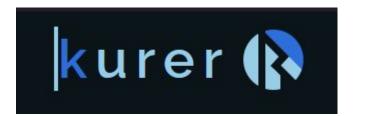
Kurer for Thunderbird

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.

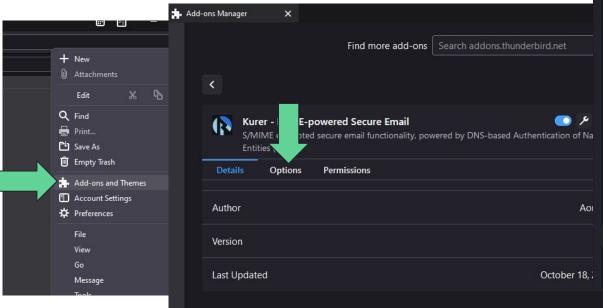
It assumes users have already posted their S/MIME certificates on DANE.

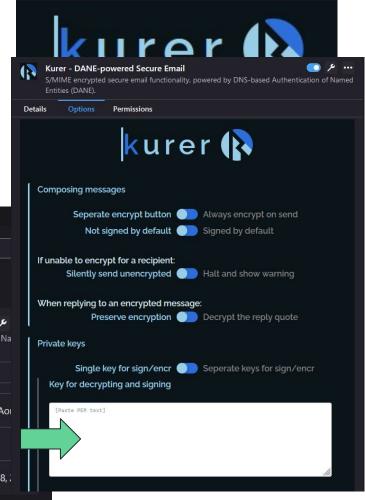
For the curious: there is a separate easy-to-use app to accomplish exactly that (daneportal.net)

... for now, let's jump right in!

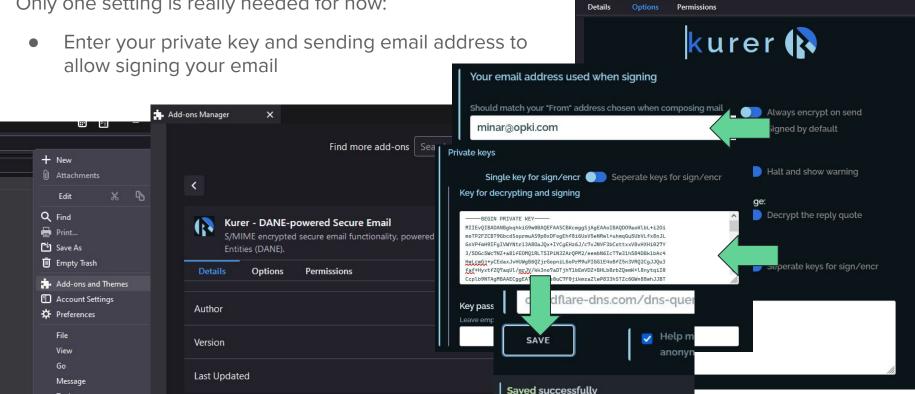
Only one setting is really needed for now:

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





Only one setting is really needed for now:



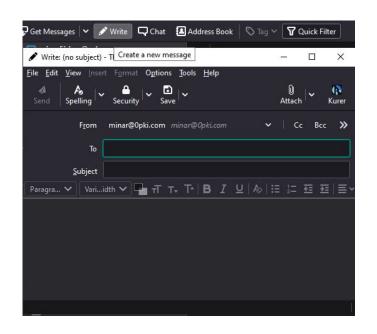
Iror

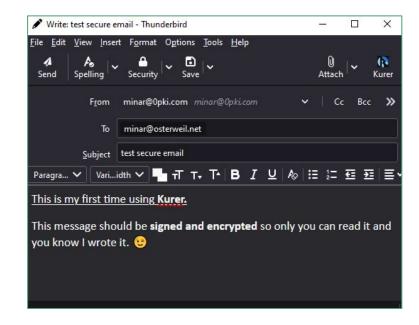
S/MIME encrypted secure email functionality, powered by DNS-based Authentication of Named

Kurer - DANE-powered Secure Email



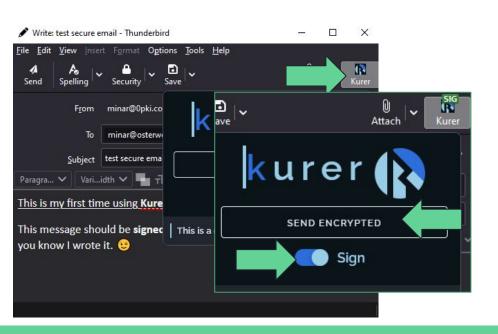
Compose an email like normal

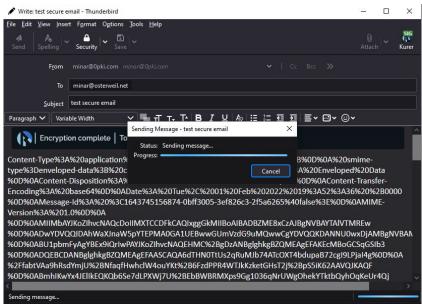






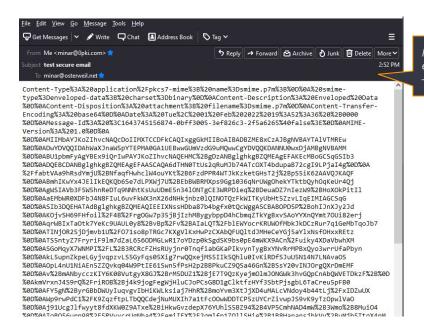
- Use the Kurer popup to toggle signing and click send encrypted
 - The SIG tag on the icon means the email will be signed when sending







The email has been sent - signed by you and encrypted for the recipient

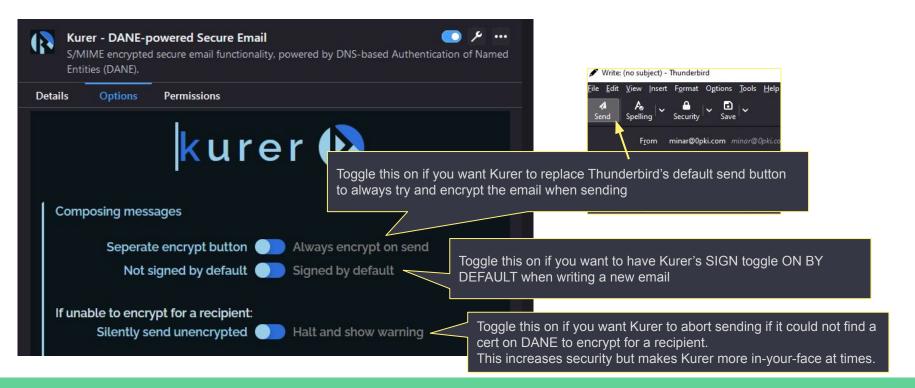


Psst: also notice how we are sending secure emails between **entirely different email domains**<u>this is usually</u> super difficult without DANE!

Making that easier



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



Reading secure email



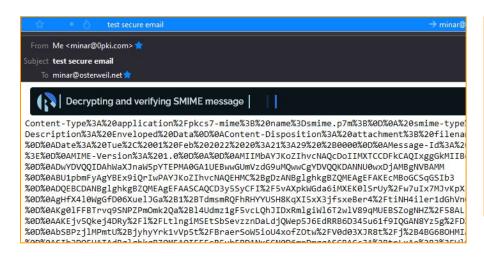
Now, let's take a look at how Kurer makes it easy to read secure email

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



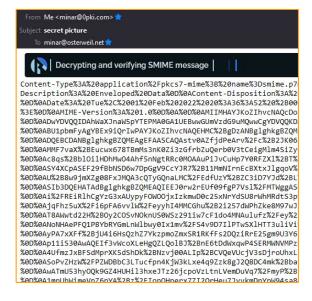


Reading secure email



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:

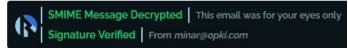




Signed-only



Signed and encrypted



Decryption failed

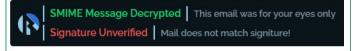
Issue on your side - you don't have the correct key set in options (DANE cert sender used does not match, etc)





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



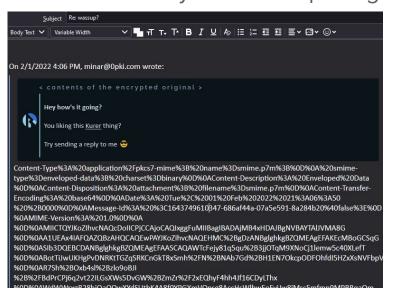


Replying



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



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

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



<u>Toggle on</u> 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

 You can use 2 different keys for signing and encrypting

Key password

Leave empty if your PKCS8 key above is not password encrypted

 Kurer supports PKCS8 passphrase protected Keys

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

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

We saw Kurer:



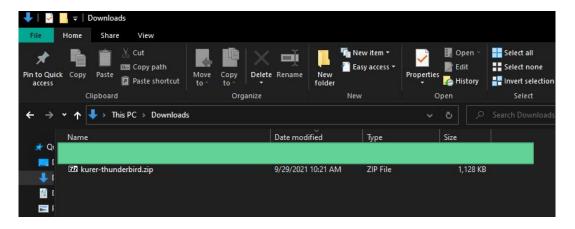
- Compose S/MIME signed / encrypted emails
- Verify / Decrypt S/MIME signed / encrypted emails
- Seamlessly reply in an encrypted conversation

Now how do we install it?



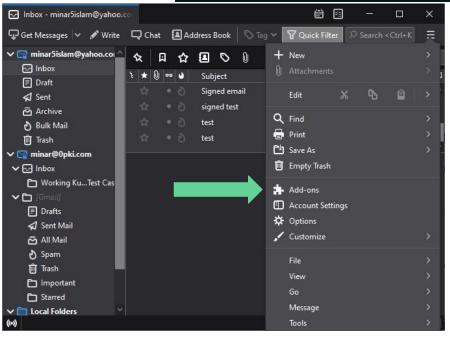
Download the packaged Kurer plugin file (.xpi or .zip) from releases page.

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



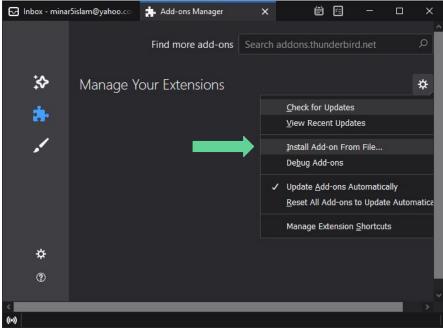
Go to add-ons menu on TB





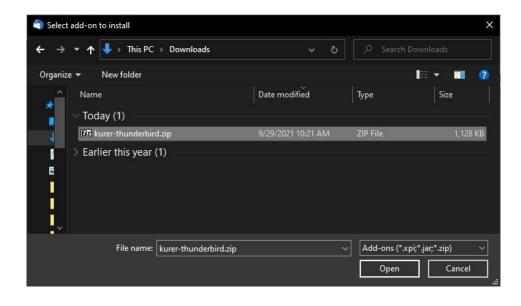
Select Install from file





Select the downloaded xpi file

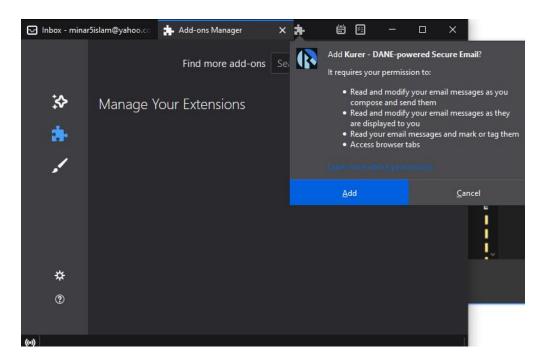






Review permissions and add Kurer

Note: to use Kurer you must enable html/rich-text emails in your Thunderbird preferences. Kurer currently does not support the Thunderbird plain-text only email viewer/editor.



And that's it!



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