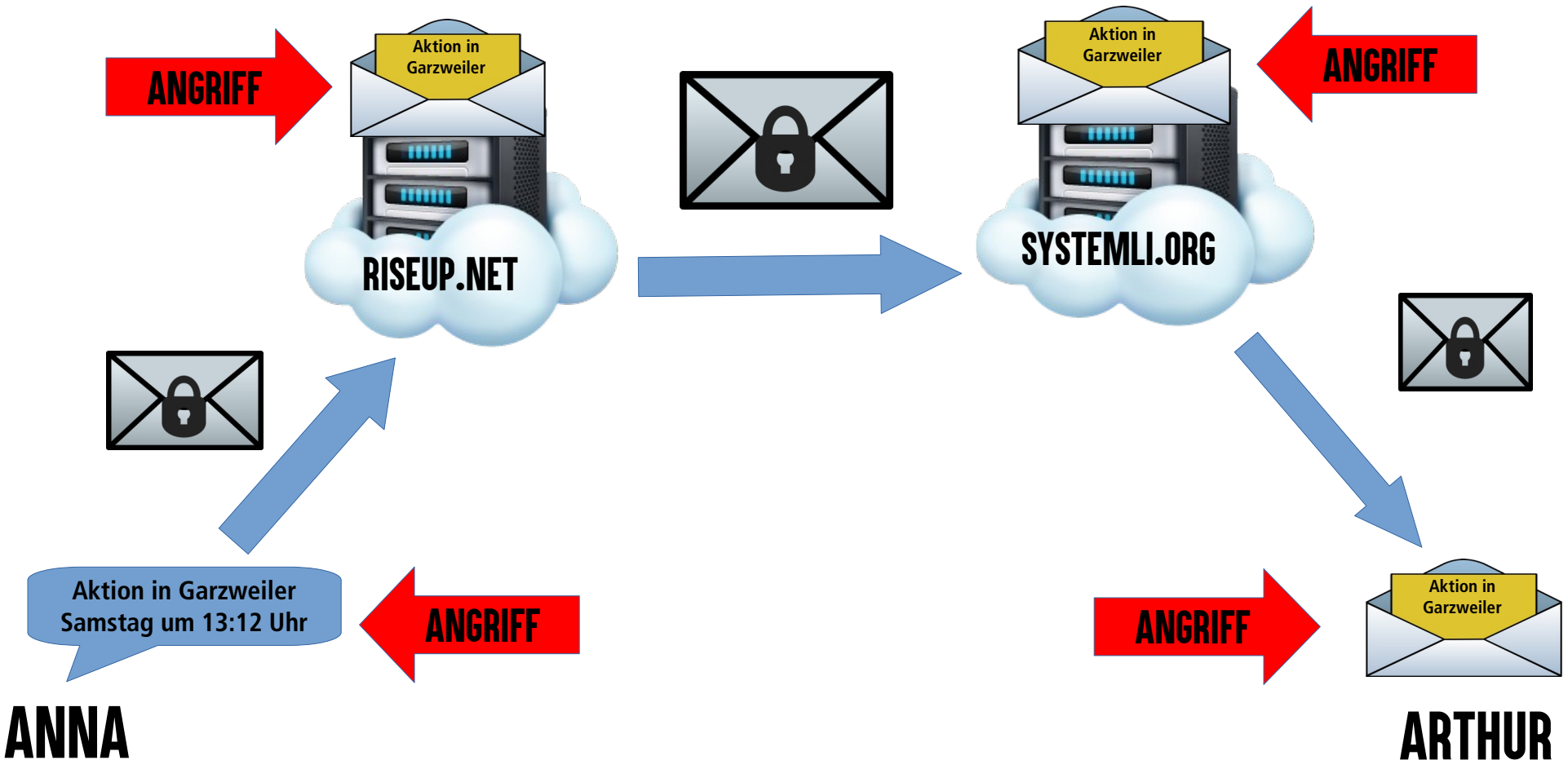
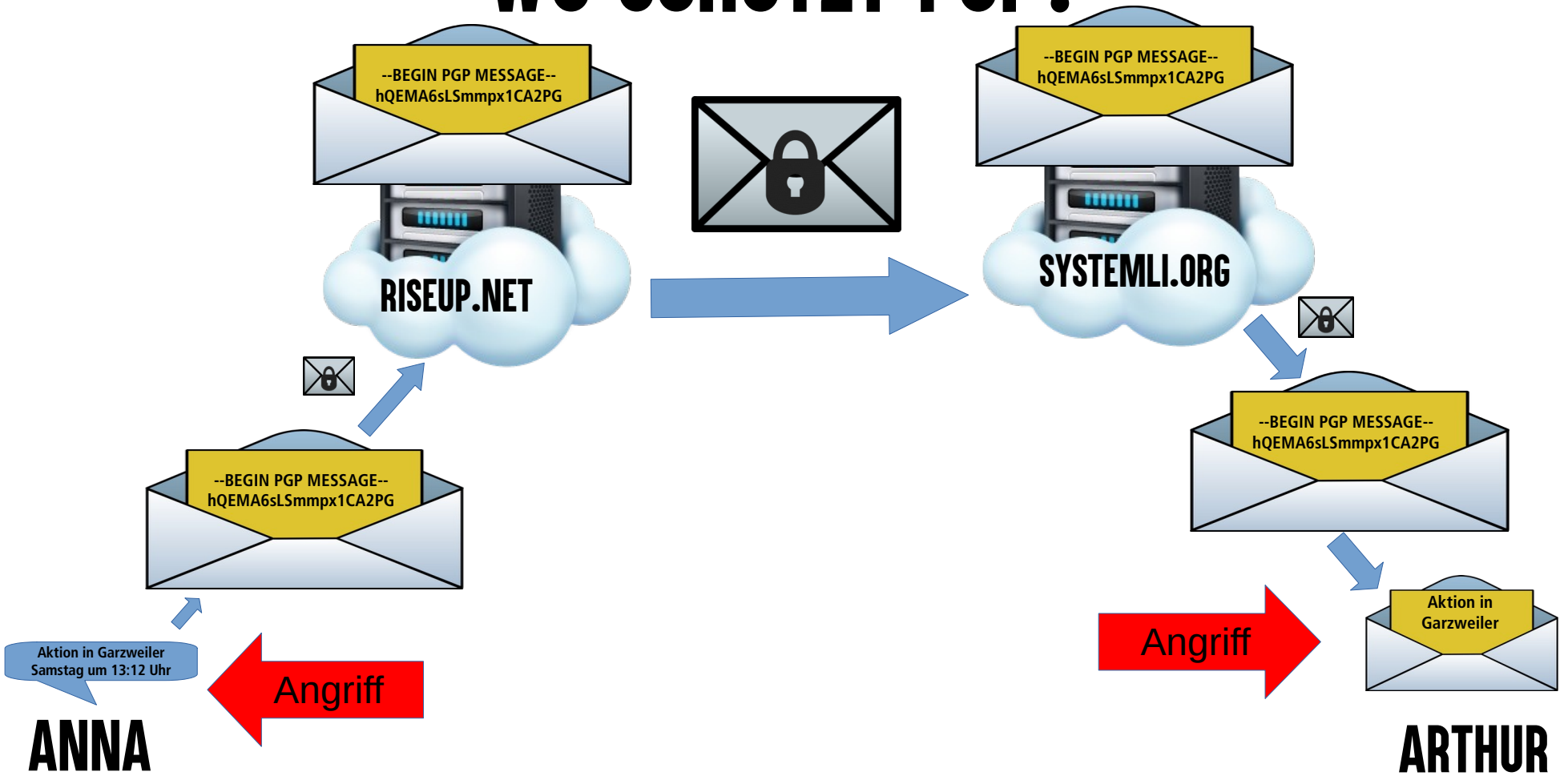
PGP VERSCHLÜSSLUNG

Einführung für Aktivist*innen

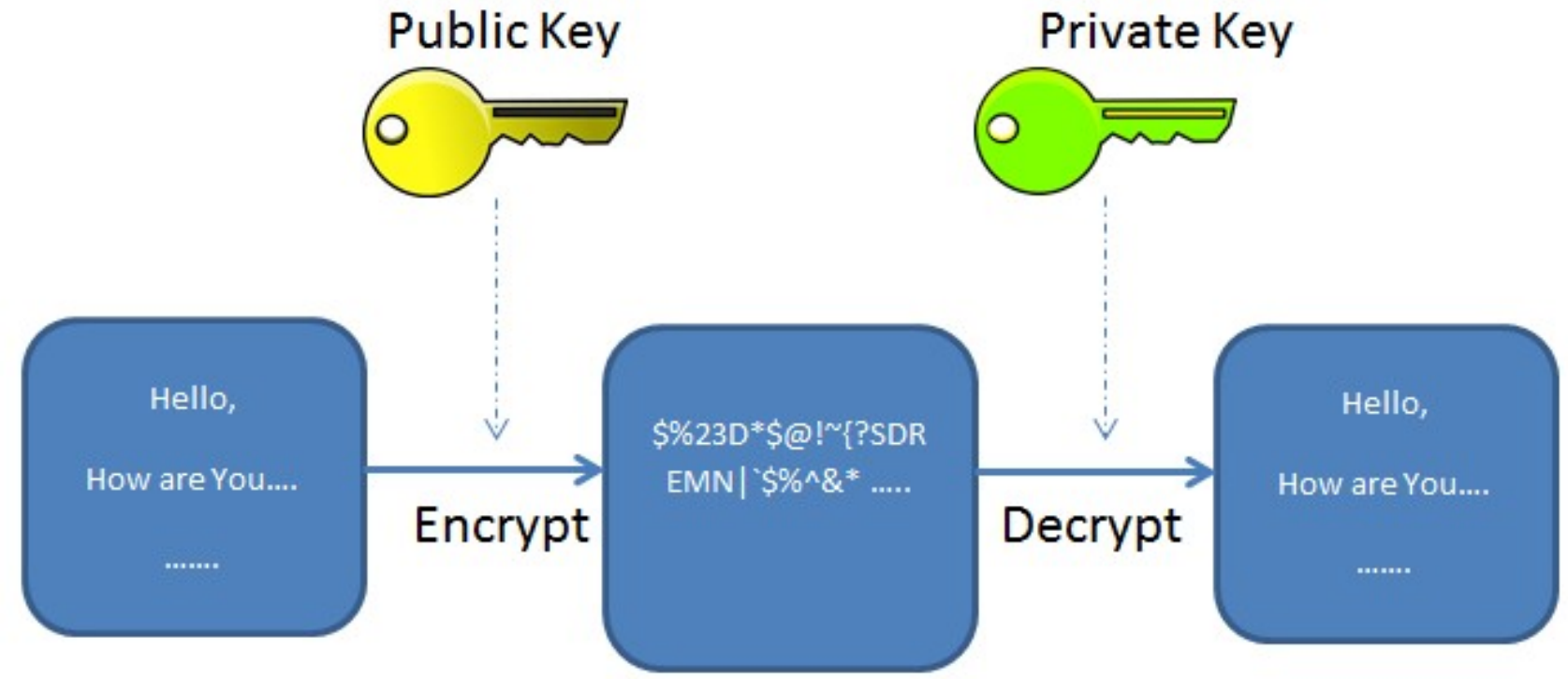
WIE FUNKTIONIERT E-MAIL?

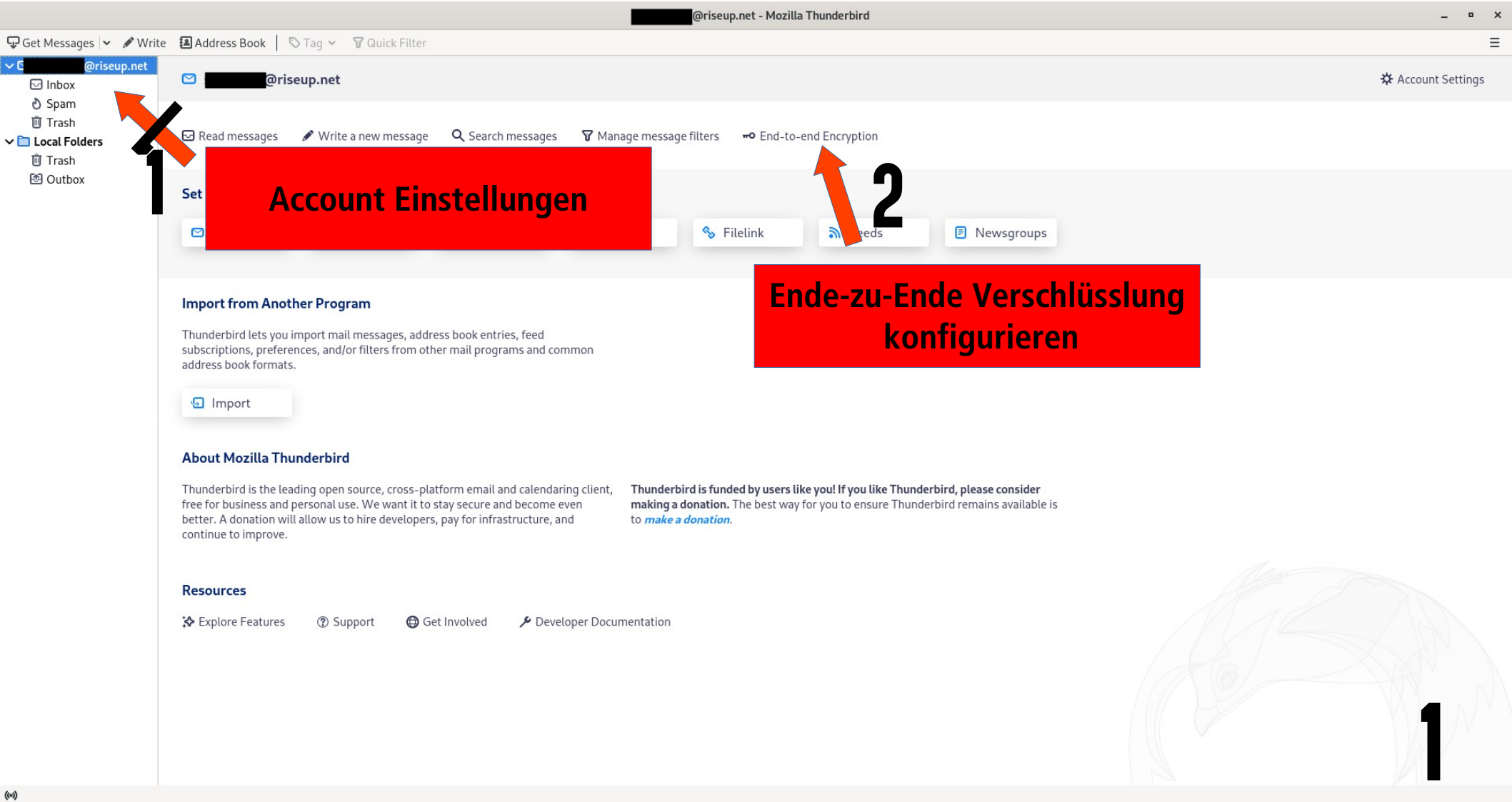


WO SCHÜTZT PGP?



WIE FUNKTIONIERT PGP?




[redacted]@riseup.net - Mozilla Thunderbird
Get Messages
Write
Address Book
Tag
Quick Filter
[redacted]@riseup.net
Inbox
Spam
Trash
Local Folders
Trash
Outbox
[redacted]@riseup.net
Account Settings
Read messages
Write a new message
Search messages
Manage message filters
End-to-end Encryption
1
Account Einstellungen
2
Filelink
Newsgroups
Ende-zu-Ende Verschlüsslung konfigurieren
Import from Another Program
Thunderbird lets you import mail messages, address book entries, feed subscriptions, preferences, and/or filters from other mail programs and common address book formats.
Import
About Mozilla Thunderbird
Thunderbird is the leading open source, cross-platform email and calendaring client, free for business and personal use. We want it to stay secure and become even better. A donation will allow us to hire developers, pay for infrastructure, and continue to improve.
Thunderbird is funded by users like you! If you like Thunderbird, please consider making a donation. The best way for you to ensure Thunderbird remains available is to make a donation.
Resources
Explore Features
Support
Get Involved
Developer Documentation
1

Account Settings - Mozilla Thunderbird

[redacted]@riseup.net | Account Settings

- [redacted]@riseup.net
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Junk Settings
  - Synchronization & Storage
  - End-To-End Encryption
  - Return Receipts
- Local Folders
  - Junk Settings
  - Disk Space
- Outgoing Server (SMTP)

Account Actions

End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more

OpenPGP

Thunderbird doesn't have a personal OpenPGP key for [redacted]@riseup.net

Add Key...

Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

OpenPGP Key Manager

Neuen Key hinzufügen

S/MIME

Personal certificate for digital signing:

Select... Clear

Personal certificate for encryption:

Select... Clear

Manage S/MIME Certificates | S/MIME Security Devices

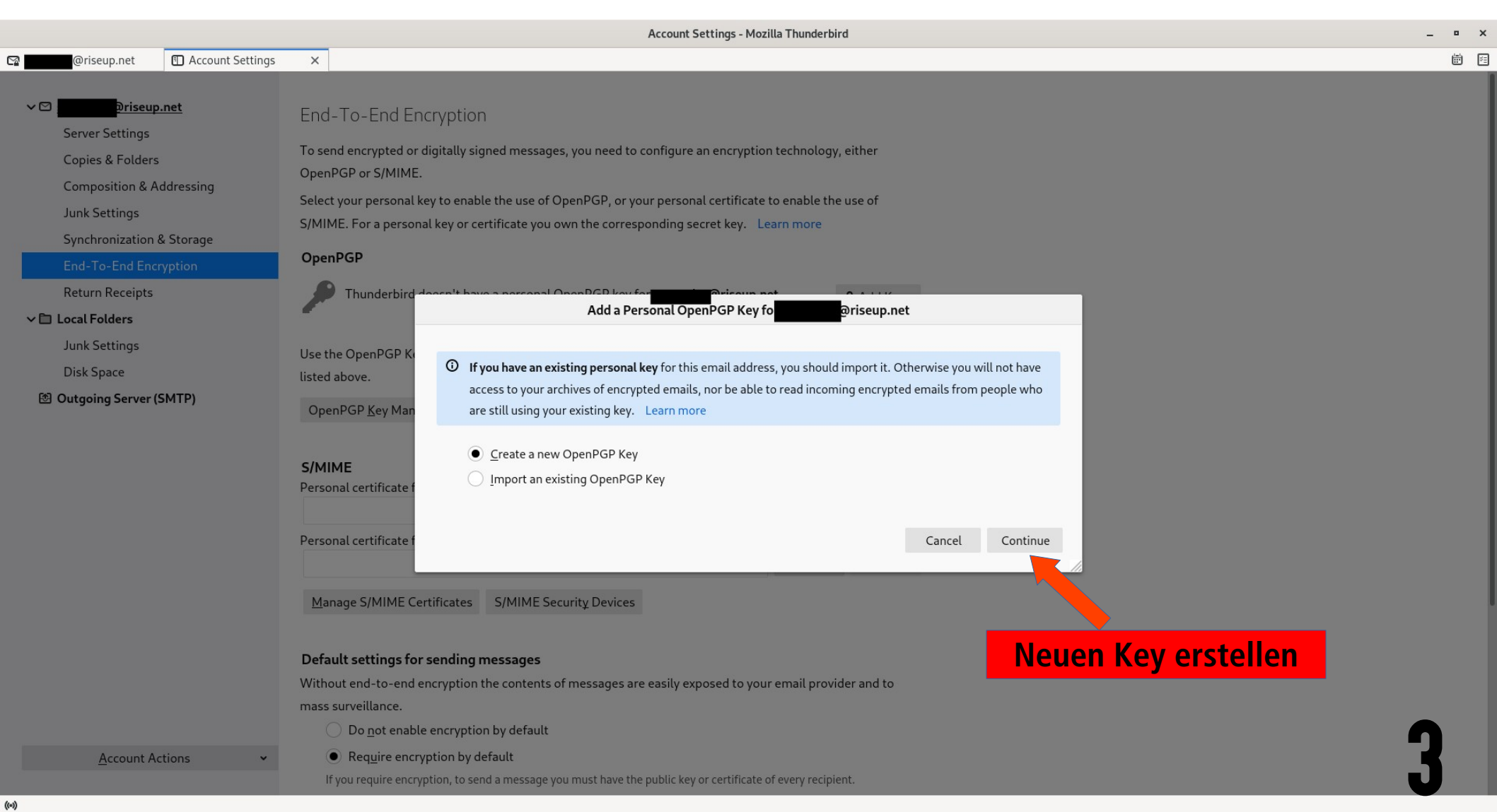
Default settings for sending messages

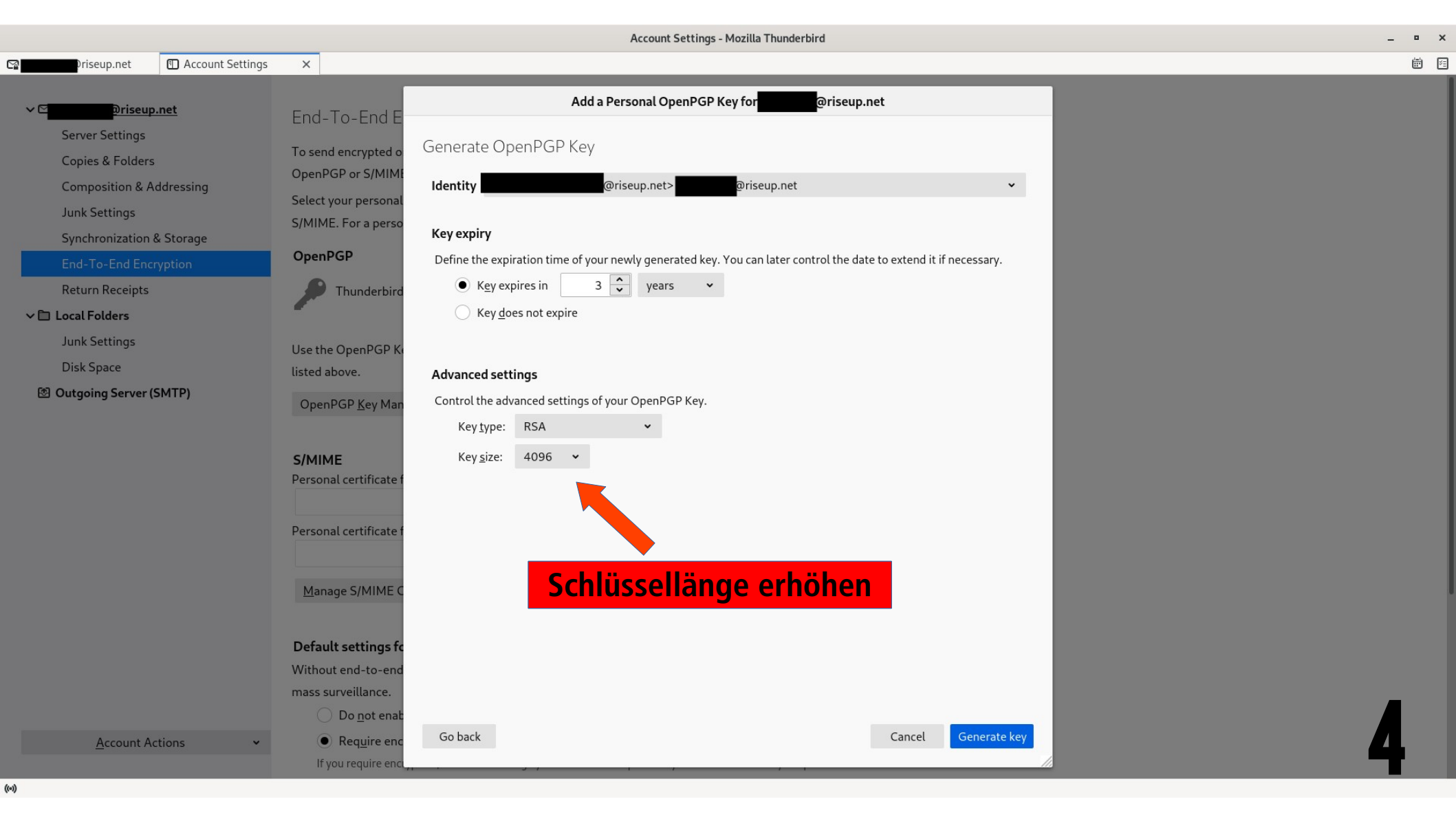
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

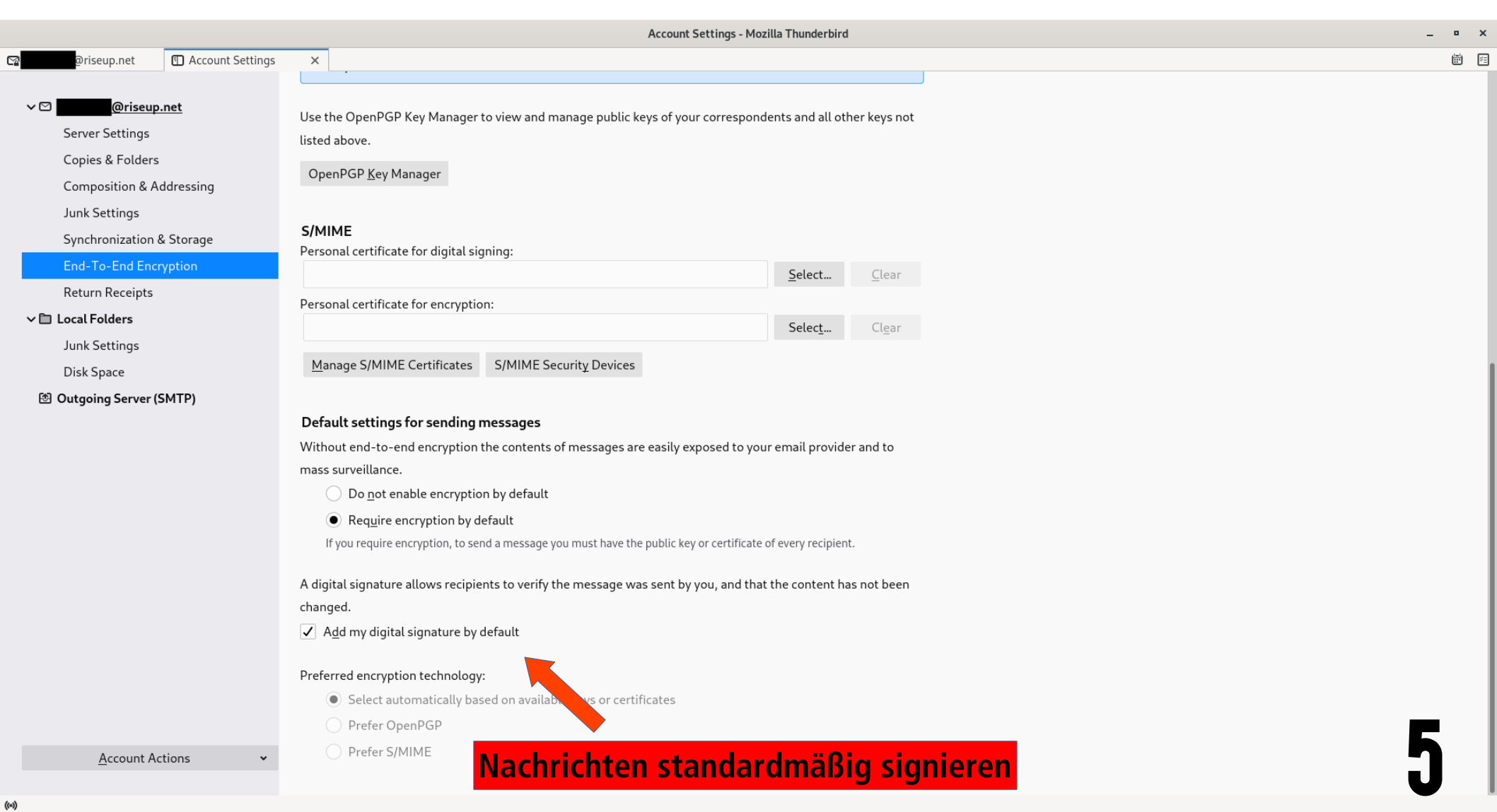
- ○ Do not enable encryption by default
- ● Require encryption by default

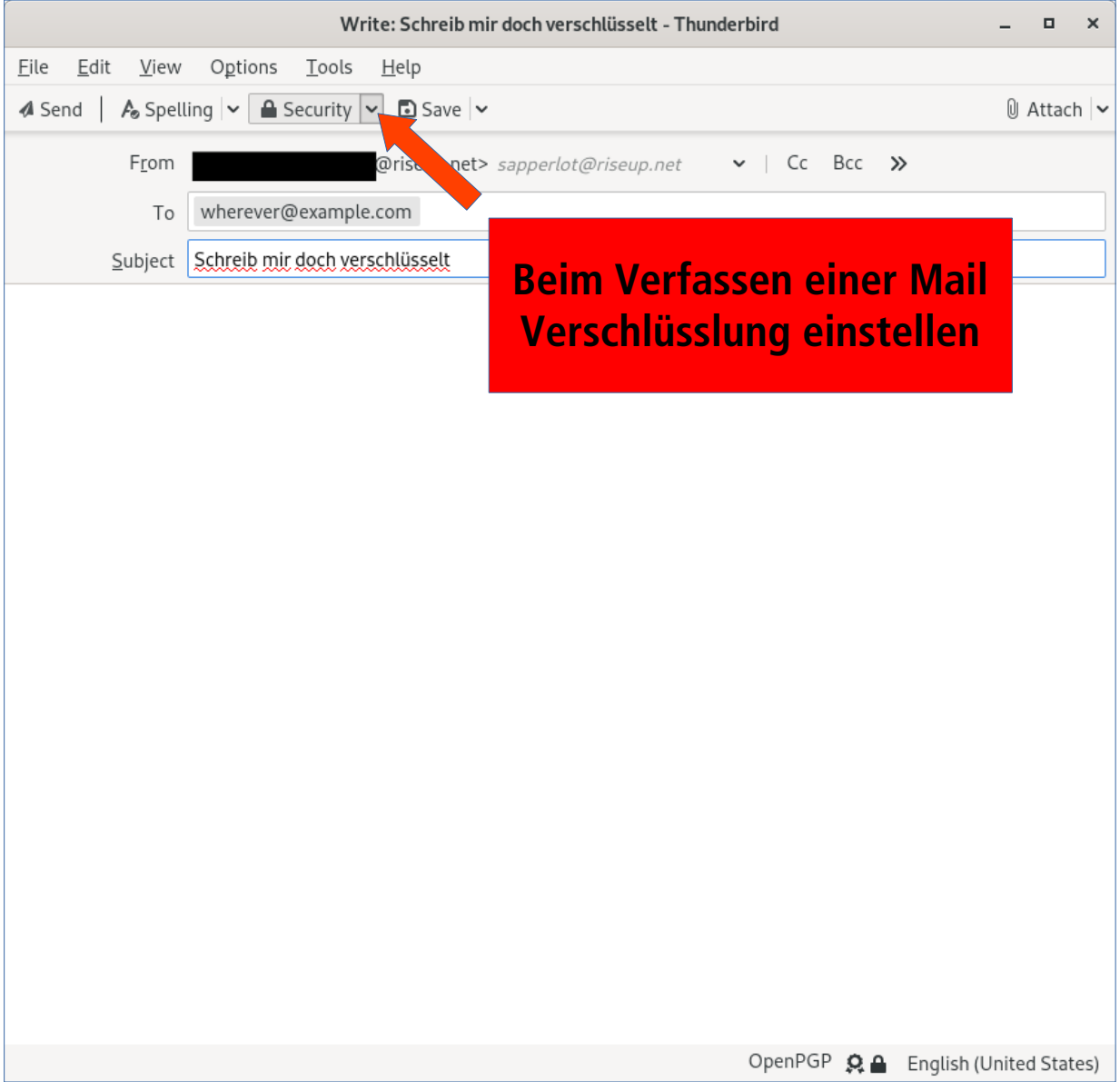
If you require encryption, to send a message you must have the public key or certificate of every recipient.

2


Account Settings - Mozilla Thunderbird
[redacted]@riseup.net
Account Settings
[redacted]@riseup.net
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
End-To-End Encryption
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Account Actions
End-To-End Encryption
To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.
Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more
OpenPGP
Thunderbird doesn't have a personal OpenPGP key for [redacted]@riseup.net
Use the OpenPGP K
listed above.
OpenPGP Key Man
S/MIME
Personal certificate f
Personal certificate f
Manage S/MIME Certificates
S/MIME Security Devices
Default settings for sending messages
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.
Do not enable encryption by default
Require encryption by default
If you require encryption, to send a message you must have the public key or certificate of every recipient.
Add a Personal OpenPGP Key fo[redacted]@riseup.net
If you have an existing personal key for this email address, you should import it. Otherwise you will not have access to your archives of encrypted emails, nor be able to read incoming encrypted emails from people who are still using your existing key. Learn more
Create a new OpenPGP Key
Import an existing OpenPGP Key
Cancel
Continue
Neuen Key erstellen
3

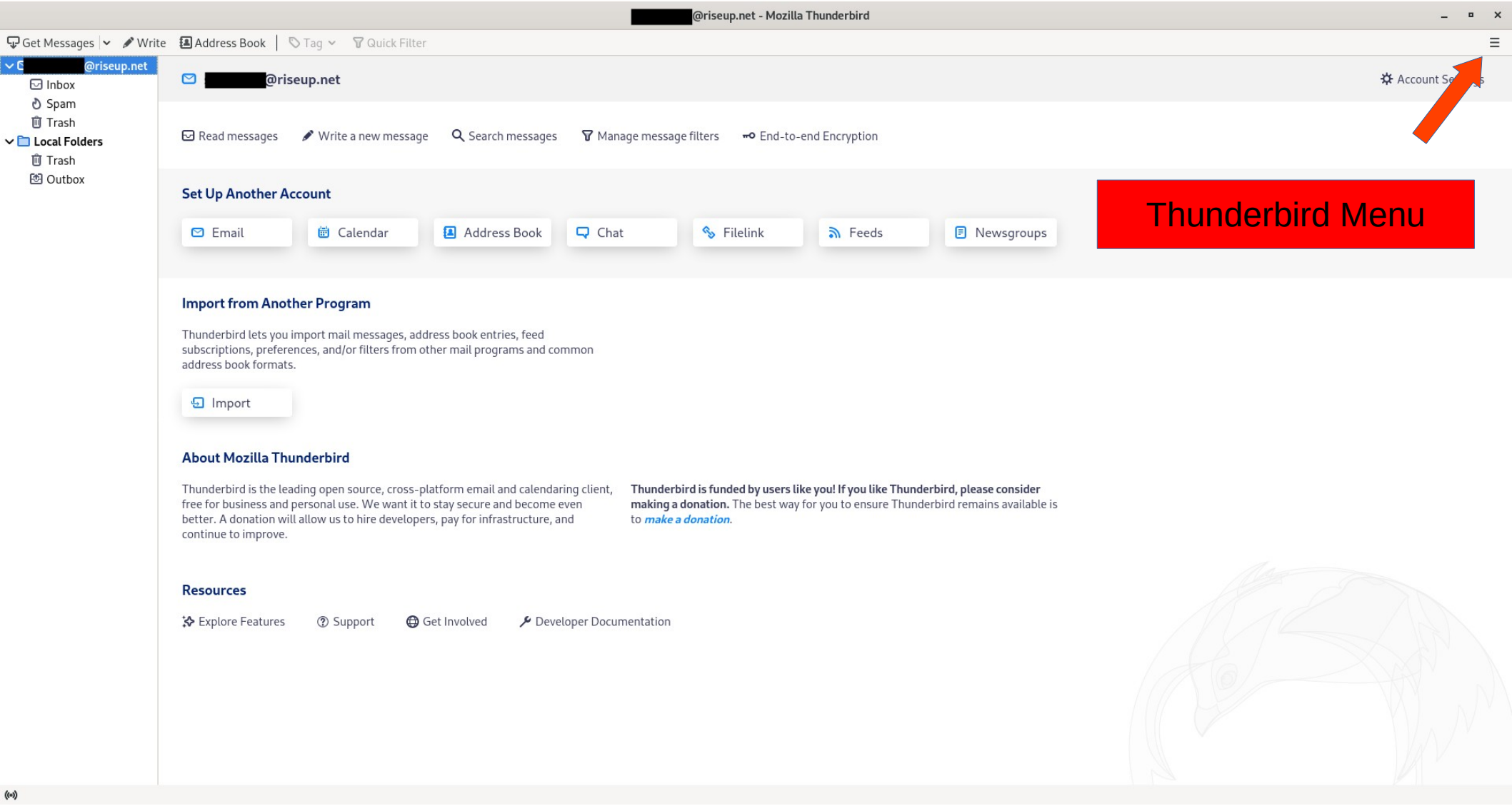

Account Settings - Mozilla Thunderbird
[redacted]riseup.net
Account Settings
[redacted]@riseup.net
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
End-To-End Encryption
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Account Actions
End-To-End E
To send encrypted o
OpenPGP or S/MIME
Select your personal
S/MIME. For a perso
OpenPGP
Thunderbird
Use the OpenPGP K
listed above.
OpenPGP Key Man
S/MIME
Personal certificate f
Personal certificate f
Manage S/MIME C
Default settings fo
Without end-to-end
mass surveillance.
Do not enab
Require enc
If you require enc
Add a Personal OpenPGP Key for [redacted]@riseup.net
Generate OpenPGP Key
Identity [redacted]@riseup.net> [redacted]@riseup.net
Key expiry
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.
Key expires in 3 years
Key does not expire
Advanced settings
Control the advanced settings of your OpenPGP Key.
Key type: RSA
Key size: 4096
Schlüssellänge erhöhen
Go back
Cancel
Generate key
4


Account Settings - Mozilla Thunderbird
[redacted]@riseup.net
Account Settings
[redacted]@riseup.net
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
End-To-End Encryption
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Account Actions
Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.
OpenPGP Key Manager
S/MIME
Personal certificate for digital signing:
Select...
Clear
Personal certificate for encryption:
Select...
Clear
Manage S/MIME Certificates
S/MIME Security Devices
Default settings for sending messages
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.
Do not enable encryption by default
Require encryption by default
If you require encryption, to send a message you must have the public key or certificate of every recipient.
A digital signature allows recipients to verify the message was sent by you, and that the content has not been changed.
Add my digital signature by default
Preferred encryption technology:
Select automatically based on availab ys or certificates
Prefer OpenPGP
Prefer S/MIME
Nachrichten standardmäßig signieren
5


Write: Schreib mir doch verschlüsselt - Thunderbird
File Edit View Options Tools Help
Send Spelling Security Save Attach
From [redacted] sapperlot@riseup.net Cc Bcc
To wherever@example.com
Subject Schreib mir doch verschlüsselt
Beim Verfassen einer Mail
Verschlüsslung einstellen
OpenPGP English (United States)

KEY MANAGER

- **Zugriff über:**
  Thunderbird Menü (Drei horizontale Streifen oben Rechts) -> Tools -> OpenPGP Key Manager
- **Alle Keys aufgelistet (privat Keys fett)**
- **Möglichkeit Public and Private Keys zu importieren**
  File-> Import*


[redacted]@riseup.net - Mozilla Thunderbird
Get Messages
Write
Address Book
Tag
Quick Filter
[redacted]@riseup.net
Inbox
Spam
Trash
Local Folders
Trash
Outbox
[redacted]@riseup.net
Account Settings
Read messages
Write a new message
Search messages
Manage message filters
End-to-end Encryption
Set Up Another Account
Email
Calendar
Address Book
Chat
Filelink
Feeds
Newsgroups
Thunderbird Menu
Import from Another Program
Thunderbird lets you import mail messages, address book entries, feed subscriptions, preferences, and/or filters from other mail programs and common address book formats.
Import
About Mozilla Thunderbird
Thunderbird is the leading open source, cross-platform email and calendaring client, free for business and personal use. We want it to stay secure and become even better. A donation will allow us to hire developers, pay for infrastructure, and continue to improve.
Thunderbird is funded by users like you! If you like Thunderbird, please consider making a donation. The best way for you to ensure Thunderbird remains available is to make a donation.
Resources
Explore Features
Support
Get Involved
Developer Documentation

SONSTIGE HINWEISE

- **Masterkey: Schützt eure Keys auf eurem PC (falls euer PC beschlagnahmt wird)**
- **Backup: Sichert eure privaten (am besten auch alle öffentlichen) Keys!**
  - **Thunderbird: KeyManager -> Key anklicken -> Edit -> Backup Secret Key to File**
  - **Gutes Passwort wählen**
  - **Am besten nur in Passwortmanager speichern**

VERSCHLÜSSELTE E-MAIL VERTEILER
3 ALTERNATIVEN

1. Schleuder
2. Manuelle Schleuder
3. Liste mit geteiltem Key

SCHLEUDER

- Alle haben Public Key der Liste
- Es wird an listname@example.com geschrieben und verschlüsselt
- Server verschlüsselt an alle

SCHLEUDER

Vorteile	Nachteile
Intuitiv	Server muss vertraut werden
Schnelle Weiterleitung	Server muss alle Public Keys haben
Nur Public Key der Liste muss verteilt werden	Einrichtung schwieriger

MANUELLE SCHLEUDER

- Alle haben Public Key der Liste/einer E-Mail Addrese
- Es wird an listname@example.com geschrieben und verschlüsselt
- Vertrauenswürdiges Team leitet E-Mails manuell weiter

MANUELLE SCHLEUDER

Vorteile	Nachteile
Intuitiv für Nutzer*innen	Arbeit von Team notwendig
Nur Public Key der Liste muss verteilt werden	Team muss alle Public Keys verwalten
Nur Public Key der Liste muss verteilt werden	Weiterleitung kann dauern

LISTE MIT GETEILTEM KEY

- Ein Schlüsselpaar das ALLE haben
- Es wird an listname@example.com geschrieben und verschlüsselt
- Alle empfangen die E-Mail und entschlüsseln mit private Key

LISTE MIT GETEILTEM KEY

Vorteile	Nachteile
Intuitiv	Schlüssel muss sicher verteilt werden
Schnelle Weiterleitung	Menschen exkludieren schwierig
Einfache Einrichtung z.B. über Riseup	

FRAGEN?

OPSEC

- Tails nutzen (vermindert Metadaten)
- Eine E-Mail Adresse pro Zusammenhang
- Passwort Manager nutzen
- Computer und Backup verschlüsseln
- Alte E-Mails (und Daten) löschen

MEHR MATERIAL

Hilfreiche Guides von Menschen mit Ahnung:
https://beschlagnahmt.org/themen/

FAQ OpenPGP mit Thunderbird:
https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq

SONSTIGE TIPPS

- **E-Mail Verschlüsslung auf dem Handy: K9 + Open Keychain**
- **Passwortmanager der PGP Keys als Anhang speichern kann: KeePassXC**
- **Thunderbird kann auch GPG als PGP Backend verwenden -> Für Hardwaretoken sinnvoll**