Kurer for Thunderbird

Secure email powered by **DANE**

Kurer for Thunderbird

- Modern add-on for Thunderbird Clients
- No-click solution for seamless DANE S/MIME
- Open-source
  - https://github.com/gmu-msl/kurer-thunderbird

What can it do?

- **Compose** S/MIME signed / encrypted emails
- **Verify / Decrypt** S/MIME signed / encrypted emails
- **Seamlessly reply** in an encrypted conversation

And most importantly,

- Power all the above with **intuitive user settings** and minimal set-up

A side note

The following will show sending and receiving secure email using Kurer.

It assumes users have already posted their S/MIME certificates on DANE.

For the curious: there is a separate easy-to-use app to accomplish exactly that

(daneportal.net)

… for now, let's jump right in!

Jump right in to sending secure email

Only one setting is really needed for now:

● Enter your private key and sending email address to allow signing your email

Jump right in to sending secure email

Only one setting is really needed for now:

● Enter your private key and sending email address to allow signing your email

Jump right in to sending secure email

- Compose an email like normal
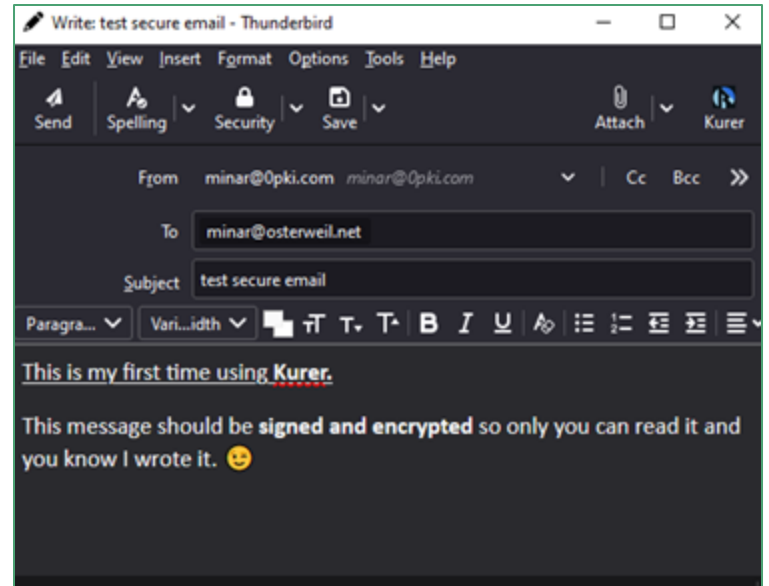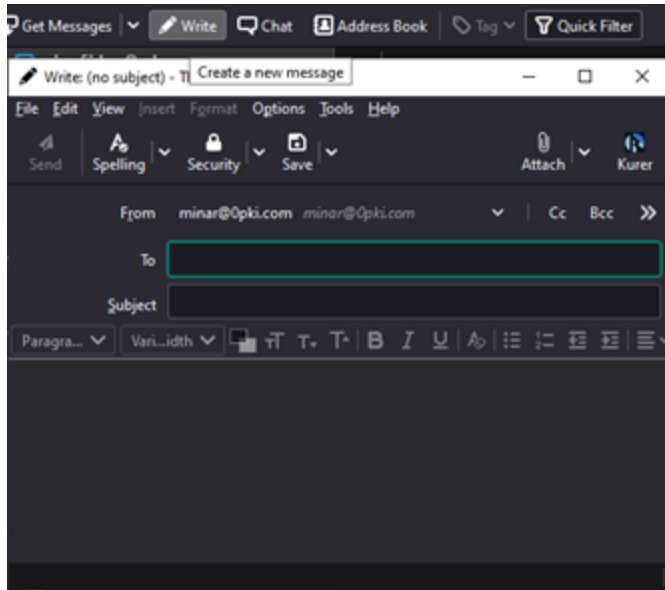
Jump right in to sending secure email

- Use the Kurer popup to toggle signing and click send encrypted
  - The SIG tag on the icon means the email will be signed when sending
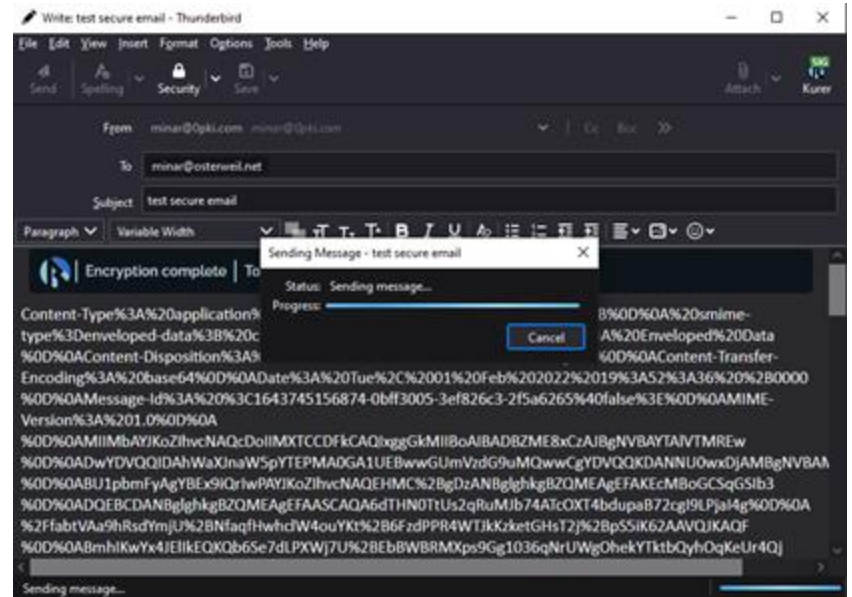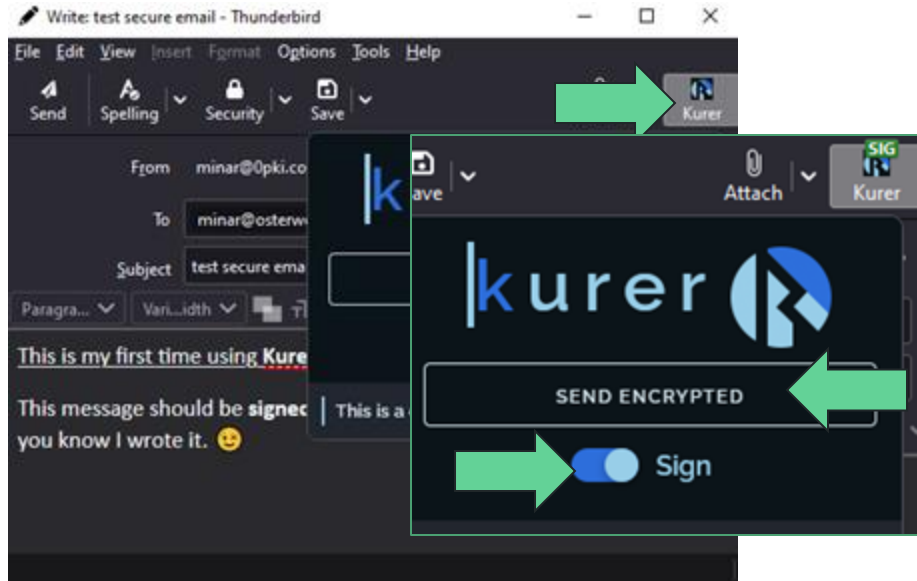
Jump right in to sending secure email
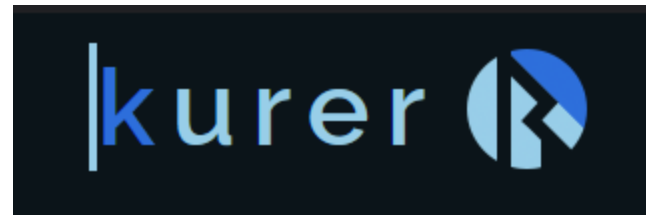
● The email has been sent - signed by you and encrypted for the recipient
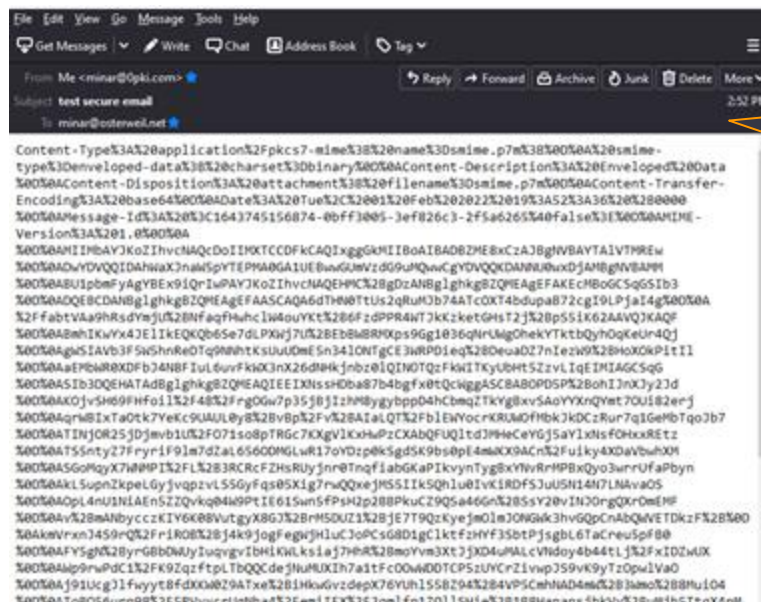
Psst: also notice how we are sending secure emails between **entirely different email domains** — this is usually super difficult without DANE!

Making that easier

Jumping back to the options for a sec, let's look at how you could customize the composing experience:

Kurer - DANE-powered Secure Email
S/MIME encrypted secure email functionality, powered by DNS-based Authentication of Named Entities (DANE).

Details   **Options**   Permissions

Composing messages

Seperate encrypt button ⬤ Always encrypt on send

Not signed by default ⬤ Signed by default

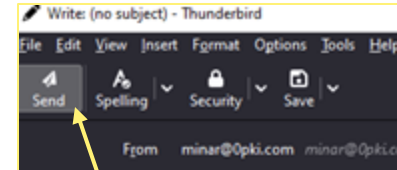**If unable to encrypt for a recipient:**

Silently send unencrypted ⬤ Halt and show warning

Write: (no subject) - Thunderbird
File Edit View Insert Format Options Tools Help
Send   Spelling   Security   Save
From   minar@0pki.com   minar@0pki.co

Toggle this on if you want Kurer to replace Thunderbird's default send button to always try and encrypt the email when sending

Toggle this on if you want to have Kurer's SIGN toggle ON BY DEFAULT when writing a new email

Toggle this on if you want Kurer to abort sending if it could not find a cert on DANE to encrypt for a recipient.
This increases security but makes Kurer more in-your-face at times.

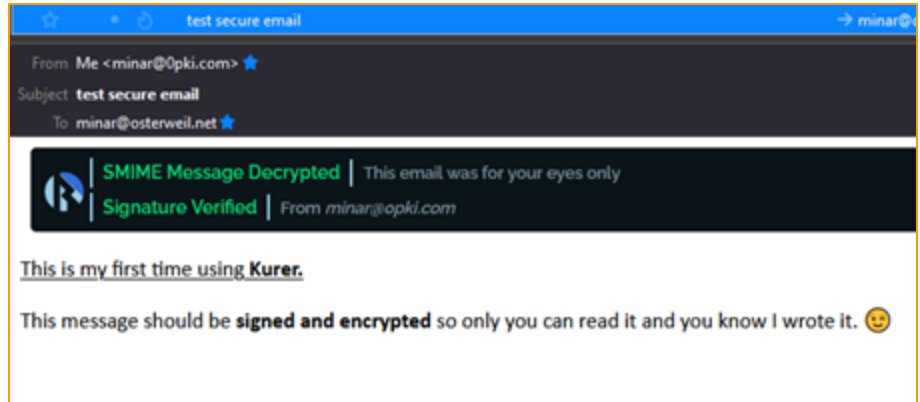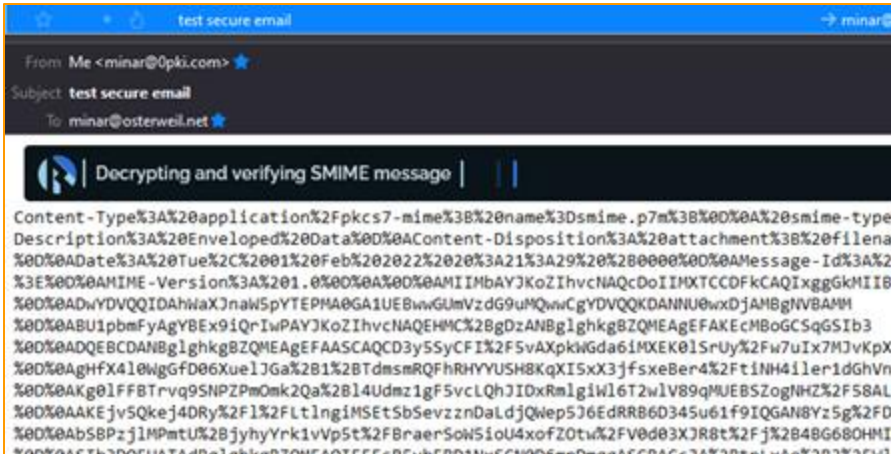# Reading secure email

Now, let's take a look at how Kurer makes it easy to read secure email

Reading secure email

Now, let's take a look at how Kurer makes it easy to read secure email

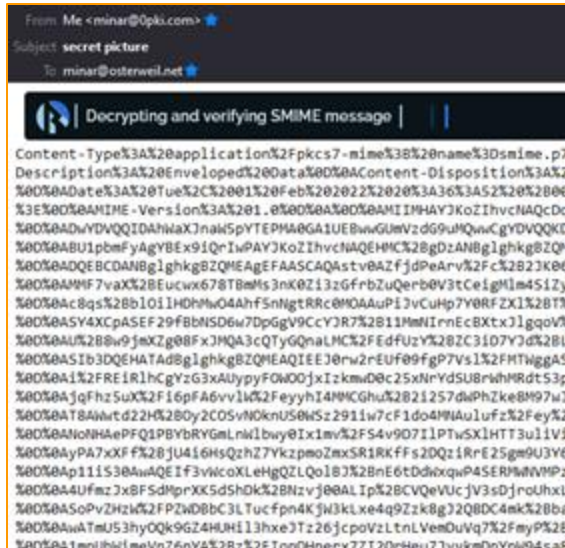- Simply click on an email in your inbox and let Kurer do its magic

Reading secure email

Now, let's take a look at how Kurer makes it easy to read secure email

- You can read any email, even with heavy HTML

Informative status messages

When you click on an email, Kurer will detect S/MIME automatically and attempt to decrypt and verify

Kurer will let you know if something goes wrong decrypting,
along with the verification status of a signed email:
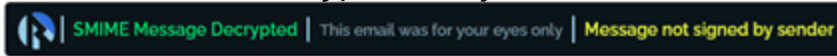
Decryption failed
Issue on your side - you don't have the correct key set in options (DANE cert sender used does not match, etc)

Encrypted-only

Signed-only

Verification failed
Issue on sender side - honest setup error, spoofed message, tampered message, etc

Signed and encrypted

Replying

Kurer makes it easy to reply to secure emails
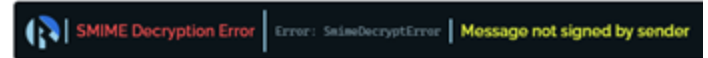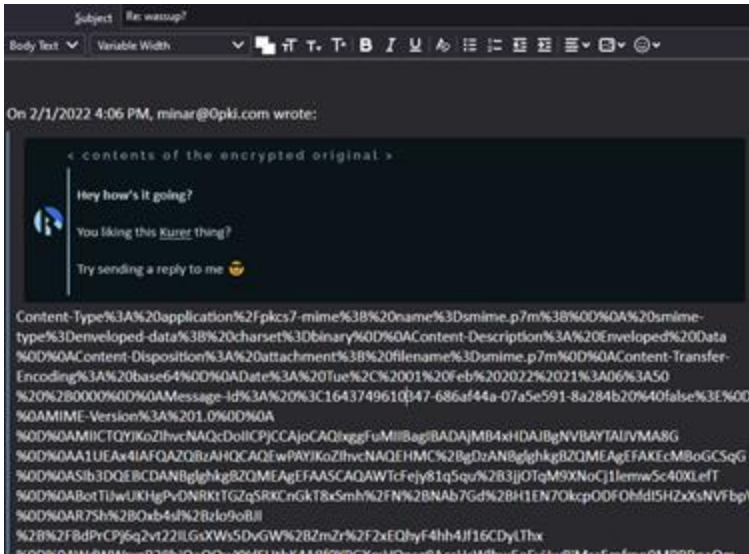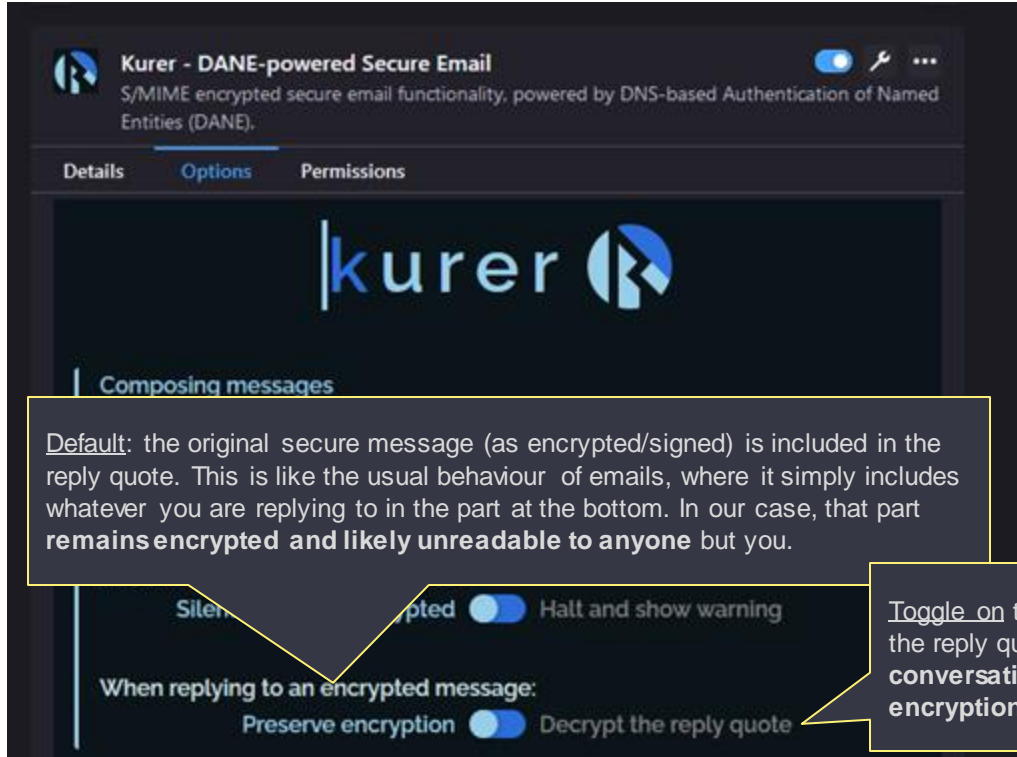
- Just use the normal reply button, and Kurer will show the content of the secure email while you are composing

- Write whatever you like in the usual space above the reply quote and then use any of the usual secure methods when sending

  *This demonstrates the **default** behavior of replies - but that can be customized in the options*

Replying - options

Jumping back to the options once more - we can customize what happens when replying to a secure email.

Kurer - DANE-powered Secure Email
S/MIME encrypted secure email functionality, powered by DNS-based Authentication of Named Entities (DANE).

Details   Options   Permissions
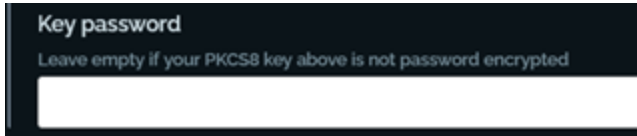
Composing messages

Default: the original secure message (as encrypted/signed) is included in the reply quote. This is like the usual behaviour of emails, where it simply includes whatever you are replying to in the part at the bottom. In our case, that part **remains encrypted and likely unreadable to anyone** but you.

Sile...   ...pted   Halt and show warning

When replying to an encrypted message:
Preserve encryption   Decrypt the reply quote

Toggle on to actually include the decrypted version of the original message in the reply quote. This will make it **look more like a normal email conversation**, but is **potentially reducing security by undoing the encryption** that the sender made.

Other options

Private keys

Single key for sign/encr ⬤ Seperate keys for sign/encr
Key for decrypting and signing

Key password
Leave empty if your PKCS8 key above is not password encrypted

DNS recursive resolver to use for DANE
cloudflare-dns.com/dns-query

- You can use 2 different keys for signing and encrypting

- Kurer supports PKCS8 passphrase protected Keys

- For advanced users, you can customize which DNS resolver to use for DANE

We saw Kurer:

- Compose S/MIME signed / encrypted emails
- Verify / Decrypt S/MIME signed / encrypted emails
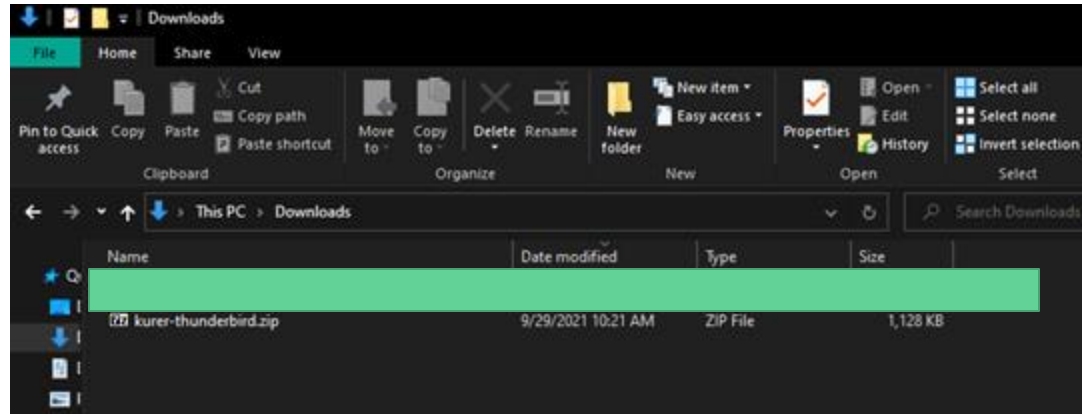- Seamlessly reply in an encrypted conversation

Now how do we install it?

Set up Kurer
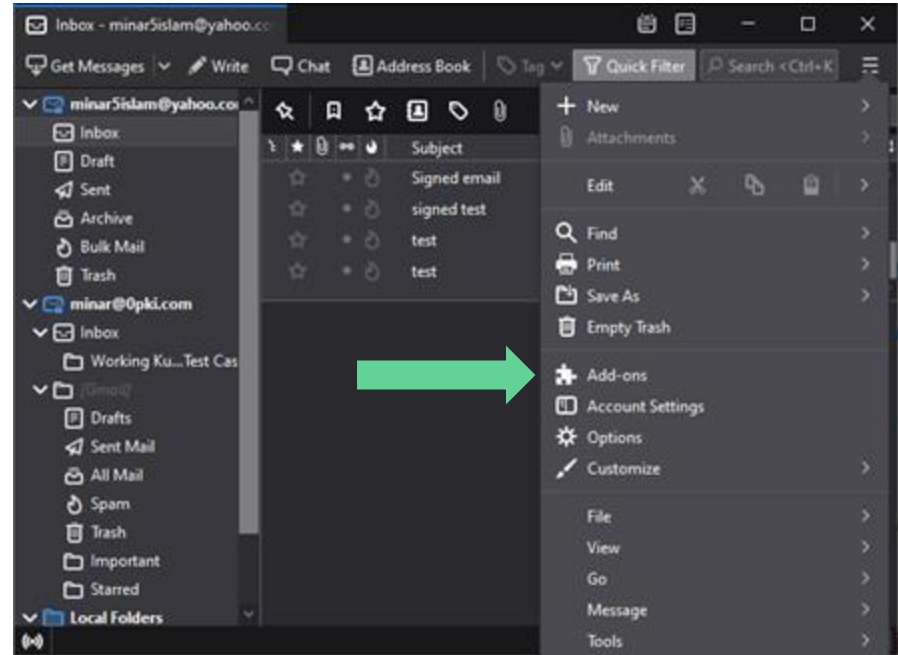
Download Kurer as a zip file.

(https://github.com/gmu-msl/kurer-thunderbird)
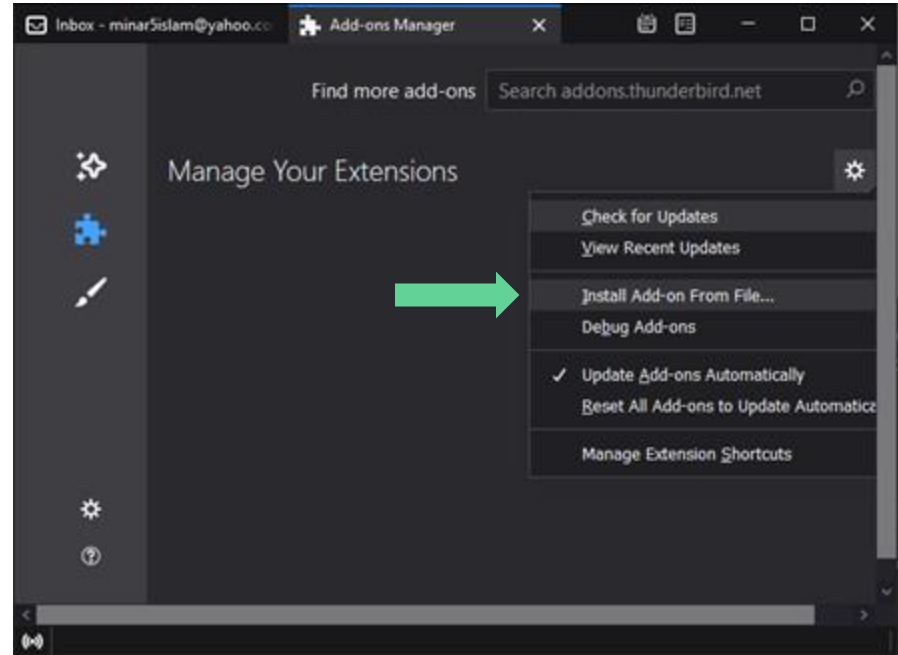
Set up Kurer

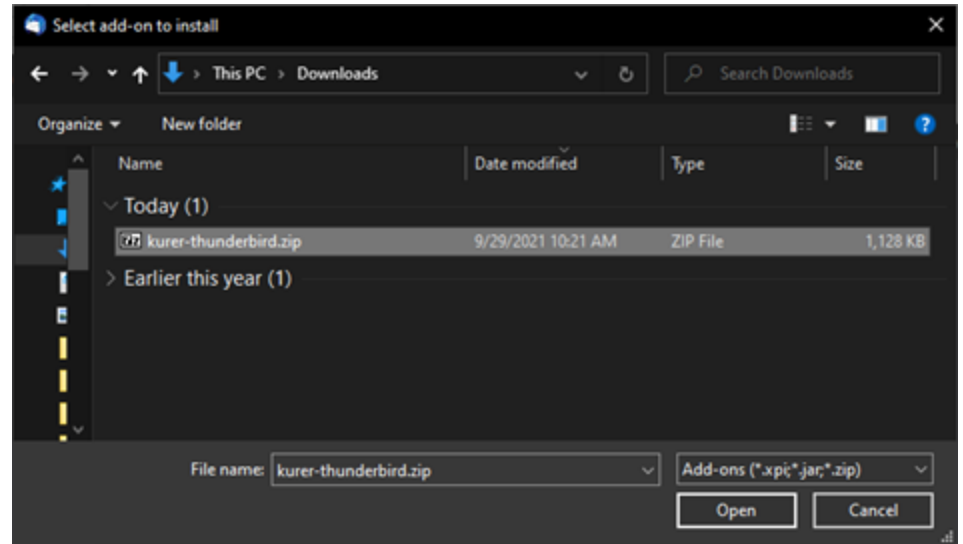

Go to add-ons menu on TB

Set up Kurer

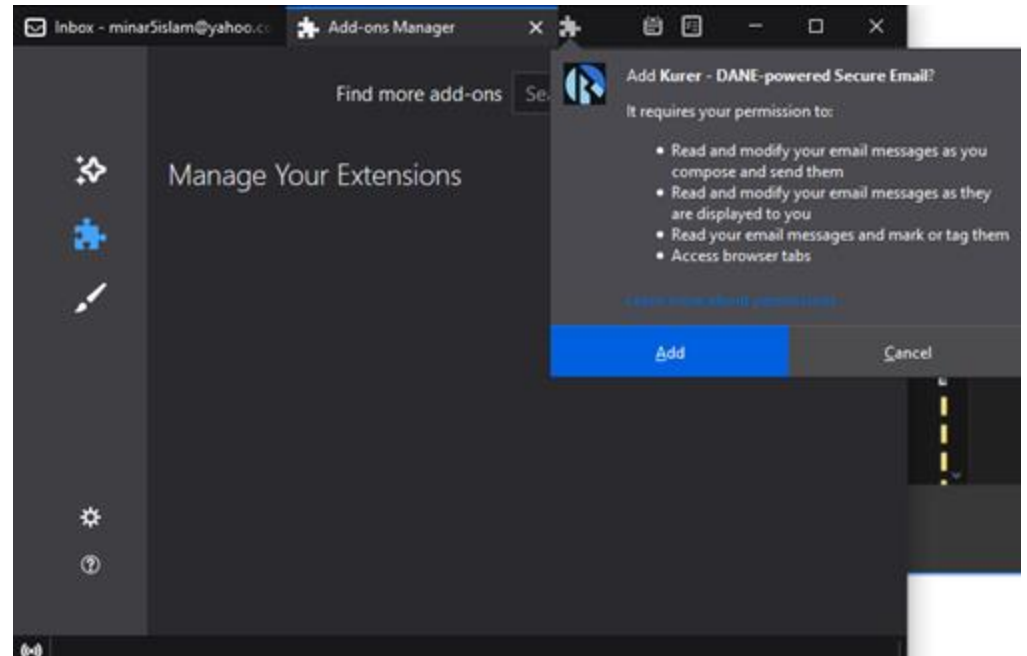Select Install from file

Set up Kurer

Select the downloaded zip file

Set up Kurer

Review permissions and add Kurer

And that's it!

Be sure to check out DANE portal to learn about the certificate-management side of the equation