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.

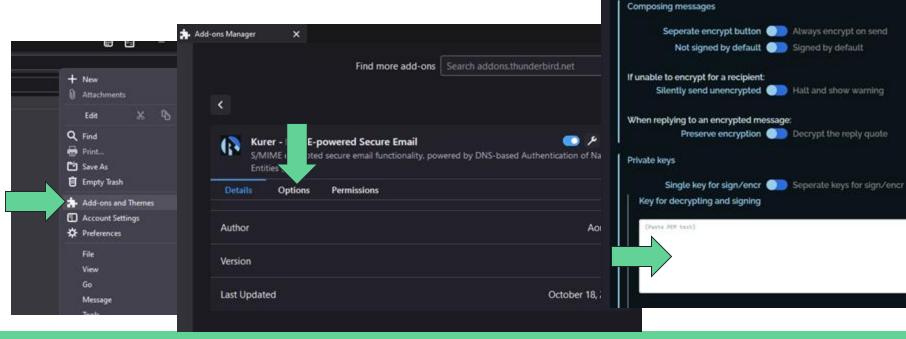
For the curious: there is a separate easy-to-use app to accomplish exactly that

(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



Iror 🚯

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

kurer 🚯

Kurer - DANE-powered Secure Email

Permissions

Details

Entities (DANE)

Options

Only one setting is really needed for now:

Add-ons Manager

٠

Details

Author

Version

Last Updated

5 E

+ New

Q Find

🖶 Print_

C Save As

Empty Trash

* Preferences

File

View

Message

Go

Add-ons and Themes Account Settings

Edit

Attachments

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

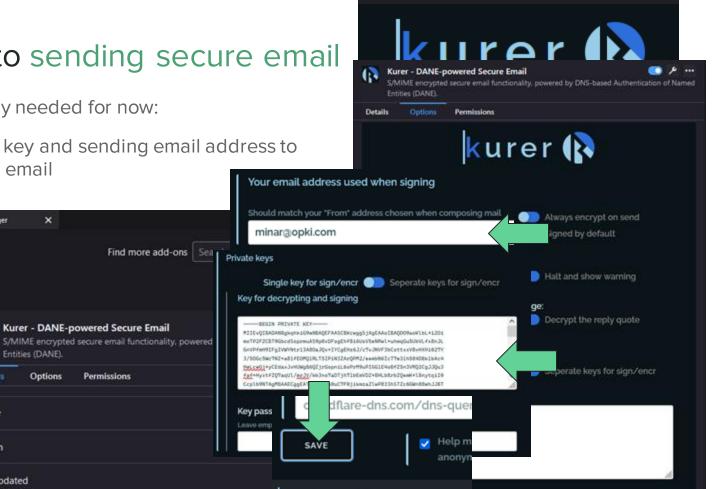
×

Entities (DANE).

Options

Kurer - DANE-powered Secure Email

Permissions



Saved successfully



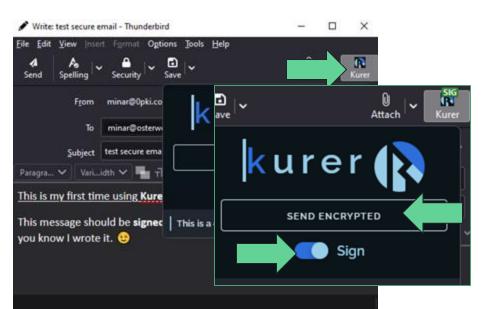
• Compose an email like normal

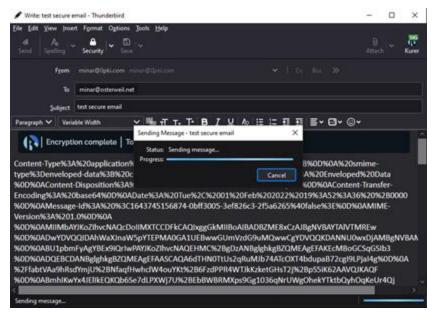
Get Messages 🗸 🖍 Write 🖵 Chat 🛛 Address Book 🛛 🗞 Tag 🗸	۲	uick Fil	ter
✔ Write: (no subject) - T Create a new message	-		×
Elle Edit View Insert Format Options Tools Help Al Ag Send Spelling V Security V Save V	0 Attach	~	() Kurer
Ftom minar@0pki.com minor@0pki.com ↔	Ce	Bcc	»
То			
Subject			
Paragra Variidth V 🖬 T T+ T+ B I U A> 🗄	≣ ¦=	<u>e</u> 2	! ≣~

🖋 Write: test secure er	nail - Thunderbird	-		\times
<u>File Edit V</u> iew Inser	Format Options Tools Help			
A A Send Spelling ∽	<mark>≜</mark> Security ❤ Save ❤	() Attaci	, ~	(P Kurer
From	minar@0pki.com minar@0pki.com 🗸	l c	c Bo	• »
То	minar@osterweil.net			
<u>S</u> ubject	test secure email			
Paragra 🗸 Varii	ath 🗸 🏪 नТ Т+ Т+ 🖪 🛛 🖳 🗞	i≡ 1=	€Đ	∃ ≣
This is my first tim	e using Kurer.			
This message sho you know I wrote	uld be signed and encrypted so only yo it. 😉	u can i	read it	t and



- 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







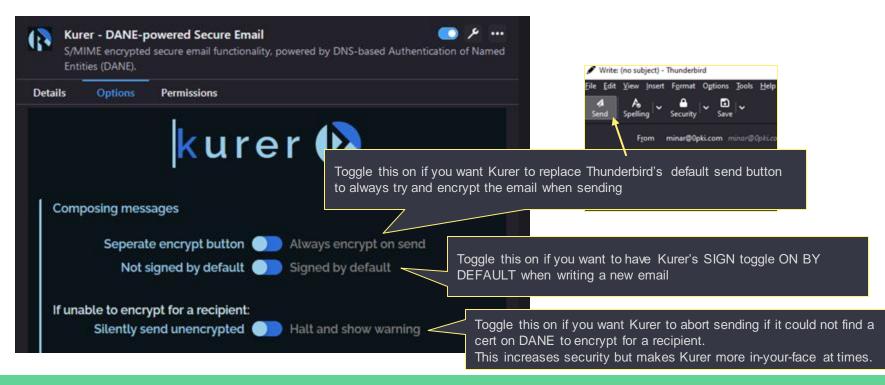
The email has been sent - signed by you and encrypted for the recipient

Ele Edit View Go Message Jools Help Get Messages	ddress Book 🛛 Tag 🛩	Ξ	
From Me «minar@Opti.com» * Subject text secure email To minar@osterweil.net #	Supp A Forward 🙆 Archive	👌 Junk 📋 Delete More 🗸 2:52 PM	Psst: also notice how we are sending secur emails between entirely different email do — this is usually super difficult without DAN
type%lbenveloped-dat%lB%lecharset% %DD%aAcontent-Disposition%la%lecharset% %DD%aAcontent-Disposition%la%lecharset% %DD%aAcontent-Disposition%la%lecharset% %DD%aAbsta%lecharset%lecharset% %DD%aAbsta%lecharset%lecharset%lecharset% %DD%aAbsta%lecharset%lecharset%lecharset%lecharset% %DD%aAbsta%lecharset%lech	37 = mineX3EX20maneX3Dsmine.p7mX3EX00X0AX; 3DblnaryX80X8AContent DescriptionX3AX200 ChementX3EX20F1LenameX3Dsmine.p7mX00X8AC; 874 = 0bff30e5 = 3ef02613 = 2f5a6265X40Fa1seX; FkCAQIXqggGkH1B0ABADB2ME8xCzA3BgHVBAY74 11E8uxGUW4G05MQucGgYDVQQCDMNU0xxDJAN UE8uxGUW4G05MQucGgYDVQQCDMNU0xxDJAN VCMQEHMCX28gDzAH8g1ghkgB2QWEAgFFAKECM8 QA6dTHW0TUS2QUUD3AAFCXT404Upa822cgT M6dFTW0TUS2QUUD3AAFCXT404Upa822cgT M6dFTW0TUS2QUUD3AAFCXT404Upa822cgT M2256F2d97AAFCXT404Upa822cgT M2256F2d97AAFCXT404Upa822cgT M2256F2d97AAFCXT404Upa822cgT M2256F2d97AAFCXT404Upa822cgT M2256F2d97AAFCXT404Upa822cgT M2556F3400F3C23F2 2d40H4;nbz01QT07QFFkHTTxyU0H75ZxL1GET 17M28EbB48890Q5950g1036QHCMQgCheW15ZzxL1GET 17M28EbB48890Q590g103CH22701282W3 2d40H4;nbz01QT07QFFkHTTxyU0H75ZxVL1GET 17M28FD488742CXADQFC41ggA5C4B800P59782b0 3558J1zhM8ygybpD4AhCbmqTKryBXxSAOYYXnQ p22F4X28AL4QT22b1EW7orKRU04FH6X3kDCz1 7XKgVXXxAM42CXADQFUJ1d1MHecGYGJS4T1AN Sun5FPH228EF1KSQh10BTxK1RDF53UUSHAH0 Sun5FPSH2228B67Ug124F51K5Qh10BTxK1RDF53UUSHAH0 Sun5FPSH228B67Ug151K5Qh10BTxK1RDF53UUSHAH0 Sun5FPSH228B67Uy33X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A0444 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25J2042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25JX0404445 Lks1aJ7H8X2B807Um3X25JX042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25JX042842V5Cm10A04445 Lks1aJ7H8X2B807Um3X25JX04284242CM1044445 Lks1aJ7H8X2B807Um3X25JX04284242CM1044445 Lks1aJ7H8X2B807Um3X25JX044445 Lks1aJ7H8X2B807Um3X25JX04284445 Lks1aJ7H8X2B807Um3X25JX044445 Lks1aJ7H8X2B807Um3X25JX044445 Lks1aJ7H8X2B807Um3X25JX04444	inveloped%200ata ontent-Transfer- St20%28040 INX00%0AMINE- AlVTHREW BgN/MAMM SGCSqGSID3 DLPjal4g%00%0A 2AAVQJXAQF 2BHOX0APITI1 UTAGCSqG 1JJNCJy23d Ymt70U182erjj KMC7QIGeHbTq03b7 SGOHXAEtz KDAVbMAM D3mrrUf#Pbyn 7LMAVGS TGQArGHH Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 Cn4bQWYETDKzF%28%00 XZ2028%00 XZ2028%00	

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



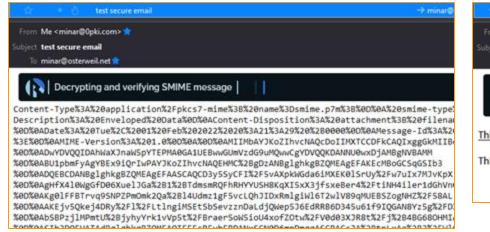
Now, let's take a look at how Kurer makes it easy to read secure email

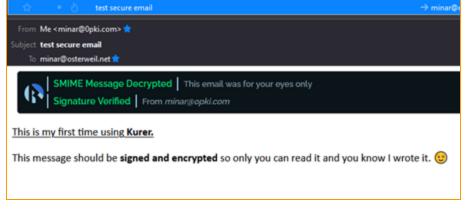
Reading secure email



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



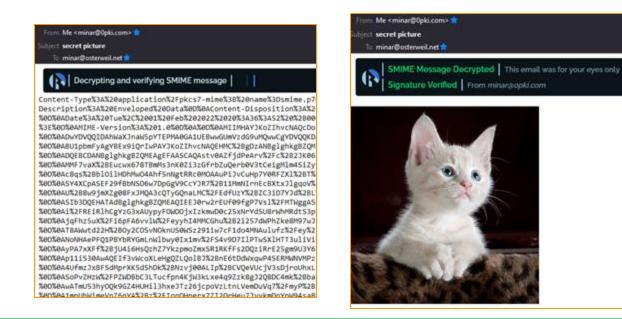


Reading secure email



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:



Decryption failed

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

SMIME Decryption Error Error: SnimeDecryptError Message not signed by sender



Replying



Kurer makes it easy to reply to secure emails

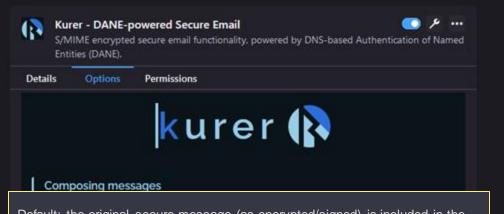
 Just use the normal reply button, and Kurer will show the content of the secure email while you are composing

	5-	bject Re: wassup?																		
Body Text	~	Variable Width	×	•	π	т. Т [.]	в	I	¥	ħ	II	12	£5	Đ	Ē,		• 6	•		
On 2/1/2	022	4:06 PM, mina	@Opki.d	com v	wrote															
¢	18 V(contents of t ey how's it going? Subling this <u>Kurer</u> y sending a reply t	thing?			orig														
type%3 %00%0 Encodie %20%2 %0AMII %00%0 %00%0 %00%0 %28%2	Der ACo 800 ME- AM AA: ASI ABA ARI FBd	pe%3A%20appli weloped-data% sntent-Dispositis 3A%20%05%05%0AMes Version%3A%20 UICTQVIKo2Ihvch UIEAv4IAYQA20 b3DQEBCDANBg stTiwUIKIgPvD 75h%2BOxb4sh% PrCPj6g2v12210 diMinuen 260	BB%20ch xm%3A% DD%0AD sage 1d9 11.0%0D IAQcDol RzAHQC Ighkg82 iRKtTG2 2BzIo9o SiXWs51	harse 20att Aate% 63A% 63A% 63A% 60A ICPJC CAQE0 CQME CQME CQME BII DVGW	t%30 tachr 13A% 20% CAjo wPA AgEF CnGl	binar nent9 20Tu 20Tu 20Tu 20Tu 30Tu 30Tu 30Tu 30Tu 30Tu 30Tu 30Tu 3	y%0 63B% e%20 4374 kggFr hvcN AQA mh%	D%0 206 %206 %206 %620 9610 #MII AQE WTo 2FN 2xE0	ACo lena 2019 (347 Bag HM Fejy %28 26yF	inter ime9 620F 7-686 IBAD C962 81q5 INAb 4hb	it-De 63D eb% 5af4 MJM BgD 5qu7 67Ge 4JF1	escr smit 6200 4a-0 1845 2AN 628 1962 6CD	iptic me.p 2022 27a5 aHDv 18gle 3jjO BH1	on% p7m H62i ie59 AJBg ghkg TqN EN7	3A% %00 021% 1-8a (NVB (BZQ (9XN '0kc)	20Env 960A0 3A06 284b AYTAI MEAg oC[1] x0DFi	relo Cont (63 20% UVN (EFA emw Obd	ped% tent-T ASO HOfal AA8G KEcN vSc4C dISHZ	20Da ransfi Ise%3 IBoGi XX.ef XX.sN	er- E%0D CSqG T VFbp\

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 🚯

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

<u>Default</u>: 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.

pted) Halt and show warning

When replying to an encrypted message:

Sile

Preserve encryption Decrypt the reply quote

<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:



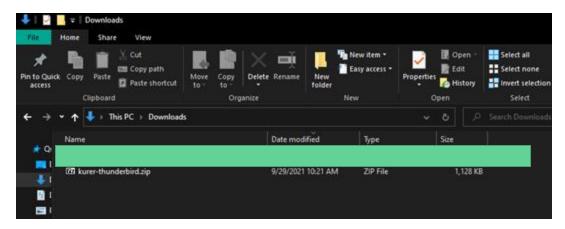
- Compose S/MIME signed / encrypted emails
- Verify / Decrypt S/MIME signed / encrypted emails
- Seamlessly reply in an encrypted conversation

Now how do we install it?

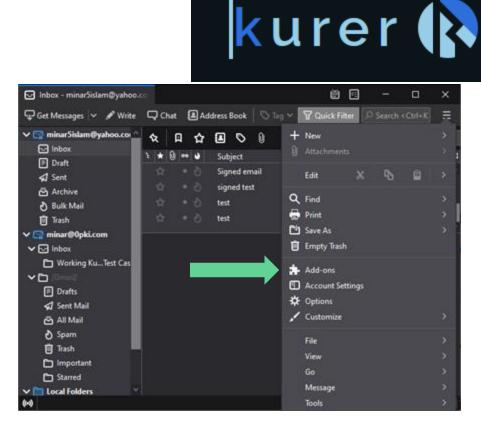


Download Kurer as a zip file.

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



Go to add-ons menu on TB



Select Install from file



☑ Inbox - minar5islam@yahoo.co	Add-ons Manager	×	Ű 🖸			×
	Find more add-ons	Search a	ddons.thunderbi	rd.net		٩
℅ Manage	Your Extensions					*
			Check for Updates	i		
			View Recent Upda	ites		
1			Install Add-on Fro	m File		
			Debug Add-ons			
		1	Update Add-ons A Beset All Add-ons			matica
			Manage Extension			
*						
0						
140		_		_	100	

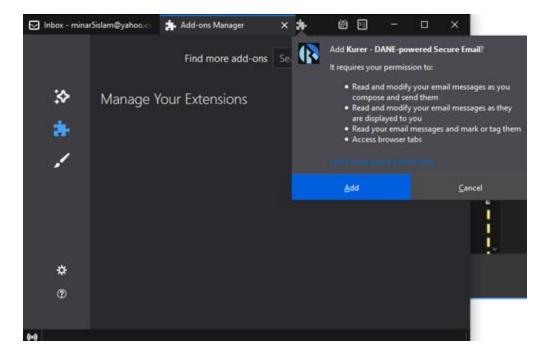


Select the downloaded zip file

Select add-on to install			×
← → ▾ ↑ 🗣 > This PC → Downloads	ٽ ~		
Organize 👻 New folder		Ŀ	- 🔳 😲
^ Name	Date modified	Туре	Size
🖌 🗸 🗸 Today (1)			
kurer-thunderbird.zip	9/29/2021 10:21 AM	ZIP File	1,128 KB
> Earlier this year (1)			
File name: kurer-thunderbird.zij	p ~	Add-ons (*.xpi;*.j Open	ar;*.zip) ~ Cancel



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