggan.fourecks.de.
kilbeggan IN AAAA 2001:DB8::e99
kilbeggan IN A 88.198.54.132
```

```
kilbeggan IN AAAA 2001:DB8::e99
kilbeggan IN A 88.198.54.132
```

```
easterhegg.eu. IN AAAA 2001:DB8::e99
easterhegg.eu. IN A 88.198.54.132
```

```
easterhegg.eu. IN AAAA 2001:DB8::e99
```

<DNS>

PTR

```
$ORIGIN 54.198.88.in-addr.arpa
132 IN PTR kilbeggan.fourecks.eu.
```

```
$ host -t MX easterhegg.eu

easterhegg.eu mail is handled by 10
kilbeggan.fourecks.de.
```

```
$ host kilbeggan.fourecks.de

kilbeggan.fourecks.de has address
88.198.54.132

kilbeggan.fourecks.de has IPv6
address 2a01:4f8:131:1302::1
```

```
$ host 88.198.54.132

132.54.198.88.in-addr.arpa domain
name pointer kilbeggan.fourecks.de.
```

```
$ host 2a01:4f8:131:1302::1

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.3
.1.1.3.1.0.8.f.4.0.1.0.a.2.ip6.arpa
domain name pointer
kilbeggan.fourecks.de.
```

<DNS>

FQDN

<DNS>

FQDN

Fully **Q**ualified **D**omain **N**ame

Ich mag keine Emails!

NULL MX

```
IN MX 0 .
```

```
$ host -t MX ssltest.security.fail

ssltest.security.fail mail is handled
by 0 .
```

Danke an @TheSecurityFail

Achievement unlocked

Achievement unlocked

SPF

Sender Policy Framework

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

```
example.com. IN TXT
"v=spf1 ip4:192.0.2.0/24
ip4:198.51.100.128
ip6:2001:DB8::e99/64 mx -all"
```

Qualifier

~ soft fail

- hard fail

+ no policy

DNS Typen

a

mx

all

/ SPF

/ Sender Policy Framework

Sender ID

spf2.0/mfrom
spf2.0/mfrom,pra
spf2.0/pra

spf2.0/mfrom
spf2.0/mfrom,pra
spf2.0/pra

spf2.0/mfrom
spf2.0/mfrom,pra
spf2.0/pra

spf2.0/mfrom
spf2.0/mfrom,pra
spf2.0/pra

/ Sender ID

DKIM

Domain Key Identified Mail

aMTA

+ DKIM-Signature:

rMTA

✔ From:

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODk
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODk
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODk
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OD
kwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

DKIM Setup

```
apt-get install dkim-filter
```

```
$ openssl genrsa -out \
default-2016-03-25.private 4096
```

```
$ openssl rsa -in \
default-2016-03-25.private -out \
default-2016-03-25.public -pubout \
-outform PEM

$ grep -v -e "^-" \
default-2016-03-25.public | tr -d "\n"
```

```
default-2016-03-25._domainkey IN TXT
"v=DKIM1\; k=rsa\; t=y\;
p=MIGfMA0GCSqGSIb3[…]EBAQUAA4GNADCB"
```

Postfix

```
$EDITOR main.cf

smtpd_milters = inet:localhost:8893
```

```
$EDITOR /etc/dkim-filter.conf
```

```
OmitHeaders  Return-
Path,Received,Comments,Keywords,Bcc,Resent-
Bcc
SubDomains yes
X-Header   yes
Background yes
Selector   default-2016-03-25
Canonicalization  relaxed/simple
KeyFile /etc/dkim/default-2016-03-25.private
```

/ DKIM

/ Domain Key Identified Mail

DMARC

Domain based **M**essage **A**uthentication, **R**eporting and **C**onformance

<DNS>

TXT

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

```
v=DMARC1; p=quarantine;
rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf; ri=86400
```

Postmark

https://dmarc.postmarkapp.com/

DMARC Weekly Digest

Postmark

May 26 – June 2 • wildbit.com

4,966	2,023	58
Processed	40% Fully Aligned	1% Failed

Trusted Sources 4,908

Trusted sources are servers that have passed DKIM, SPF or both when validated against your DNS records. To be fully DMARC compliant, both SPF and DKIM must be fully aligned according to your DMARC policy.

mtasv.net	Total	SPF ✓	SPF ✗	DKIM ✓	DKIM ✗
70.21.631.127	2,055	1,766	289	2,055	-
70.21.631.125	2,063	✓		✓	
70.21.631.121	310	305	5	310	-

/ DMARC

/ **D**omain based **M**essage **A**uthentication, **R**eporting and **C**onformance

Fazit

DANE

DNS-Based Authentication of Named Entities

/ 2. Akt

3. Akt

Blacklisting

RBLS, DNSBL

NiX Spam

http://www.dnsbl.manitu.net/

Greylisting

Greylisting

Whitelisting

Tarpitting

Early Talker

main.cf

```
smtpd_helo_required = yes
```

Rate limiting

Header Checks

Header Checks

X-Flags:
X-BeenThere:
X-Provags-ID:
X-Mailman-Version:
X-Enigmail-Version:
X-Y-GMX-Trusted:
X-Scan-Signature:
X-Gm-Message-State:
X-Google-DKIM-Signature:
X-To-Get-Off-This-List:
X-MS-TNEF-Correlator:
X-MS-Has-Attach:
X-GMX-Antivirus:
X-Amavis-Alert:
X-MSFBL:
X-Virus-Scanned:
X-Cron-Env:
X-Pgp-Agent:
X-GMX-Antispam:
X-Greylist:
X-Brightmail-Tracker:
X-Sender:
X-Originating-IP:
X-Dcc-Metrics:
X-PHP-Originating-Script:
X-GMX-UID:
X-OriginalArrivalTime:
X-Spam-Status:
X-Spam-Level:
X-Spam-Score:
X-Spam-Flag:
X-Inode-Forwarded:
X-Inode-Scanner:
X-Original-Sender:
X-SourceIP:
X-Content-Filtered-By:
X-Inode-SpamScore:
X-Inode-SpamReport:
X-Inode-SpamBar:
X-SA-Exim-Version:
X-Quarantine-ID:
X-Google-Sender-Auth:
X-Phorum:
X-Virus-Status:
X-YMail-OSG:
X-MIMEOLE:
X-MimeOLE:
X-MSMail-Priority:
X-Source:
X-Source-Dir:
X-Source-Args:
X-SA-Exim-Mail-From:
X-SA-Exim-Scanned:
X-Yahoo-Newman-Property:
X-Yahoo-Newman-Id:
X-SA-Exim-Connect-IP:
X-Image-Url:
X-Smtp-Server:
X-Mailman-Approved-At:

X-Original-To:
X-Sieve:
X-Mailer:
X-Received:
X-Inode-SpamFlag:
X-Facebook:
X-FuHaFi:
X-Facebook-Notify:
X-FACEBOOK-PRIORITY:
X-Universally-Unique-Identifier:
X-AntiAbuse:
X-MSMail-priority:
X-Sent-To:
X-MANTSH:
X-CLX-Spam:
X-CLX-Score:
X-Original-Authentication-Results:
X-GitHub-Recipient:
X-GitHub-Recipient-Address:
X-Authenticated-User:
X-SG-EID:
X-AuditID:
X-Sendgrid-EID:
X-Listbox-Post-Id:
X-Listbox-List-ID:
X-Brightmail-scanned:
X-Accept-Language:
X-SG-ID:
X-policyd-weight:
X-Info:
X-Authentication-Warning:
X-IP-stats:
X-Yahoo-SMTP:
X-twfbl:
X-CERTat-MailScanner:
X-CERTat-MailScanner-SpamCheck:
X-CERTat-MailScanner-ID:
X-CERTat-MailScanner-From:
X-Antivirus:
X-Priority:
X-Avast:
X-Antivirus-Status:
X-RT-Loop-Prevention:
X-Default-Received-SPF:
X-mailstream:
X-Sendgrid-ID:
X-CLX-Shades:
X-Report-Abuse:
X-Authenticated:
X-UI-Out-Filterresults:
X-Authenticated-Sender:
X-MyRbl:
X-Proofpoint-Spam-Details:
X-Proofpoint-Virus-Version:
X-Broadcast-Id:

X-Topics:
X-ACL-Warn:
X-Df-Sender:
X-Apple-Content-Length:
X-campaignid:
X-Campaign:
X-RZG-CLASS-ID:
X-RZG-AUTH:
X-Spam-Processed:
X-GMX-Htest:
X-Originating-Email:
X-bounce-key:
X-PMX-Version:
X-cid:
X-Spam:
X-MDaemon-Deliver-To:
X-Return-Path:
X-sgxh1:
X-DKIM_SIGN_REQUIRED:
X-Univie-Virus-Scan:
X-rext:
X-Enigmail-Draft-Status:
X-Scanned-By:
X-Notifications:
X-SpamDetect:
X-MEETUP-TRACK:
X-MEETUP-RECIP-ID:
X-TMN:
X-Notification-Type:
X-Sender-ID:
X-Notification-ID:
X-Notification-Category:
X-Google-Appengine-App-Id:
X-DKIM:
X-MDRemoteIP:
X-Sasl-Enc:
X-Spam-Checker-Version:
X-Complaints-To:
X-Authenticated-IP:
X-SEQ:
X-VirtualServerGroup:
X-HTTP-UserAgent:
X-IP:
X-EmailType-Id:
X-MailingID:
X-SMHeaderMap:
X-Destination-ID:
X-Request-ID:
X-Managed-By:
X-MailGenerator:
X-MDAV-Processed:
X-Get-Message-Sender-Via:
X-MEETUP-MESG-ID:
X-Github-Recipient:
X-Rocket-MIMEInfo:
X-VirtualServerGroup-Source:
X-Hostid:

X-Google-Appengine-App-Id-Alias:
X-RT-Original-Encoding:
X-Postfix-Sender:
X-Postfix-Queue-ID:
X-Feedback-ID:
X-Subject:
X-LinkedIn-fbl:
X-Apple-Base-Url:
X-MIMETrack:
X-Microsoft-Exchange-Diagnostics:
X-Attach-Flag:
X-Business-Group:
X-PHP-Script:
X-Campaign-ID:
X-Google-Group-Id:
X-Mailer-MsgId:
X-Mailer-CSID:
X-To:
X-Brightmail:
X-SA-Do-Not-Run:
X-MIME-Autoconverted:
X-Forwarded-Message-Id:
X-UI-Message-Type:
X-DomainKeys:
X-SES-Outgoing:
X-DCC-ZID-Univie-Metrics:
X-Forwarded-For:
X-LinkedIn-Class:
X-MC-User:
X-Forwarded-To:
X-LinkedIn-Template:
X-AntiVirus:
X-AV-Do-Run:
X-Spam-TU-Processing-Host:
X-Connecting-Host:
X-Connecting-Addr:
X-Sent-From:
X-Mailgun-Sid:
X-Auto-Response-Suppress:
X-OriginatingIP:
X-No-Archive:
X-Cloudmark-Score:
X-Spam-DCC:
X-IronPort-Anti-Spam-Result:
X-IronPort-Anti-Spam-Filtered:
X-IronPort-AV:
X-HELO-Warning:
X-BTPH:
X-A1Mail-Track-Id:
X-message-flag:
X-SMType:
X-SMSignature:
X-SMRef:

X-Rocket-Received:
X-SpamTest-Info:
X-TorMail-User:
X-AOL-IP:
X-Accounttype:
X-Suspected-Spam:
X-Reply-To:
X-Forefront-Antispam-Report:
X-List-Administrivia:
X-Authority-Analysis:
X-DKIM-Authentication-Results:
X-Library:
X-Abuse:
X-PVIQ:
X-CTCH-RefID:
X-Bounce:
X-Ack:
X-Injected-Via-Gmane:
X-Gmane-NNTP-Posting-Host:
X-CSA-Complaints:
X-CLX-UnSpecialScore:
X-Apple-Mail-Signature:
X-ecm-part-format:
X-mailer:
X-H-Notify:
X-Forefront-PRVS:
X-Apple-Mail-Remote-Attachments:
X-Twitterimpressionid:
X-PhaseofMoon:
X-WR-ALARMUID:
X-Sasl-enc:
X-Steve:
X-Apple-Windows-Friendly:
X-Google-Original-From:
X-ABUID:
X-Footer:
X-Mao-Original-Outgoing-Id:
X-Should-Pgp-Sign:
X-Should-Pgp-Encrypt:
X-Request-UUID:
X-All-Senders-In-Circles:
X-Eon-Sig:
X-Eon-Dm:
X-Apple-Auto-Saved:
X-Return-Receipt-To:
X-Notes-Item:
X-Disposition-Notification-To:
X-MB-Message-Type:
X-MB-Message-Source:
X-X-Sender:
X-Spam-Report:
X-no-archive:
X-Sequence:
X-Phorum--Version:
X-Phorum--Thread:
X-Phorum--Parent:
X-Phorum--Forum:
X-smtpID:

X-Apple-Mail-Stationery:
X-TradeDoubler-MailID:
X-TradeDoubler-EmailId:
X-TradeDoubler-EmailCategoryType:
X-MS-Exchange-Transport-CrossTenantHeadersStamped:
X-Modwest-MailScanner:
X-Binding:
X-jID:
X-cuID:
X-cID:
X-aID:
X-Gpgmail-State:
X-Mimeole:
X-AOL-SENDER:
X-LLPP:
X-Glassboard-Message-ID:
X-CTCH-Spam:
X-URL:
X-Failed-Recipients:
X-MailScanner-From:
X-MA-Reference:
X-Elrippo-NOT-TRUSTED-Header:
X-Mokka:
X-Apple-Mail-Plain-Text-Draft:
X-eC-messenger-mid:
X-eC-messenger-email:
X-eC-messenger-cid:
X-Type:
X-Server-Quench:
X-RCPT-To:
X-Mail-From:
X-Authentic-SMTP:
X-AuthRoute:
X-nextra-mail01-rcpt:
X-WR-CALNAME:
X-CTCH-VOD:
X-CTCH-Flags:
X-AMAZON-RTE-VERSION:
X-AMAZON-MAIL-RELAY-TYPE:
X-Face:
X-UFL-Spam-Level:
X-rim-org-msg-ref-id:
X-Trac-Version:
X-Trac-Project:
X-Resent-To:
X-Resent-For:
X-Resent-By:
X-Microsoft-Antispam:
X-Interia-Antivirus:
X-FID:
X-Trac-Ticket-URL:
X-Trac-Ticket-ID:
X-Exchange-Antispam-Report-CFA-Test:
X-MS-Exchange-CrossTenant-OriginalArrivalTime:

X-MS-Exchange-CrossTenant-FromEntityHeader:
X-Exchange-Antispam-Report-Test:
X-Microsoft-Antispam-PRVS:
X-Inode-ss:
X-PGP-Fingerprint:
X-Mail-Calendar-Part:
X-Language-Identified:
X-AuthFastPath:
X-RocketYMMF:
X-EOPAttributedMessage:
X-Mandrill-User:
X-AuthReport-Spam:
X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp:
X-MS-Exchange-CrossTenant-Id:
X-info1:
X-code:
X-Unsubscribe-Web:
X-KeepSent:
X-Message-Info:
X-Matching-Connectors:
X-CTCH-ScoreCust:
X-CTCH-Score:
X-CTCH-Rules:
X-CTCH-SenderID:
X-CTCH-SenderID-TotalVirus:
X-CTCH-SenderID-TotalSuspected:
X-CTCH-SenderID-TotalSpam:
X-CTCH-SenderID-TotalRecipients:
X-CTCH-SenderID-TotalMessages:
X-CTCH-SenderID-TotalConfirmed:
X-CTCH-SenderID-TotalBulk:
X-CTCH-SenderID-BlueWhiteFlag:
X-ClientProxiedBy:
X-TM-AS-Product-Ver:
X-Mailer-SID:
X-TM-AS-Result:
X-Mailer-Sent-By:
X-Mailer-LID:
X-GPG-Fingerprint:
X-Match:
X-Scanner:
X-ME-Bayesian:
X-Elrippo-SMTP-Header:
X-IADB-IP:
X-IADB-IP-REVERSE:
X-Campaignid:
X-MarketoID:
X-Mailfrom:
X-Ffncampaignrp-ID:
X-Mailer-RecptId:
X-Twittersenderscreenname:

X-Twittersendername:
X-Twittersenderid:
X-Twitterrecipientscreenname:
X-Twitterrecipientname:
X-Twitterrecipientid:
X-Twitteremailtype:
X-Twittercreatedat:
X-BLTSYMAVREINSERT:
X-Recipient:
X-Friv-Forum:
X-DSNContext:
X-Confirm-Reading-To:
X-eC-messenger-sender-domain:
X-VirusChecked:
X-StarScan-Version:
X-Inode-Mailcheck:
X-Env-Sender:
X-BigFish:
X-SpamTest-Version:
X-Msg-Ref:
X-Barracuda-URL:
X-Barracuda-Start-Time:
X-Barracuda-Connect:
X-ASG-Orig-Subj:
X-ASG-Debug-ID:
X-Modwest-MailScanner-From:
X-CNFS-Analysis:
X-CM-Score:
X-return-path-rewrite:
X-Yandex-Uniq:
X-Tracker:
X-SpamTest-Status:
X-SpamScore:
X-Spam-RelayCountries:
X-Spam-Language:
X-MessageID:
X-ref:
X-ray:
X-TNEFEvaluated:
X-PMWin-Version:
X-Campaign-Id:
X-CCS-MailScanner:
X-CCS-MailScanner-Info:
X-Original-MessageID:
X-nextra-mail02-rcpt:
X-WU-uvscan-status:
X-User-Agent:
X-Ivanova:
X-Originating-Ip:
X-Barracuda-Envelope-From:
X-ListMember:
X-Report-Abuse-To:
X-AuthVirus-Status:
X-eC-messenger-token:
X-TRID:
X-SpamTest-Status-Extended:
X-SpamTest-Rate:
X-SpamTest-Method:
X-SpamTest-Group-ID:

main.cf

```
header_checks = regexp:/etc/postfix/
                header_checks
```

```
/^Date: .* 199[0-9]/                REJECT \
Your mail Date is way in the past, please
 buy a realtime clock for your computer!
```

/^X-LinkedIn-Class: / REJECT Go away!

Body Checks

main.cf

```
body_checks = pcre:/etc/postfix/
body_checks
```

Spamassassin

master.cf

```
smtp inet n - - - - smtpd
   -o content_filter=spamassassin
submission inet n - - - - smtpd
   -o content_filter=spamassassin

spamassassin unix - n n - - pipe
  user=debian-spamd argv=/usr/bin/spamc -f
-e /usr/sbin/sendmail -oi -f ${sender} $
{recipient}
```

```
# How many hits before a message is
considered spam.

required_hits                 5.0
```

```
# Text to prepend to subject if
rewrite_subject is used

rewrite_header Subject  [**Lovely SPAM**]
```

```
add_header all Status _YESNO_,
score=_SCORE_ required=_REQD_
tests=_TESTS_ autolearn=_AUTOLEARN_
version=_VERSION_
```

```
X-Spam-Status: No, score=-1.9 required=3.5
tests=AWL,BAYES_00,SPF_PASS,
 T_RP_MATCHES_RCVD autolearn=ham
version=3.3.1
```

```
whitelist_from_dkim *@easterhegg.eu \
easterhegg.eu

score USER_IN_DKIM_WHITELIST -4.0
score DKIM_VERIFIED -1.3
score DKIM_POLICY_TESTING 0
```

AntiVirus, -Malware, -Phishing

ClamAV/Clamd

Pyzor

Razor

Amavisd-new

Local Delivery

LMDA

main.cf

```
virtual_transport = lmtp:unix:private/
dovecot-lmtp
```

Dovecot

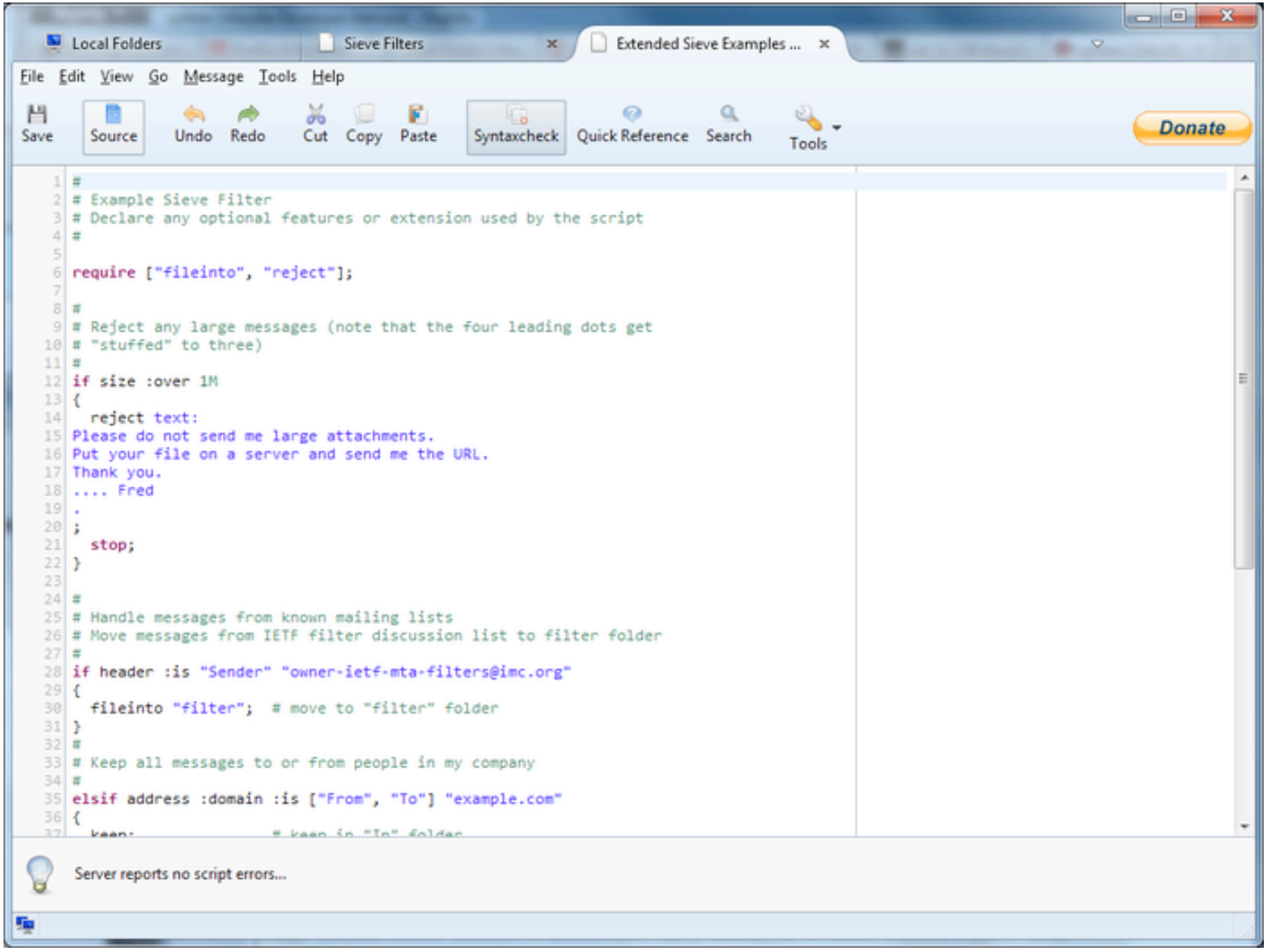
/etc/dovecot/conf.d/20-lmtp.conf

```
protocol lmtp {
  postmaster_address =
postmaster@domainname   # required
  mail_plugins = quota sieve
}
```

Filtering/Sorting

```
if address :is ["From", "To"]
"mailinglist@example.com" {
   fileinto "INBOX.mailinglist";
}
```

<Managesieve>

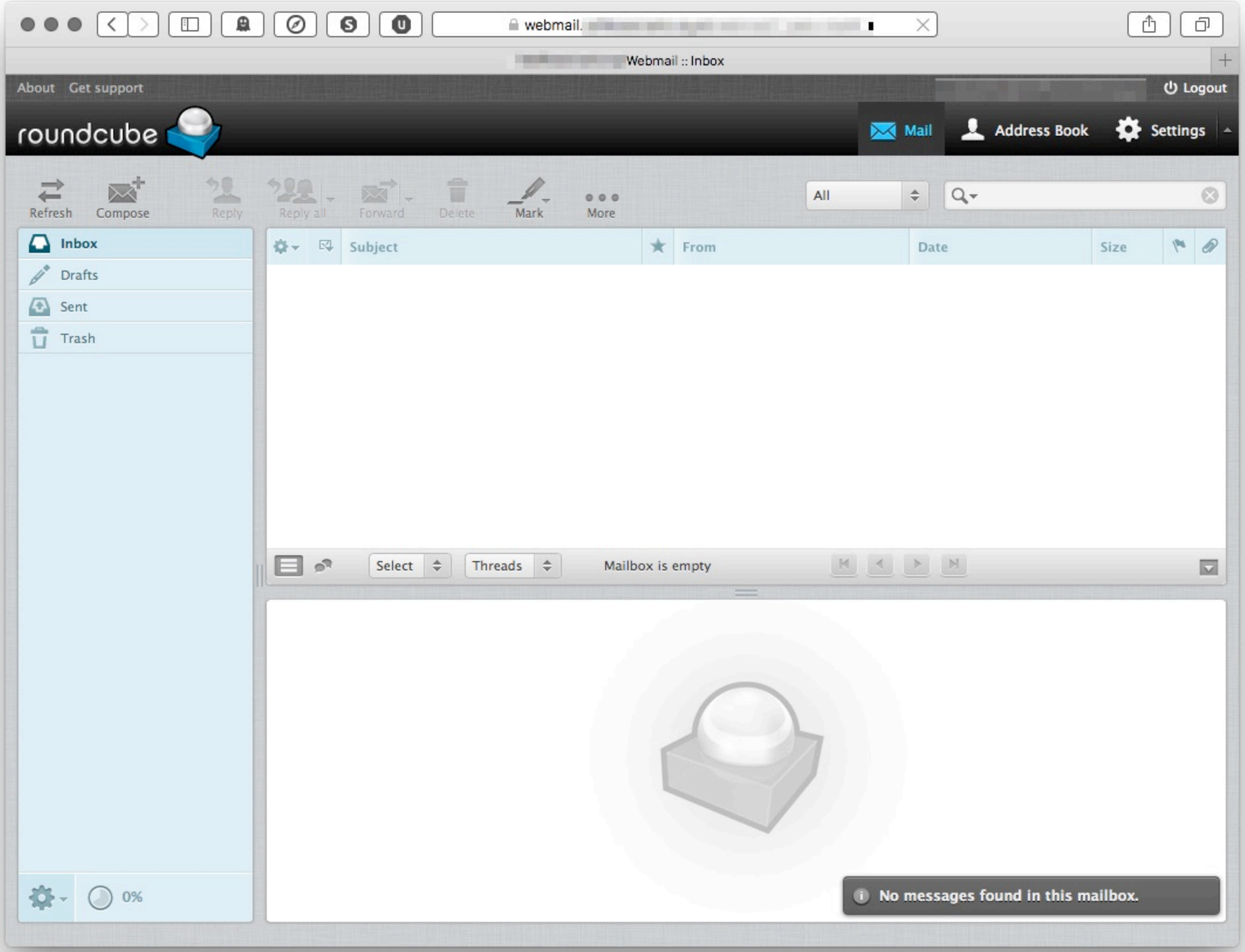

Local Folders
Sieve Filters
Extended Sieve Examples ...
File Edit View Go Message Tools Help
Save
Source
Undo
Redo
Cut
Copy
Paste
Syntaxcheck
Quick Reference
Search
Tools
Donate
1 #
2 # Example Sieve Filter
3 # Declare any optional features or extension used by the script
4 #
5
6 require ["fileinto", "reject"];
7
8 #
9 # Reject any large messages (note that the four leading dots get
10 # "stuffed" to three)
11 #
12 if size :over 1M
13 {
14 reject text:
15 Please do not send me large attachments.
16 Put your file on a server and send me the URL.
17 Thank you.
18 .... Fred
19 .
20 ;
21 stop;
22 }
23
24 #
25 # Handle messages from known mailing lists
26 # Move messages from IETF filter discussion list to filter folder
27 #
28 if header :is "Sender" "owner-ietf-mta-filters@imc.org"
29 {
30 fileinto "filter"; # move to "filter" folder
31 }
32 #
33 # Keep all messages to or from people in my company
34 #
35 elsif address :domain :is ["From", "To"] "example.com"
36 {
Server reports no script errors...

/ 3. Akt

4. Akt

Webmail

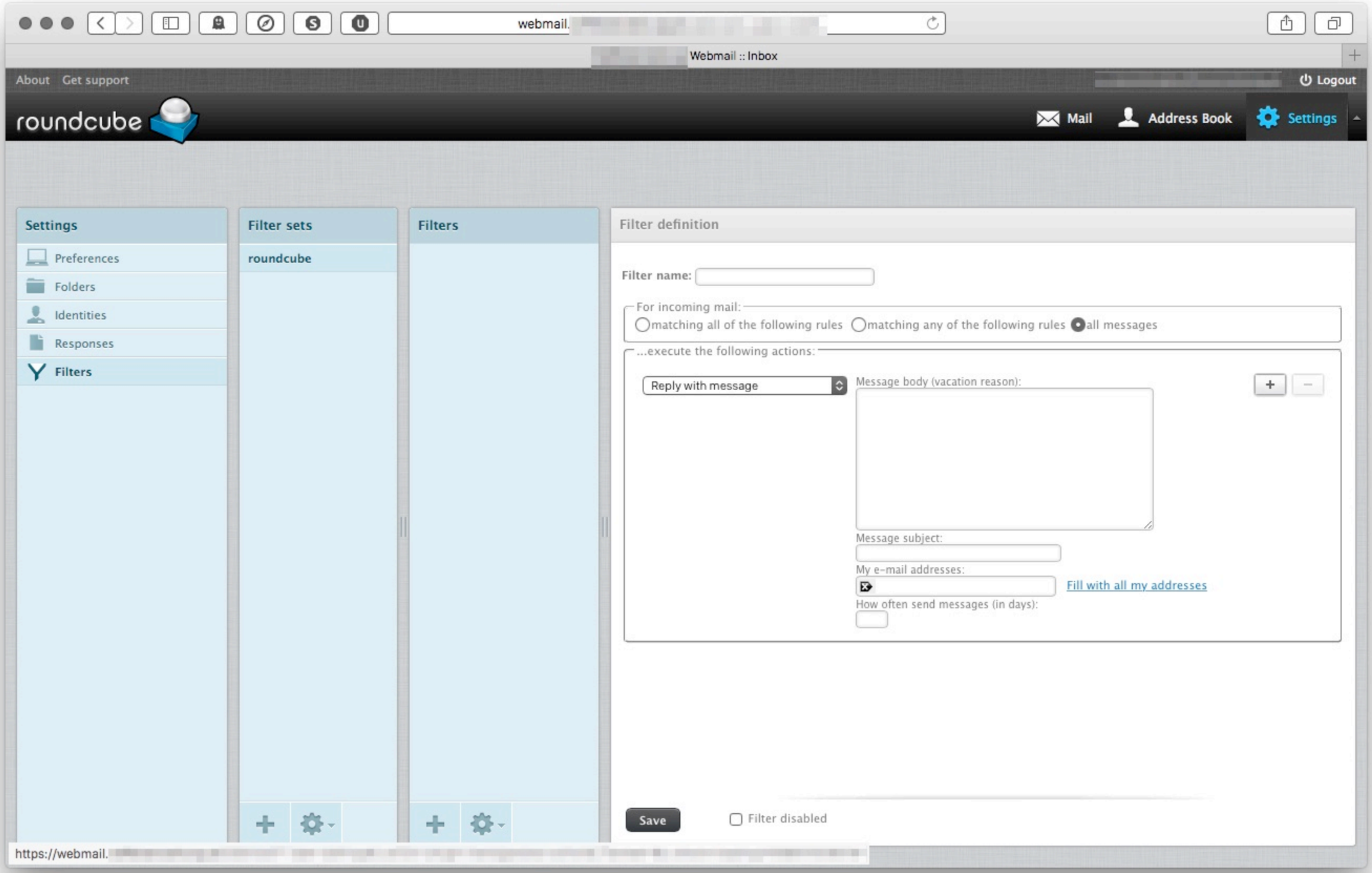
roundcube


webmail.
Webmail :: Inbox
About
Get support
Logout
roundcube
Mail
Address Book
Settings
Refresh
Compose
Reply
Reply all
Forward
Delete
Mark
More
All
Inbox
Drafts
Sent
Trash
Subject
From
Date
Size
Select
Threads
Mailbox is empty
0%
No messages found in this mailbox.

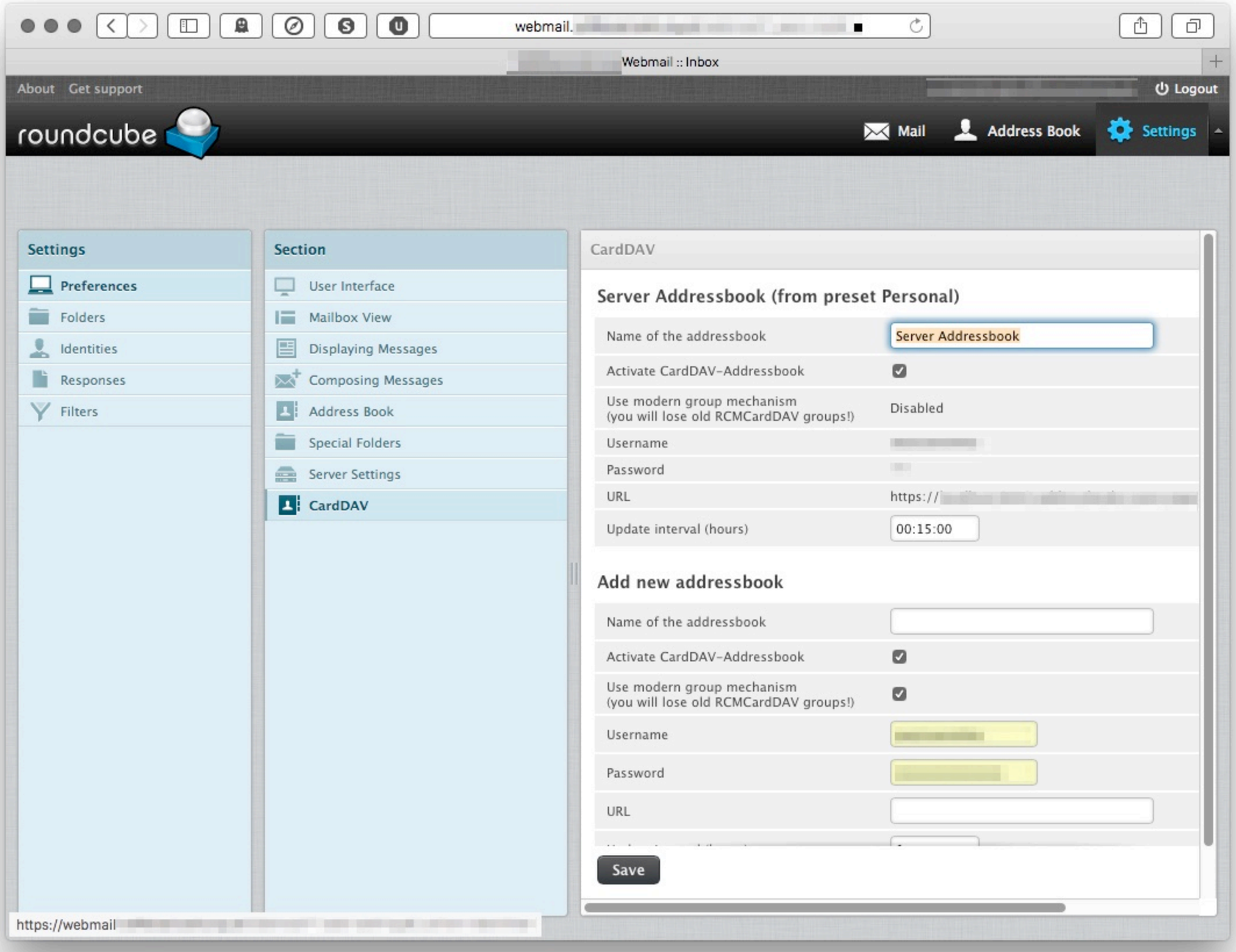
Roundcube Plugins

https://plugins.roundcube.net/

johndoh/sieverules

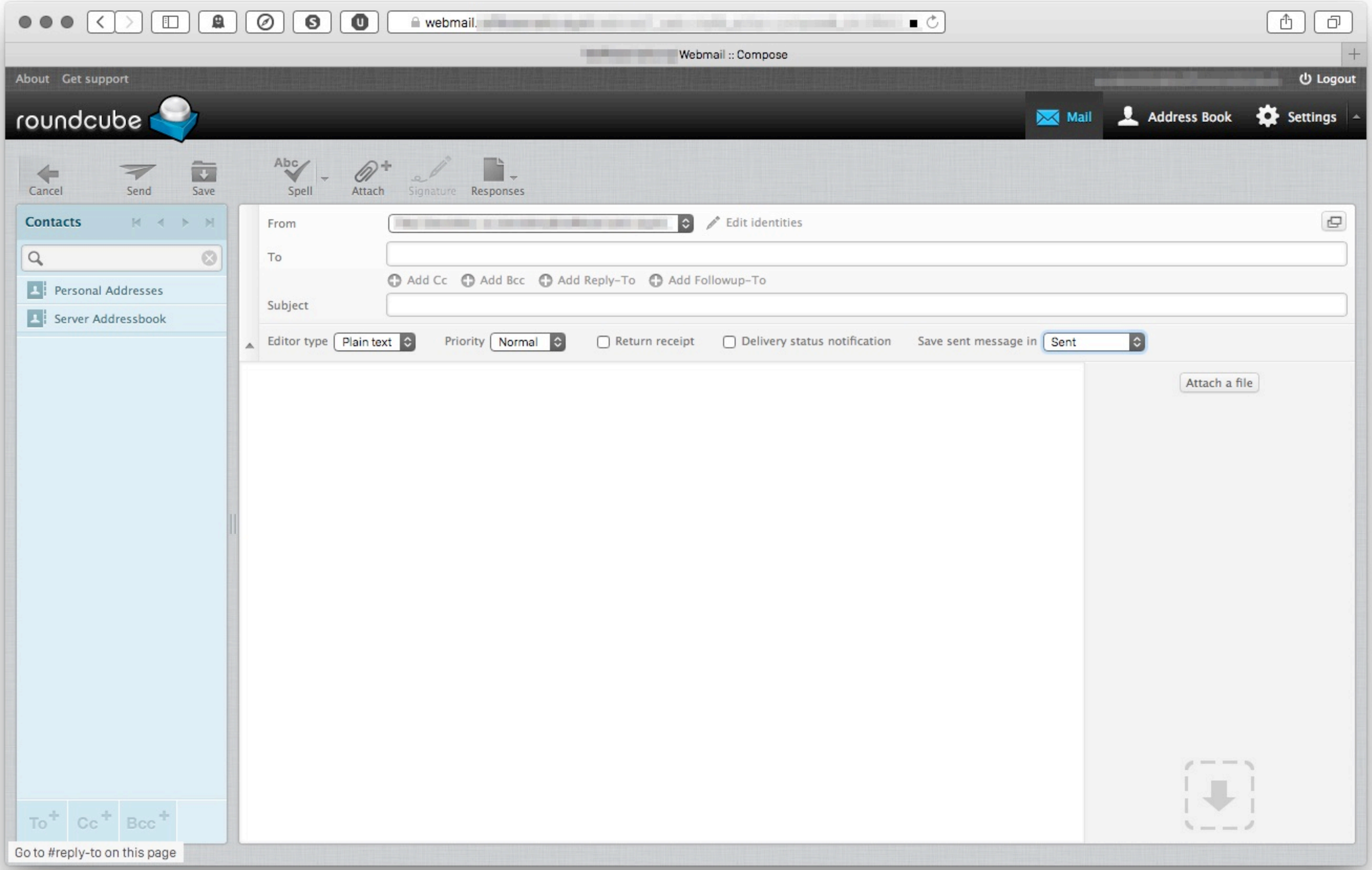

webmail.
Webmail :: Inbox
About
Get support
Logout
roundcube
Mail
Address Book
Settings
Settings
Preferences
Folders
Identities
Responses
Filters
Filter sets
roundcube
Filters
Filter definition
Filter name:
For incoming mail:
matching all of the following rules
matching any of the following rules
all messages
...execute the following actions:
Reply with message
Message body (vacation reason):
Message subject:
My e-mail addresses:
Fill with all my addresses
How often send messages (in days):
Save
Filter disabled
https://webmail.

roundcube/carddav


webmail.
Webmail :: Inbox
About
Get support
Logout
roundcube
Mail
Address Book
Settings
Settings
Preferences
Folders
Identities
Responses
Filters
Section
User Interface
Mailbox View
Displaying Messages
Composing Messages
Address Book
Special Folders
Server Settings
CardDAV
CardDAV
Server Addressbook (from preset Personal)
Name of the addressbook
Server Addressbook
Activate CardDAV-Addressbook
Use modern group mechanism
(you will lose old RCMCardDAV groups!)
Disabled
Username
Password
URL
https://
Update interval (hours)
00:15:00
Add new addressbook
Name of the addressbook
Activate CardDAV-Addressbook
Use modern group mechanism
(you will lose old RCMCardDAV groups!)
Username
Password
URL
Save
https://webmail

jirutka/virtuser_ldap

mat_krauser/image_paster


webmail.
Webmail :: Compose
About
Get support
Logout
roundcube
Mail
Address Book
Settings
Cancel
Send
Save
Spell
Attach
Signature
Responses
Contacts
Personal Addresses
Server Addressbook
From
Edit identities
To
Add Cc
Add Bcc
Add Reply-To
Add Followup-To
Subject
Editor type
Plain text
Priority
Normal
Return receipt
Delivery status notification
Save sent message in
Sent
Attach a file
To
Cc
Bcc
Go to #reply-to on this page

roundcube/customizr

roundcube/chbox

kitist/html5_notifier

Two-Factor-Authentication

northox/roundcube-yubikey-plugin
alexandregz/twofactor_gauthenticator
rcdevs/openotp_authentication

Push Notifications für

https://github.com/st3fan/dovecot-xaps-daemon

st3fan / **dovecot-xaps-daemon**

Watch 21 Star 67 Fork 9

Code Issues 4 Pull requests 1 Pulse Graphs

No description or website provided.

53 commits **2** branches **4** releases **2** contributors

Branch: **master** New pull request New file Find file HTTPS https://github.com/st3fan Download ZIP

st3fan Added a basic systemd service file — Latest commit **7ea8a01** on 23 May 2015

etc	Added a basic systemd service file	10 months ago
src/cmd/xapsd	Logging improvements	10 months ago
vendor/src/github.com/st3fan/apns	Import of dependencies	10 months ago
.gitignore	Changed gitignore to match a Go project	10 months ago
.travis.yml	Added a travis file	10 months ago
LICENSE	Added the MIT licence	2 years ago
README.md	Added a build status image to the README	10 months ago

/ 4. Akt

iRedMail - Free, Open Source Mail Server Solution

The right way to build your mail server with open source softwares. Since 2007.
Works on Red Hat Enterprise Linux, CentOS, Debian, Ubuntu, FreeBSD, OpenBSD.

DOWNLOAD NOW

With iRedMail, you can deploy an **OPEN SOURCE**, **FULLY FLEDGED**, **FULL-FEATURED** mail server in several minutes, for free.

We did the heavy lifting of putting all the open source components together and applying best practices. Our product does all the major tasks for you. Furthermore we offer professional support to back you up in case you have some problems.

Why iRedMail

Privacy

You have all personal data on your own hard disk, you can control the email security, inspect transaction log. No other

Open Source

All components used in iRedMail are open source softwares, and you get the bug fixes and updates from the Linux/BSD

Secure By Default

End users are forced to use mail services through secure connections (POP3/IMAP/SMTP over TLS, webmail

@leyrer
@MacLemon