



Kurer and DANeportal.net

Minar Islam - tislam20@gmu.edu

Pavan Kumar Dinesh - pdinesh@gmu.edu

Josh Yuen - jyuen2@gmu.edu

Tomofumi Okubo - tomofumi.okubo@digicert.com

Eric Osterweil - eoster@gmu.edu

Support from Commonwealth Cyber Initiative (CCI)

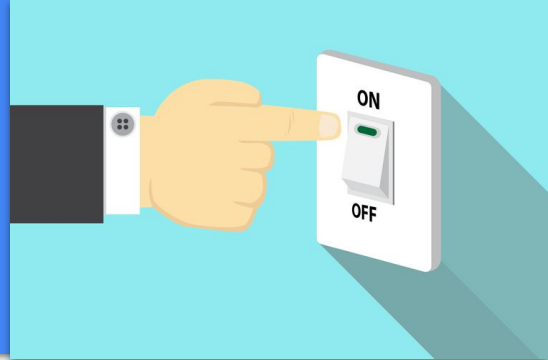
Making DANE easy

Using DANE protocols to power S/MIME

DANE is a powerful protocol suite:

- It makes doing security and privacy **easier**
- But what can we do to make **DANE easier?**

For the everyday person



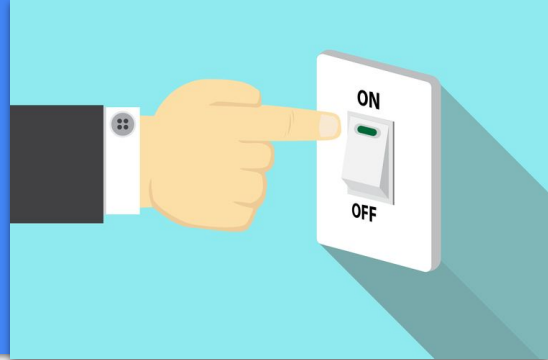
- Why can't people to simply “turn on” secure messaging on the Internet?
 - Platform limitations
 - Organizational boundaries
 - Usability concerns
 - ... Anything else?



We are launching basic research into how **DANE** can unlock **long-needed protections**

- mHealth, Smart and Connected Cities, CTI sharing, 5G/NextG and much more

For the everyday person



- Why can't people to simply “turn on” secure messaging on the Internet?
 - Platform limitations
 - Organizational boundaries
 - Usability concerns
 - ... Anything else?



We are launching basic research into how **DANE** can unlock **long-needed protections**

- mHealth, Smart and Connected Cities, CTI sharing, 5G/NextG and much more

... it starts with **core internet protocols which everyone uses: email**

- To find out exactly what **people need** to make end-to-end Internet security **seamless** and turned on **everywhere: make it invisible**



We need usable tools out there!

“Make it easy”: **secure email with DANE**

- **Setting up DANE** needs work from domain holders / zone admins
- **Using certs from DANE** needs integration with users' mail clients

We need usable tools out there!

“Make it easy”: **secure email with DANE**

- **Setting up DANE** needs work from domain holders
 - Cert management portal [DANEportal.net](https://daneportal.net)

- **Using certs from DANE** needs integration with users' mail clients



We need usable tools out there!

“Make it easy”: **secure email with DANE**

- **Setting up DANE** needs work from domain holders
 - Cert management portal [DANEportal.net](https://daneportal.net)
- **Using certs from DANE** needs integration with users' mail clients
 - MUA add-on [Kurer](#)



We need usable tools out there!

“Make it easy”: **secure email with DANE**

- **Setting up DANE** needs work from domain holders
 - Cert management portal [DANEportal.net](https://daneportal.net)



- **Using certs from DANE** needs integration with users' mail clients
 - MUA add-on [Kurer](#)



... and find out what people need to make **E2E security a default**

We know one thing for sure:

- E2E needs **key management**, and **cert discovery**



And if our ambitions are **Internet-scale**:

DANE is an excellent answer — *and we made just the tool to make it easy*

Making DANE easy:



daneportal.net

- An open-source **federated cert management** portal and dedicated DNS infrastructure **to make DANE easy**
 - Domain holders **enable DANE** for their DNSSEC-signed zone
 - Email users **manage their certs** for their email addresses



Make a new user

- Let's see how a new domain holder would **enable DANE**

A screenshot of a web browser showing the "Create New User" form on the DANE portal. The browser's address bar shows "https://daneportal.net/login#". The page has a dark blue header with a logo on the left and a navigation menu with "LOGIN", "ABOUT", and "DOCS". The "Create New User" form is a white modal with a green header and footer. It contains four input fields: "Username" (filled with "johndoe1"), "Email Address" (filled with "john.doe@aonova.net"), "Password" (filled with dots), and "Confirm Password" (filled with dots). A green "Create User" button is at the bottom right of the form, and a red "Cancel" button is at the bottom left. A blue mouse cursor is pointing at the "Create User" button. A small "New User" notification is visible in the bottom right corner of the page.



Dashboard: claim a zone

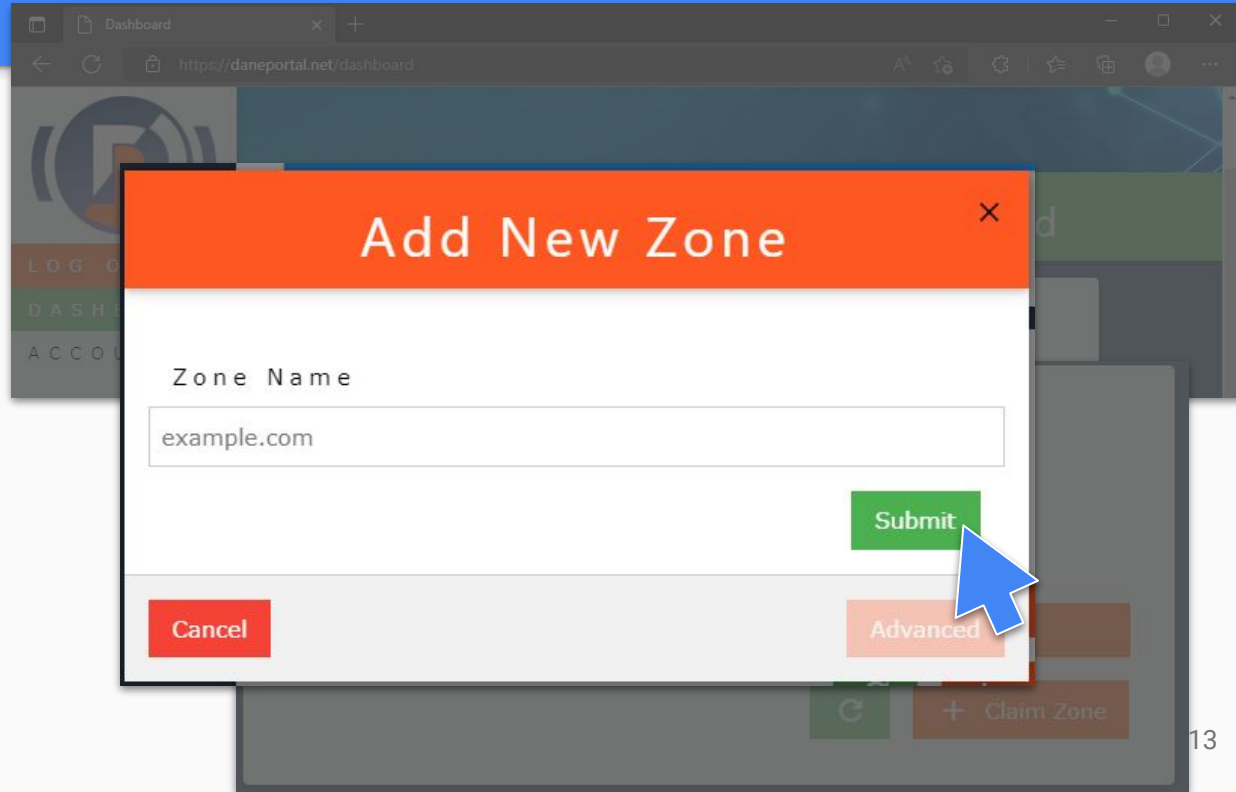
- Users can see the **dane zones** and **email addresses** managed under their portal **dashboard**
- Domain holders can **enable DANE** for their zone by first **claiming it**

The screenshot shows a web browser window with the URL <https://daneportal.net/dashboard>. The page title is "Zone Management Dashboard". On the left, there is a navigation menu with a logo and three items: "LOG OUT", "DASHBOARD", and "ACCOUNT". The main content area shows the user "user johndoe1" and a section titled "managed dane zones". An information icon (i) is followed by text: "These are the zones under your management as an admin. Click one to open the zone management page for that zone. You can claim a zone to start the process of adding your zone here". Below this is a table with two columns: "zone" and "# of emails". At the bottom right, there is a green refresh button and a red "Claim Zone" button with a plus sign, which is being pointed to by a blue mouse cursor.



Dashboard: claim a zone

- Anyone can add a zone claim to their dashboard





Dashboard: claim a zone

- But to actually **create the DANE zone** and **admin it** they will need to **verify** their claim

The screenshot shows a web browser window displaying the 'Zone Management Dashboard' at <https://daneportal.net/dashboard>. The dashboard has a dark blue header with the DANE logo and a green banner with the text 'Zone Management Dashboard'. A sidebar on the left contains a 'LOG OUT' button and links for 'DASHBOARD' and 'ACCOUNT'. The main content area is titled 'managed dane zones' and includes an information icon and text: 'These are the zones under your management as an admin. Click one to open the zone management page for that zone. You can claim a zone to start the process of adding your zone here.' Below this is a table with two columns: 'zone' and '# of emails'. The table contains one entry: 'example.com (unverified)' with a dash in the '# of emails' column. A blue mouse cursor is pointing at the 'example.com (unverified)' entry. At the bottom right of the table area, there is a green refresh button and an orange 'Claim Zone' button.

zone	# of emails
example.com (unverified)	-



Dashboard: verify a claim



To prove ownership and verify, the user will need to add a TXT record and have the zone DNSSEC enabled

A screenshot of a web browser displaying the DANE portal dashboard. The browser's address bar shows 'https://daneportal.net/dashboard'. A modal dialog box titled 'Verify Zone Claim' is open in the foreground. The dialog has an orange header bar with a close button (X) in the top right corner. The main content area is white and contains the text 'example.com verification challenge'. Below this, it says 'To prove control over zone, insert the following token as a TXT record in the _acme-challenge.example.com dns zone and click "Verify" below'. A dark grey text box contains the token 'e4060f52b65f7b33a353c5714886f6dd'. At the bottom of the dialog, there are three buttons: an orange 'Close' button with an X icon, a red 'Remove' button with a trash can icon, and a green 'Verify' button with a checkmark icon. A blue mouse cursor is pointing at the 'Verify' button. In the background, the dashboard interface is partially visible, showing a 'Claim Zone' button and a '# of emails' section.



Dashboard: verify a claim



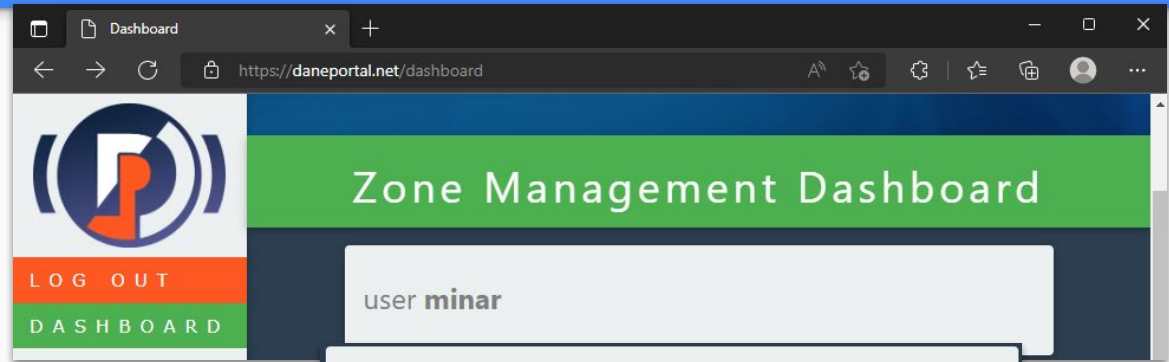
Any DNS provider will work as long as they allow those

A screenshot of a web browser displaying the DANE portal dashboard. The browser's address bar shows "https://daneportal.net/dashboard". A modal dialog box titled "Verify Zone Claim" is open, showing a verification challenge for "example.com". The challenge text reads: "To prove control over zone, insert the following token as a TXT record in the _acme-challenge.example.com dns zone and click 'Verify' below". Below the text is a text input field containing the token "e4060f52b65f7b33a353c5714886f6dd". In the foreground, a DNS record configuration form is visible, showing a record for "_acme-challenge" with type "TXT", TTL "3600", and the same token value. The form includes a "Create new record" link, a "+ Add more to this record" button, and "Cancel" and "Save" buttons. A blue mouse cursor arrow points to the "Save" button. The Google Domains logo is visible in the bottom left corner of the form area.



Let's see a real delegation



Once verified, daneportal will create the DANE zone for you



managed **dane zones**

i These are the zones under your management **as an admin**
Click one to open the **zone management page** for that zone
You can **claim a zone** to start the process of adding your zone here

zone	# of emails
aonova.net	2

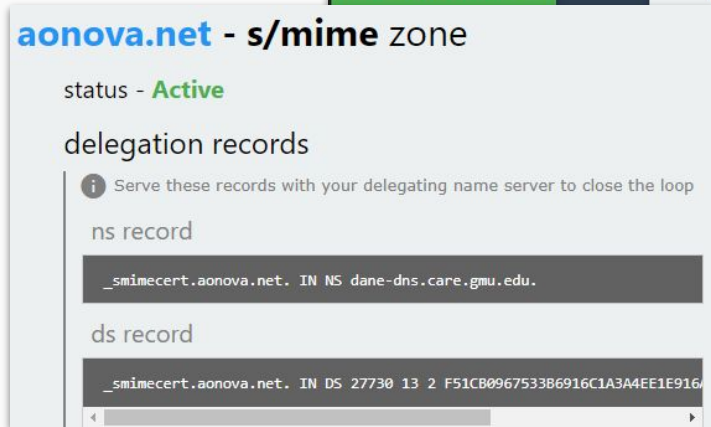
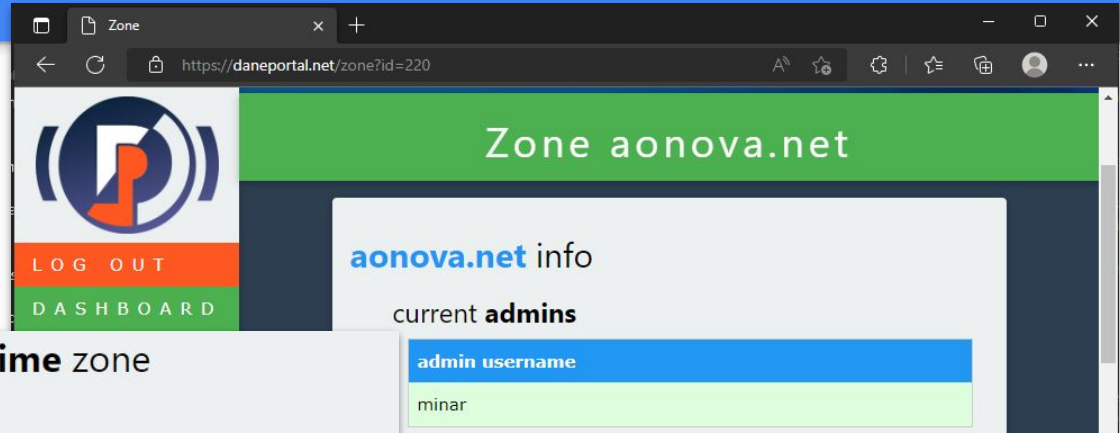
 



Zone management: delegation

Once verified, daneportal will **create the DANE zone for you**

Just complete the delegation to hook it up





Zone management: delegation

Google Domains

Host name	Type	TTL	Data
._smimecert.aonova.net	DS	1 hour	27730 13 2 f51cb0967533b6916c1a3a4ee1e916a3a560b8ec5ac5e398723 9e1b729c82a06
._smimecert.aonova.net	NS	1 hour	dane-dns.care.gmu.edu.

aonova.net - s/mime zone

status - **Active**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
._smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
._smimecert.aonova.net. IN DS 27730 13 2 F51CB0967533B6916C1A3A4EE1E916
```

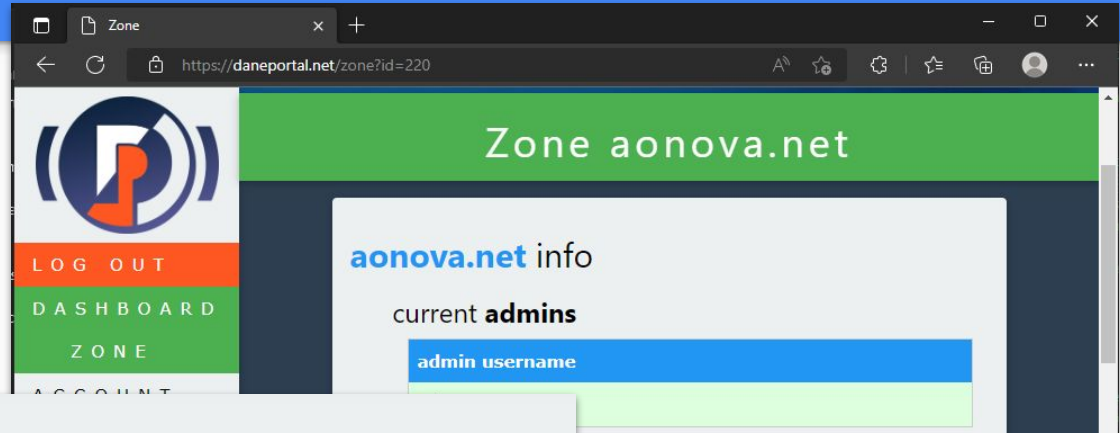
admin username

minar



Zone management: active

As admin you hold all the keys: daneportal will only serve the DANE zone when you **set it active**



aonova.net - s/mime zone
status - **Inactive**

status - **Active**

actions


+ Add domain Remove domains **Set Active**



Zone management: active


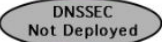
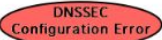
Your DANE zone is now **live** with **DNSSEC**

Confirm it checks out:
secpider.net

 **"_SMIMECERT.AONOVA.NET."**

Home
[Documentation](#)

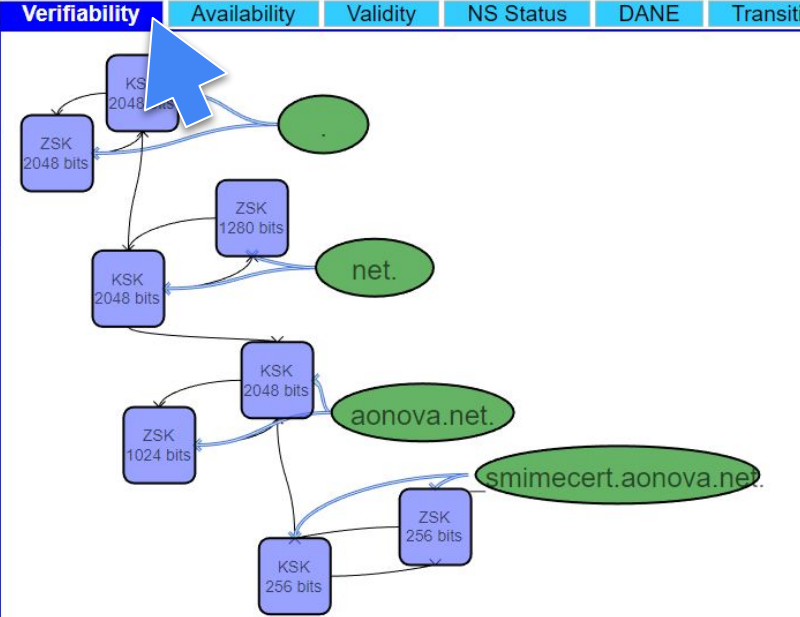
Legend:

-  DNSSEC Verified
-  DNSSEC Not Deployed
-  DNSSEC Configuration Error

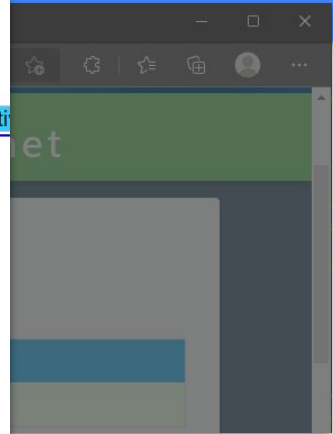
Poll zone now

Note: Polling can take several minutes.

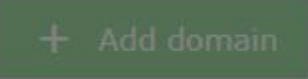

Verifiability | Availability | Validity | NS Status | DANE | Transiti



https://secpider.net/chain-of-trust.cgi?z=_smimecert.aonova.net



actions

 + Add domain 



Zone management: add new email

Zone aonova.net

aonova.net info

current **admins**

admin username

actions

+ Add domain Remove domains Set Inactive

domains

Denizen accessed domains under aonova.net S/MIME DANE zone

Domain	User	Records (active/total)
minar@aonova.net	minar	1/3
tislam20@aonova.net	minar	1/1

Add an email address to **allow cert management** for that entity on daneportal



Zone management: add new email

s/mime zone - new denizen domain

Add new denizen domain to [aonova.net](#) and grant its access to an existing DANEportal user

Domain Name (only local part)

DANEportal Username

Domain Protocol

Zone [aonova.net](#)

[aonova.net](#) info

current **admins**

actions

domains

i Denizen accessed domains under [aonova.net](#) S/MIME DANE zone

Domain	User	Records (active/total)
minar@aonova.net	minar	1/3
tislam20@aonova.net	minar	1/1



Zone management: add new email

A screenshot of a web browser displaying the DANE portal interface. The browser address bar shows the URL https://daneportal.net/zone?id=220. The page title is "Zone aonova.net". The left sidebar contains navigation links: LOG OUT, DASHBOARD, ZONE, and ACCOUNT. The main content area shows "aonova.net info" and "current admins". A modal window titled "domains" is open, displaying a table of domains accessed under the aonova.net S/MIME DANE zone.

Zone aonova.net

aonova.net info

current admins

domains

Denizen accessed domains under aonova.net S/MIME DANE zone

Domain	User	Records (active/total)
minar@aonova.net	minar	1/3
tislam20@aonova.net	minar	1/1
john.doe@aonova.net	johndoe1	0/0



Dashboard: email user

Now lets see how that newly added email user can manage their certs on DANE under your zone

A screenshot of a web browser displaying the "Zone Management Dashboard" for a user named "johndoe1". The dashboard has a green header and a sidebar with a logo and "LOG OUT" and "DASHBOARD" buttons. The main content area shows a section titled "dane-enabled email addresses" with an information icon and text: "These your email addresses which were added by zone admins | Click one to manage its public crypto keys". Below this is a table with columns for "email", "protocol", and "# of records (active/total)". One row is visible for "john.doe@aonova.net" with "SMIME" protocol and "0/0" records. A blue mouse cursor points to the row, and a green refresh button is at the bottom right.

email	protocol	# of records (active/total)
john.doe@aonova.net	SMIME	0/0



Email data: add new cert

A screenshot of a web browser displaying the 'Email Associated Data' page on the DANE portal. The browser's address bar shows the URL 'https://daneportal.net/domain?id=316'. The page has a dark blue background with a green header and a white sidebar. The sidebar contains navigation links: 'LOG OUT', 'DASHBOARD', 'EMAIL', 'ACCOUNT', 'ABOUT', and 'DOCS'. The main content area is titled 'Email Associated Data' and displays the user 'johndoe1' and email 'john.doe@aonova.net'. An information box explains that the page is for managing public data for the email identity 'john.doe@aonova.net'. Below this, a section for 'protocol s/mime' contains an information box stating that it lists 'smime certificates' and provides instructions on how to authorize, deauthorize, or delete them. At the bottom of this section, there is a green '+ New Cert' button and a blue 'Apply' button. A blue mouse cursor is pointing at the '+ New Cert' button.



Email data: add new cert

A screenshot of a web browser showing the "New Cert" form. The browser's address bar shows "https://". The left sidebar contains navigation links: "LOG OUT", "DASHBOARD", "EMAIL", "ACCOUNT", "ABOUT", and "DOCS". The main content area is titled "New Cert" and "Add new cert to john.doe@aonova.net". It features a large dashed box for "Upload certificate file" with a "Choose File" button and a "No file chosen" message. A blue mouse cursor points to a "Make a new cert" button. To the right, there are several dropdown menus: "Nickname to remember this by (optional)" (set to "Unnamed"), "Domain-issued certificate (DANE-EE)" (Usage), "Full certificate (Cert)" (Selector), "No hash used (Full)" (Matching), and "Both (default)" (Signing or encrypting). At the bottom right, there are "Defaults" and "Submit" buttons. An "Apply" button is visible in the top right corner of the form area.



Email data: create a new cert

New Cert

generate new **self-signed s/smime** key and certificate

i This is a convenient way to get a key pair needed to start using S/MIME. DANEportal does not retain any data related to this form.

These fields are for the metadata of the certificate and generally not seen by users. If you don't know/care about it, feel free to leave it at the defaults. Press [**Submit**] to generate the downloads for cert and key.

country *Two letter country code (e.g. "US")*

state *Full state or province name (e.g. "Virginia")*

locality *(e.g. city name)*

organization *(e.g. company name)*

org unit *(e.g. section / department name)*

common name *(e.g. your name)*

validity duration *# of days (e.g. 1Y: "365")*

X Close **✓ Submit**



Email data: create a new cert

A composite image showing the 'New Cert' form on the DANE portal and a download notification. The form has a blue header and contains instructions to generate a self-signed s/mime key and certificate. It includes an information icon and a note that the portal does not retain data. Below the instructions are fields for 'organization' (with 'Example Corp.' as an example) and 'country' (with a note to use two-letter codes). At the bottom of the form are 'Close' and 'Submit' buttons. The download notification is a dark grey box with a white header 'Downloads' and lists a file named '20220721T114153618Z_cert.pem' with an 'Open file' link. Two green callout boxes are overlaid on the bottom of the form: one for the 'Certificate' with the instruction 'Add this cert to DANE on this page (Usage should be "DANE-EE")' and a 'Get' button; the other for the 'Private key' with the instruction 'Install this in your mail app for signing/decrypting' and a 'Get' button.

Downloads

 20220721T114153618Z_cert.pem
[Open file](#)

Certificate

Add this cert to DANE on this page
(Usage should be "DANE-EE")

 Get

Private key

Install this in your mail app for
signing/decrypting

 Get

✕ Close

✓ Submit



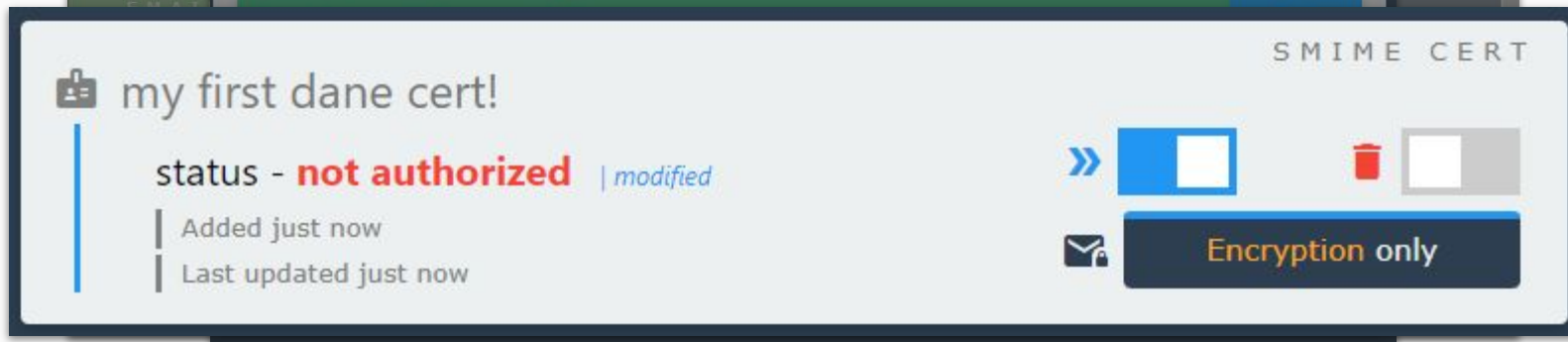
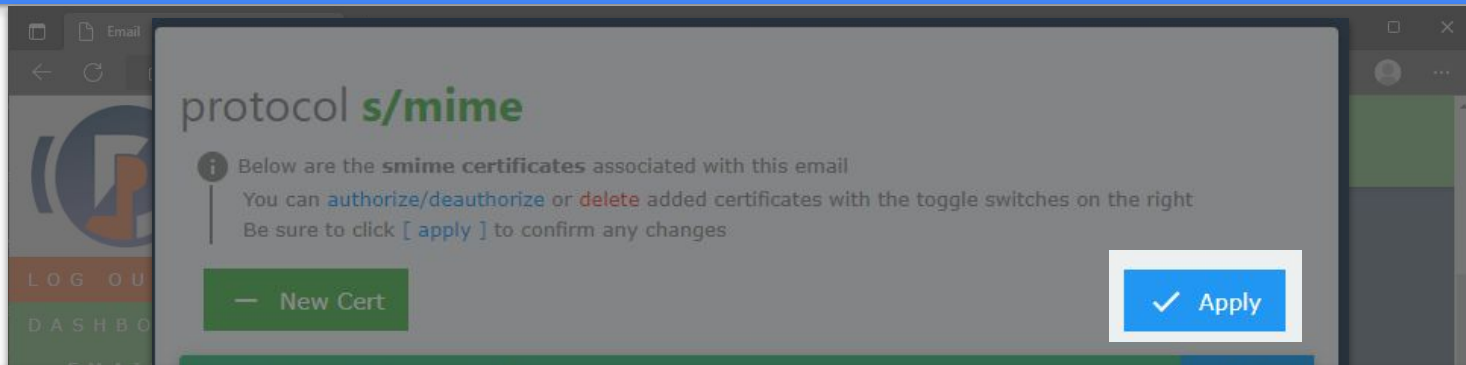
Email data: create a new cert

The screenshot shows a web-based email interface. The main content area displays the following information:

- protocol s/mime**
- An information icon followed by the text: "Below are the **smime certificates** associated with this email. You can [authorize/deauthorize](#) or [delete](#) added certificates with the toggle switches on the right. Be sure to click [[apply](#)] to confirm any changes."
- A green button labeled "New Cert" on the left and a blue button with a checkmark and "Apply" on the right.
- A green success message bar: "Certificate added successfully" with a blue "OK" button on the right.
- A section titled "my first dane cert!" with a sub-header "SMIME CERT".
- The status is "status - **not authorized**".
- Metadata: "Added just now" and "Last updated just now".
- Two toggle switches, both currently turned off.
- A button labeled "Signatures and Encryption" with an envelope icon.



Email data: configure and activate





Email data: configure and activate

A screenshot of an email client interface. The top window is titled "protocol s/mime" and contains an information icon followed by the text: "Below are the smime certificates associated with this email. You can authorize/deauthorize or delete added certificates with the toggle switches on the right. Be sure to click [apply] to confirm any changes." Below this text are two buttons: a green "+ New Cert" button and a light blue "Apply" button with a checkmark. The bottom window is titled "my first dane cert!" and shows a status of "authorized" in green. It also displays "Added 26 hours ago" and "Last updated just now". To the right, there are two toggle switches: the first is blue and active, and the second is grey and inactive. Below the toggles is a dark blue button with a mail icon and the text "Encryption only". The text "SMIME CERT" is visible in the top right of the bottom window.

Making DANE easy:



- **Admin: allow domain holders to enable DANE**
 - Create an account
 - Claim and verify their zone
 - Hook up the DANE zone by DNS delegation
 - Add email addresses / users under their zone
- **Email user: allow federated certificate management**
 - Access their email address under the portal
 - Create/add certificates under their address on DANE
 - Manage the state of their certs
- Check out the docs: <https://daneportal.net/docs>
- Give us feedback: contact@daneportal.net

We saw the first half:

- **Setting up DANE easily**
 - Cert management portal [DANEportal.net](https://daneportal.net)



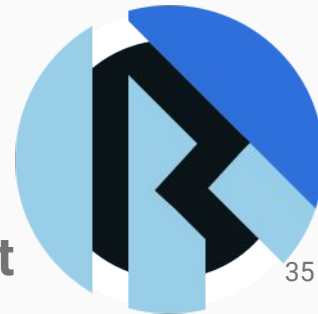
We saw the first half:

- **Setting up DANE easily**
 - Cert management portal [DANEportal.net](https://daneportal.net)



Now for the other half:

- **Using certs from DANE** needs integration with users' mail clients
 - MUA add-on [Kurer](#)



... to find out what people need to make **E2E security a default**

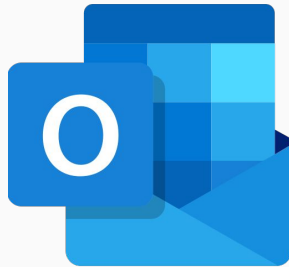
Invisible Security

- We don't have wide-scale E2E email security deployed on the Internet
- **By observing our tools in action** we can find out what makes sense if we are to **make E2E a default**
- To that end we instrumented our next tool as a **live experiment**
 - Where **you can help us** to get some **real numbers** on the human puzzle piece in security automation

Let's show just how easy it is



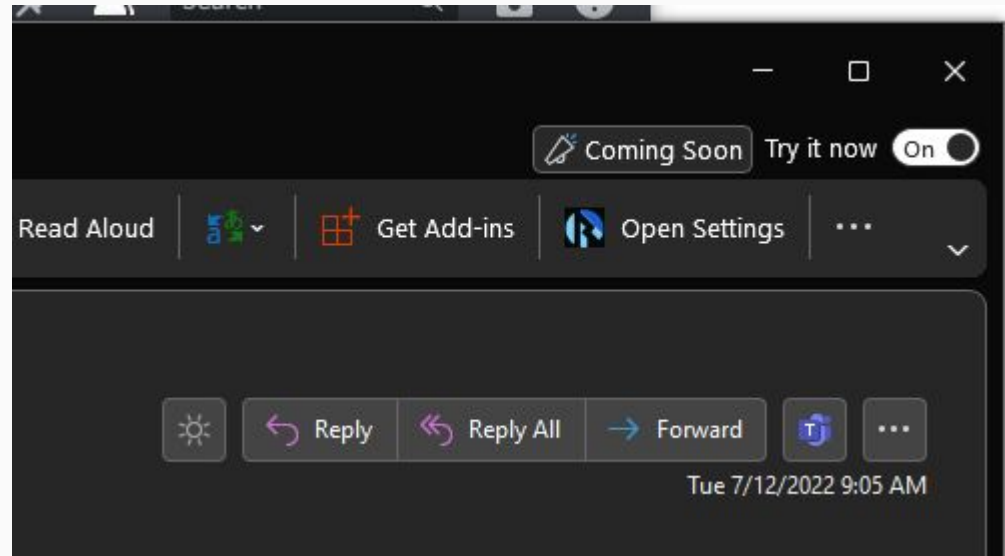
- With **Kurer** on the popular email client of your choice



Hooking it up

You just need to add your **private key** in the settings

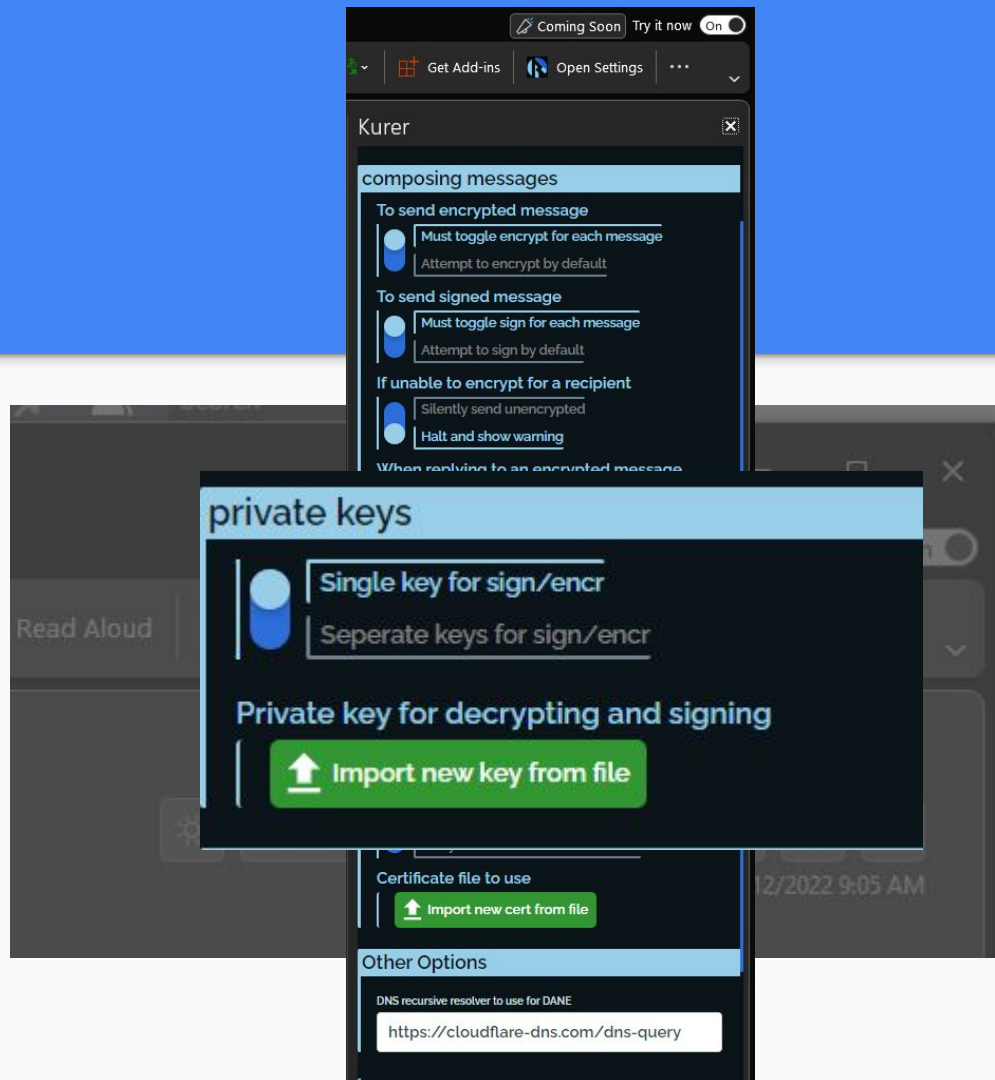
- Enable signing and decrypting



Hooking it up

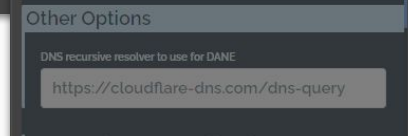
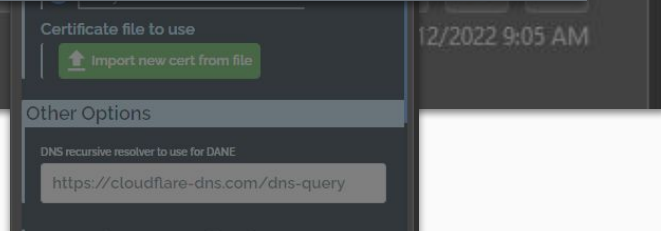
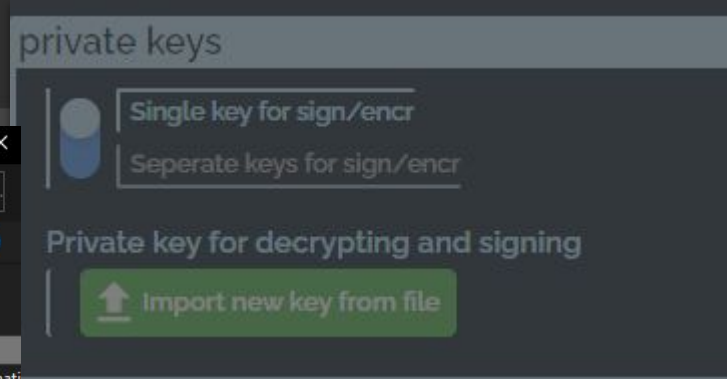
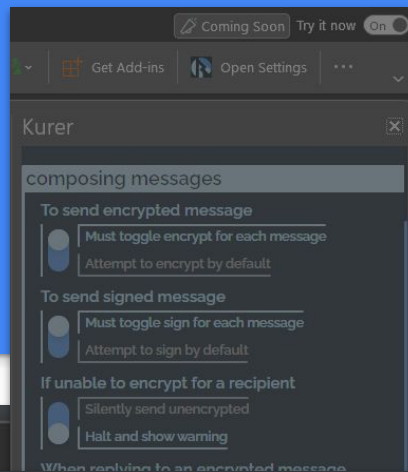
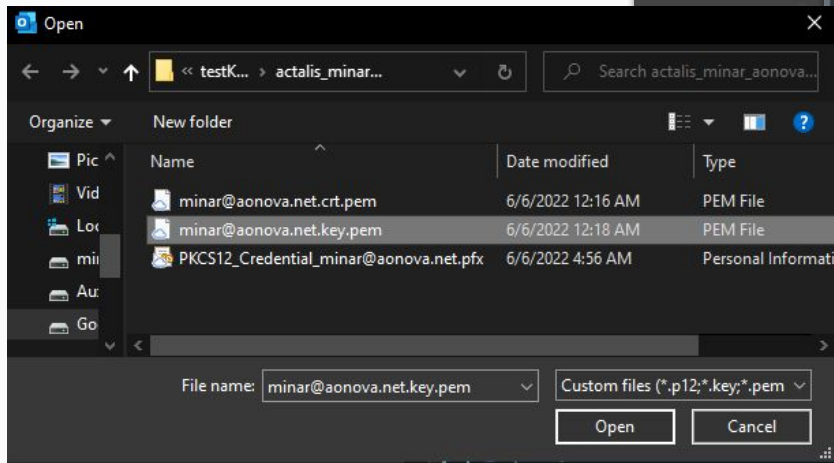
You just need to add your **private key** in the settings

- Enable signing and decrypting



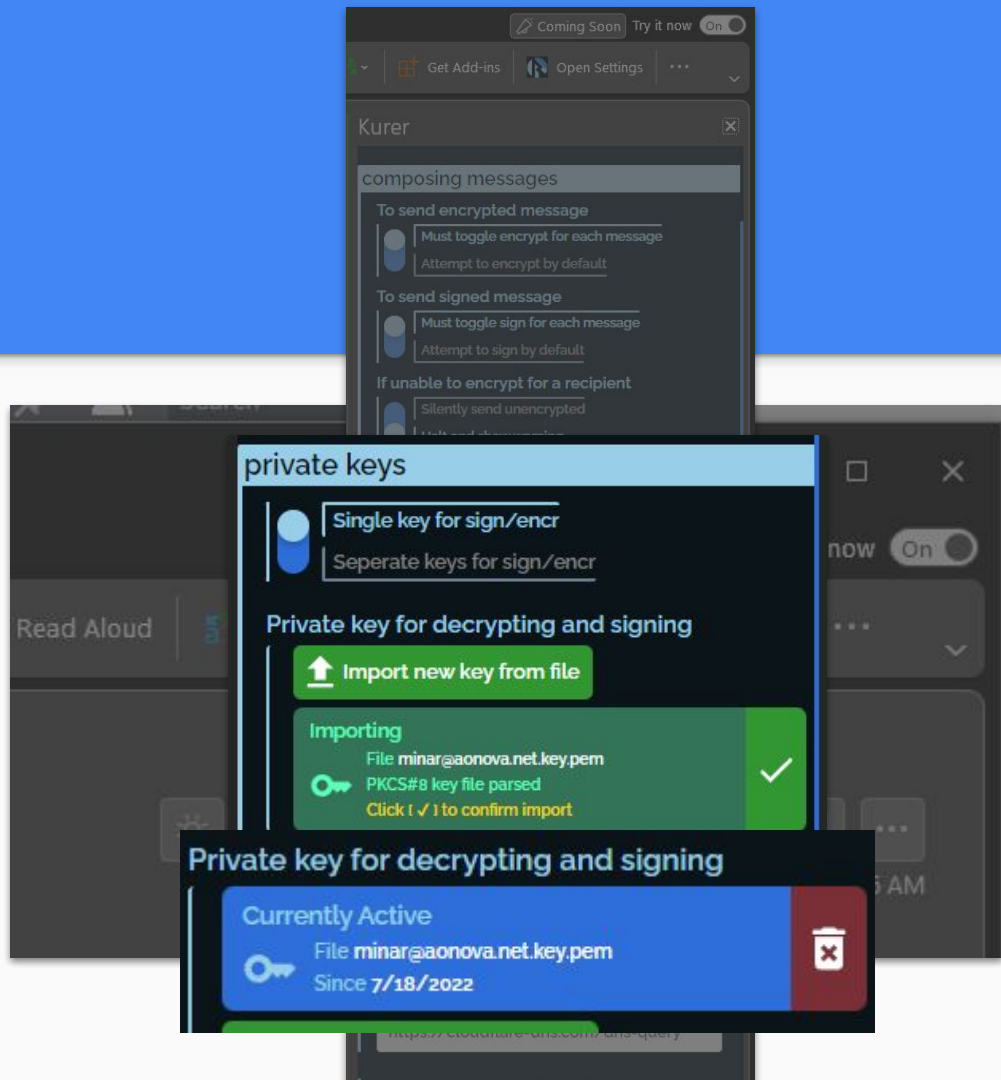
Hooking it up

You just need to add your **private key** in the settings

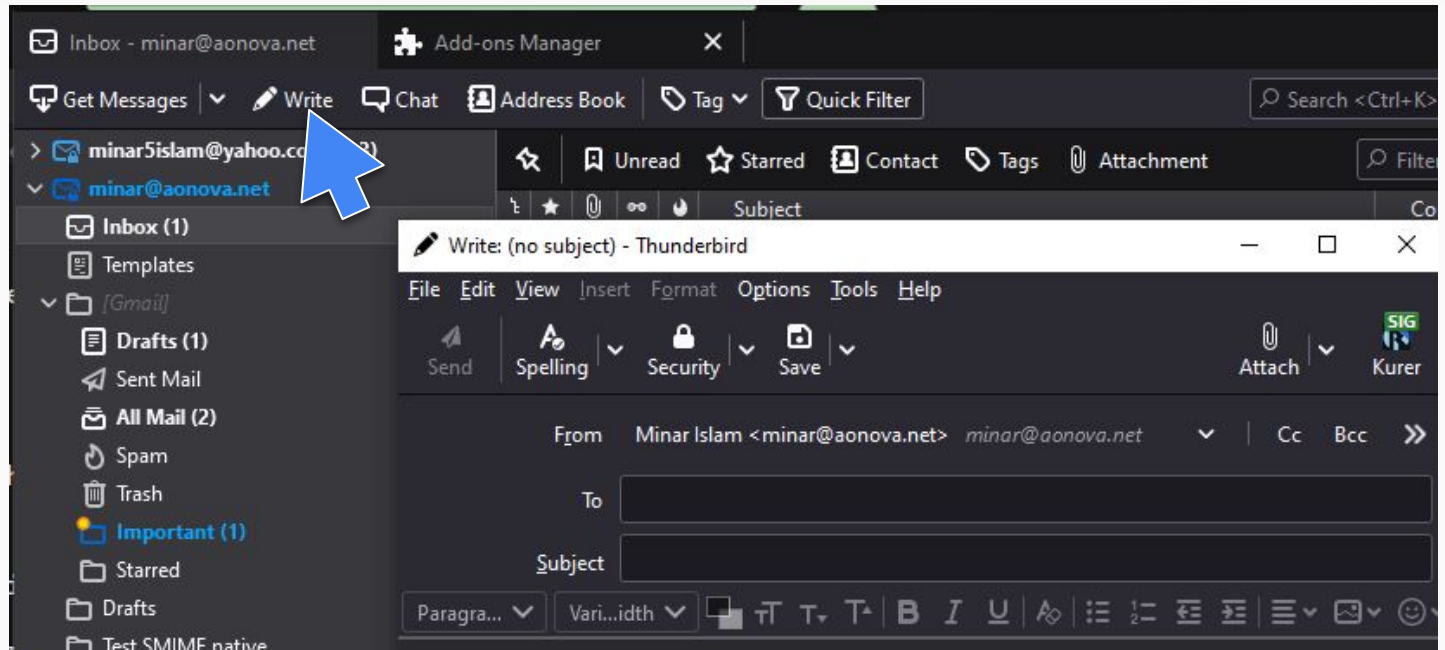


Hooking it up

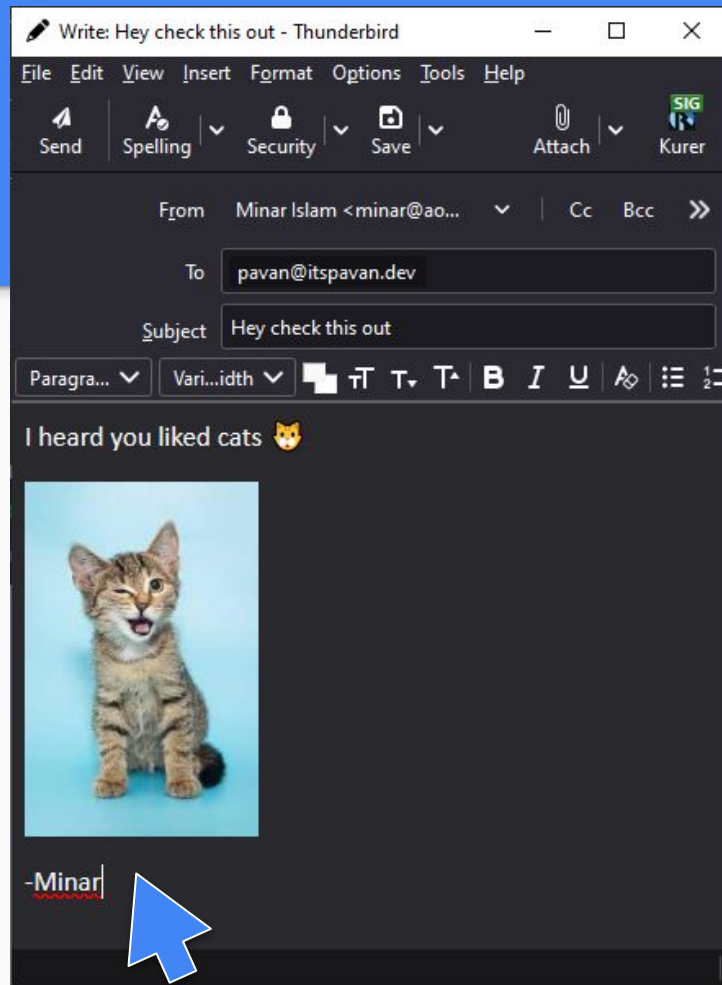
You just need to add your **private key** in the settings



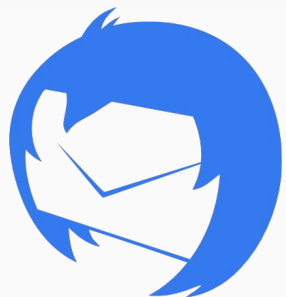
Now jump into a secure email convo with a stranger



Compose as normal



Decide to sign/encrypt



The screenshot shows a Thunderbird email composition window titled "Write: Hey check this out - Thunderbird". The window has a menu bar with "File", "Edit", "View", "Insert", "Format", "Options", "Tools", and "Help". Below the menu bar are buttons for "Send" and "Spelling". On the right side, there is an "Attach" button and a "Kurer" button with a "SIG" label. A blue mouse cursor is pointing at the "Kurer" button. A dark overlay is positioned over the right side of the window, featuring the "kurer" logo (a stylized 'R' in a circle) and the text "SEND ENCRYPTED". Below this, there is a "Sign" toggle switch that is currently turned on. At the bottom of the overlay, there is a link that says "Click to send your email encrypted". The email content is partially visible, showing "From:", "To:", "Subject:", and "I heard you liked". There is also a small image of a kitten and a signature "-Minar|".

One click secure send



Write: Hey dude, got something cool - Thunderbird

File Edit View Insert Format Options Tools Help


Send Spelling Security Save Attach

From Minar Islam <minar@aonova.net> minar

To pavan@itspavan.dev

Subject Hey dude, got something cool

Paragraph Variable Width

 Signing and encrypting to send...

SEND ENCRYPTED


Sign

Click to send your email encrypted

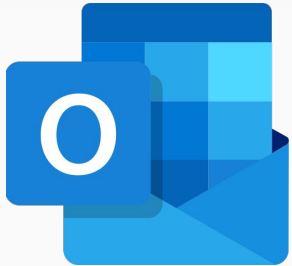
This message has been encrypted using Kurer

+1

1 Attachment 6.6 KB

 dane-smime.kurer 6.6 KB

Read it on the other end

A screenshot of the Outlook web interface. The top bar shows the Outlook logo, a search bar, and navigation icons for 'New message', 'Delete', 'Archive', 'Junk', 'Sweep', and 'Move to'. The left sidebar shows the 'Inbox' with a star icon and a 'Filter' button. A list of emails is shown, with the selected email from 'Minar Islam' having the subject 'Hey check this out' and a timestamp of '9:50 PM'. The email body shows a warning: 'This message has been encrypted using Kurer' and a file attachment 'dane-smime.ku...'. A blue mouse cursor points to the warning text. The right pane shows the email details, including the sender 'Minar Islam <minar@aonova.net>' and the recipient 'To: Pavan Kumar'. The attachment 'dane-smime.kurer' (21 KB) is listed. Below the attachment, a message states: 'This message has been encrypted using Kurer'. At the bottom, there are 'Reply' and 'Forward' buttons.

Outlook

Search

New message Delete Archive Junk Sweep Move to

Inbox ★ Filter

Minar Islam
Hey check this out
This message has been encrypted using Kurer
9:50 PM
dane-smime.ku...

Hey check this out

Minar Islam <minar@aonova.net>
To: Pavan Kumar
dane-smime.kurer
21 KB

This message has been encrypted using Kurer

Reply Forward

Quick security details



The screenshot shows the Outlook interface with an email open. A blue arrow points to a white callout box at the top that says "This message has been encrypted using Kurer". Below this, a black notification bar displays "S/MIME message detected" and "This email was encrypted to you | This email was signed". The email content includes the text "I heard you liked cats 🐱" and a photo of a kitten. At the bottom of the email, another white callout box says "This message has been encrypted using Kurer". The interface also shows an "Inbox" list on the left and "Reply" and "Forward" buttons at the bottom.

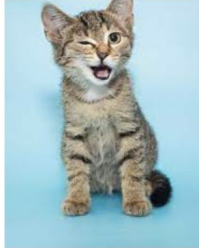
Easily start reply



Outlook

This message has been encrypted using Kurer

S/MIME message detected



-Minar

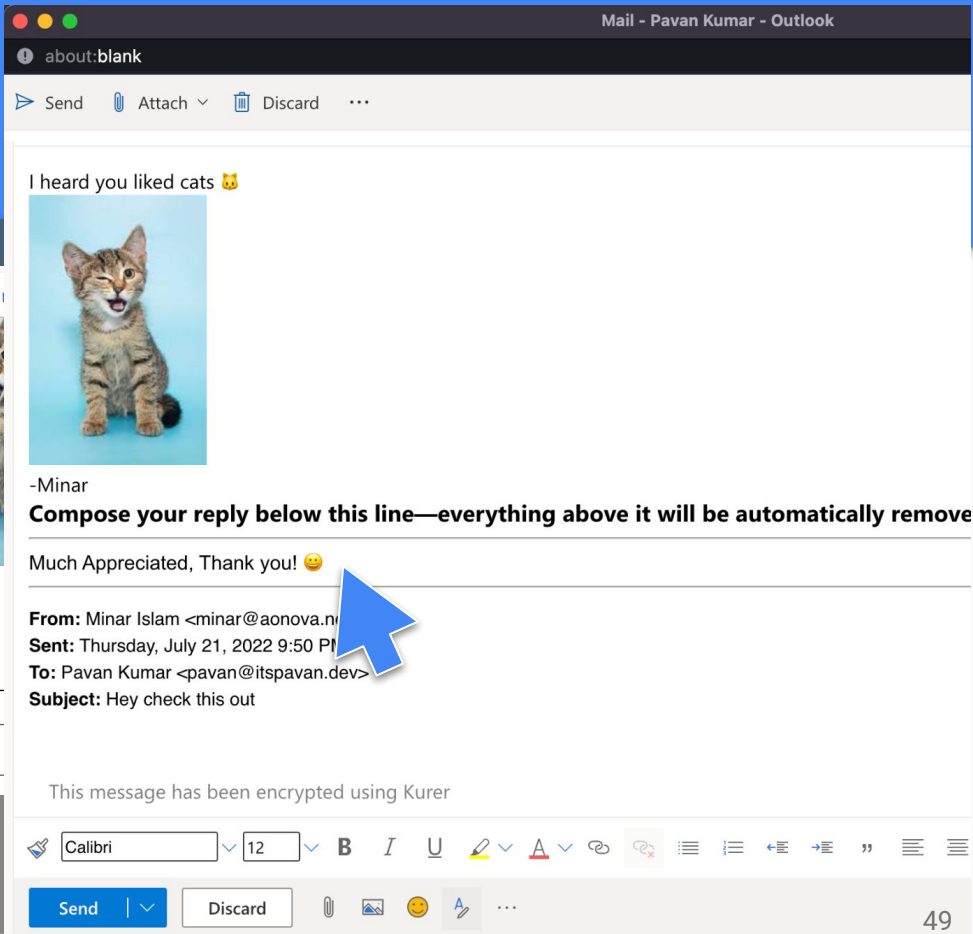
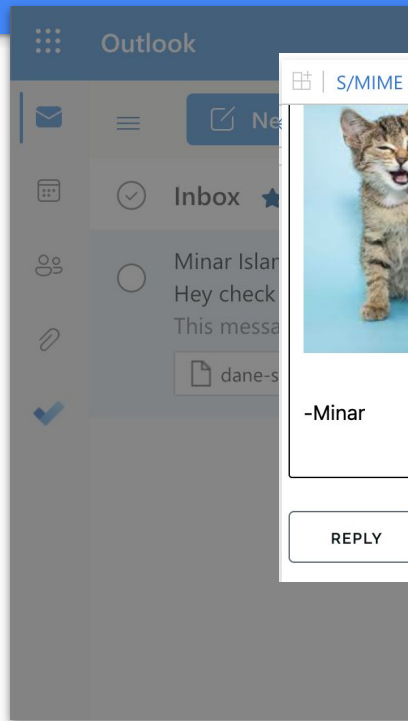
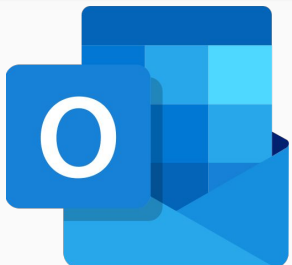
REPLY REPLY ALL FORWARD (UNDER DEVELOPMENT)

← Reply → Forward

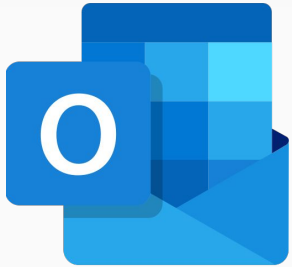
48

The image shows a screenshot of the Outlook interface. At the top, a blue banner contains the text 'Easily start reply'. On the left is the Outlook logo. The main content is a screenshot of an email client. At the top of the email view, a white box contains the text 'This message has been encrypted using Kurer'. Below this, a white box displays 'S/MIME message detected' above a photo of a small, brown and white kitten. Underneath the photo is the text '-Minar'. At the bottom of this white box are three buttons: 'REPLY', 'REPLY ALL', and 'FORWARD (UNDER DEVELOPMENT)'. A blue mouse cursor is pointing at the 'REPLY' button. In the background, the Outlook interface is visible, including an 'Inbox' list with an email from 'Minar Islam' and a 'Move to' dropdown menu. At the bottom of the Outlook window, there are 'Reply' and 'Forward' buttons with arrows. The number '48' is in the bottom right corner.

Reply as normal



Secure send reply



The screenshot shows the Outlook 'Compose your reply' interface. A context menu is open over the 'Kurer' encryption options. The menu items are:

- Editor
- Save draft
- Insert signature
- Show From
- Set importance >
- Switch to plain text
- Check for accessibility issues
- Set Permissions >
- Show message options...
- Kurer** > (highlighted)
 - Kurer
 - Open Settings
 - Toggle encryption
 - Toggle signing
- Polls
- My Templates

The email content includes a cat image, the text '-Minar', and the subject 'Compose your reply below this line—ever...'. The recipient information is: 'From: Minar Islam <minar@aonova.net>', 'Sent: Thursday, July 21, 2022 9:50 PM', 'To: Pavan Kumar <pavan@itspavan.dev>', and 'Subject: Hey check this out'. The status bar at the bottom indicates 'This message has been encrypted using Kurer'.

Read the reply



The screenshot displays the Mozilla Thunderbird email interface. The main window shows the 'Inbox - minar@aonova.net' with a list of folders and messages. A blue mouse cursor points to the 'Inbox' folder. A message titled 'Re: Hey check this out' from Pavan Kumar is selected. A secondary window titled 'Hey check this out - Mozilla Thunderbird' is open, showing the message details. The message is from Pavan Kumar <pavan@itspavan.dev> and is addressed to 'Me <minar@aonova.net>'. The subject is 'Re: Hey check this out'. The message content is a large white box with the text 'This message has been encrypted using Kurer'. At the bottom, it indicates '1 attachment: dane-smime.kurer 21.9 KB'.

Subject	Correspondents	Date
Re: Hey check this out	Pavan Kumar	10:42 PM

From: Pavan Kumar <pavan@itspavan.dev> ★

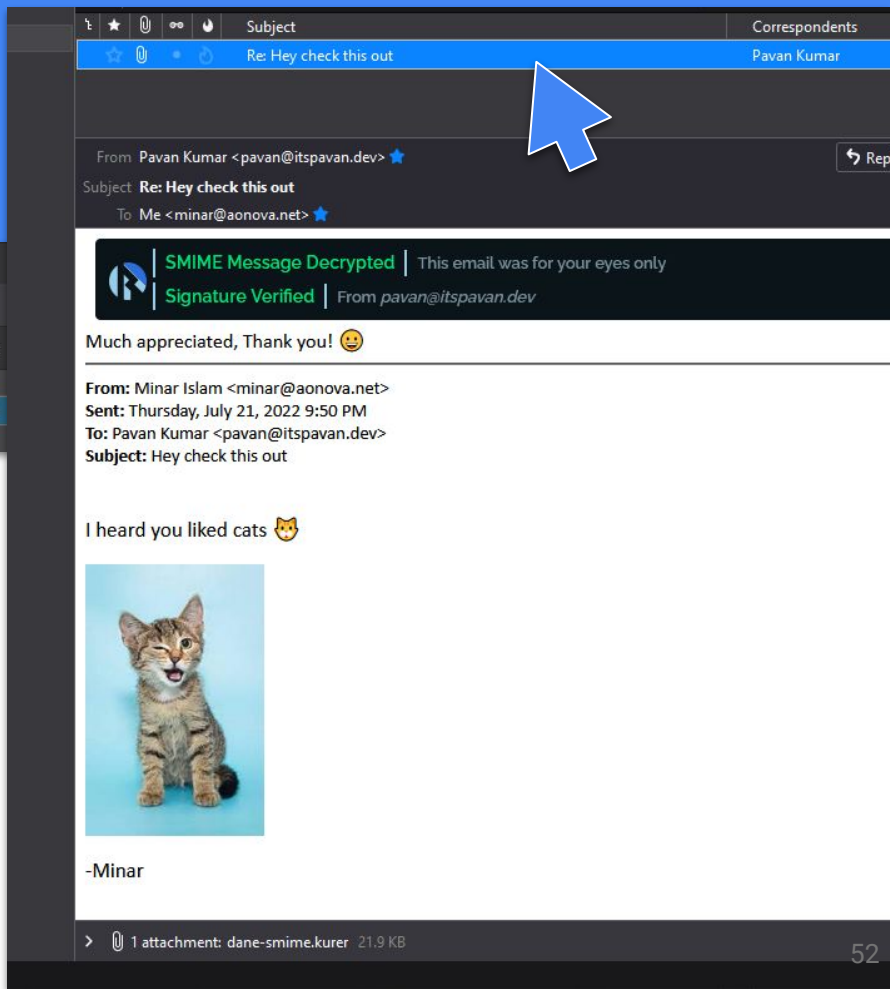
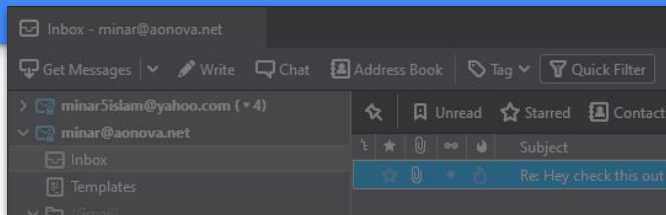
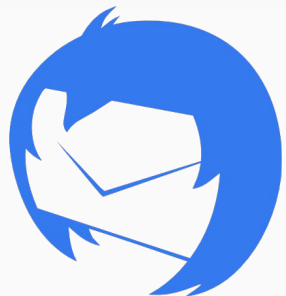
Subject: **Re: Hey check this out** 10:42 PM

To: Me <minar@aonova.net> ★

This message has been encrypted using Kurer

1 attachment: dane-smime.kurer 21.9 KB

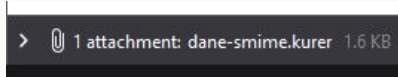
Seamless secure convo





Kurer: details

- Secure messages sent as attachments (standard PKCS7 S/MIME)



```
Content-Type: application/pkcs7-mime; name=smime.p7m;
  smime-type=enveloped-data; charset=binary
Content-Description: Enveloped Data
Content-Disposition: attachment; filename=smime.p7m
Content-Transfer-Encoding: base64
Date: Fri, 15 Jul 2022 15:46:42 +0000
Message-Id: <1657900002932-8ede23ae-29300195-27d3d300@localhost>
MIME-Version: 1.0

MIIDsgYJKoZIhvcNAQcDoIIDozCCA58CAQIxxggHiMIIB3gIBADCBljCBgTELMaKGA1UEBhMCSVQx
EDA0BgNVBAGMB0JlcmdhbW8xGTAXBgNVBACMEFBvbnRlIFNhbWV0cm8xZAVBgNVBAoMDkFj
dGFsaXMgUy5wLkEuMSwwKgYDVQQDDCNBY3RhbGZlIENSaWVudCBBDXRoZW50aW5hdGlvbiBDQSBH
```

- DANE cert resolution handled **silently** and **directly**
 - Does not step on client keystore
 - Can honor DANE cert **Usage** (even without PKIX)



Kurer: details

Live right now (<https://kurer.daneportal.net>) and open source

- For **Outlook** - Exchange synchronized add-on
- And **Thunderbird** - Standard .xpi package
- Standard installation flows

It's not just a convenient tool:

- Vital part of our research to discover **what people need and expect** to make E2E security a default at scale

What do people need?



We saw how people configure their keys, but what other settings to people need?

- We've condensed to a set of usable settings
 - with (what we believe to be) sane defaults
- What should be **silent vs explicit**?

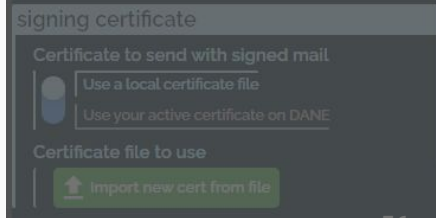
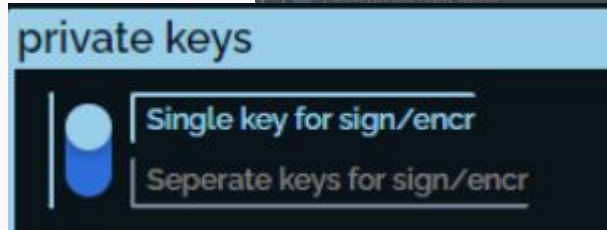


What do people need?



We saw how people configure their keys, but what other settings to people need?

- We've condensed to a set of usable settings
 - with (what we believe to be) sane defaults
- We can **learn** from what they choose



Send anonymous config preferences to help us make Internet crypto more usable

Invisible Security: how?

- Kurer lets users **opt-in** to an anonymous user study
 - IRB approved

This is where **you can help us** to see what the shape of needed security is

Did you know?

Kurer is an [open-source project](#) and part of a study looking at cryptography designed for everyday people.

You can help us make it more usable by allowing Kurer to securely share anonymous configuration (only) statistics

If you accept, Kurer will share your preferred configuration choices anonymously. (i.e., data containing the toggle options you set on the options page)

This is only sent when clicking "Save".

Kurer will never track any email activity when reading or composing emails.

Kurer will also never send any other written input fields such as your keys or passwords, etc.

You are free to decline and continue to use Kurer without any restrictions

Would you like to opt-in?

ACCEPT

NO THANKS

Send anonymous config preferences to help us make Internet crypto more usable

Invisible Security: nitty gritty

- When accepted, **certain settings toggles** will be securely shared with our telemetry server
 - Also, DoH resolver configured will be shared (if it is on the list of known public servers)

The screenshot shows a settings menu with several sections, each with a blue toggle switch and two options:

- To send encrypted message**
 - Must toggle encrypt for each message
 - Attempt to encrypt by default
- To send signed message**
 - Must toggle sign for each message
 - Attempt to sign by default
- If unable to encrypt for a recipient**
 - Silently send unencrypted
 - Halt and show warning
- When replying to an encrypted message**
 - Preserve encryption in reply quote
 - Decrypt the reply quote

Below these sections is a section titled "private keys" with a blue header bar:

- Single key for sign/encr
- Separate keys for sign/encr

At the bottom, there is a field for "DNS recursive resolver to use for DANE" with the value "https://cloudflare-dns.com/dns-query".

Send anonymous config preferences to help us make Internet crypto more usable

Invisible Security: nitty gritty

- Users can **optionally** answer basic demographic queries

Did you know?

Kurer is an [open-source project](#) and part of a study looking at cryptography designed for everyday people.

You can help us make it more usable by allowing Kurer to securely share anonymous configuration (only) statistics

You chose to opt-in to anonymous data sharing

OK CANCEL

Can you tell us a bit about yourself? (optional)

Please select your age bracket

23-25

Please select your country of residence

United States

Please select the category which best describes your occupation

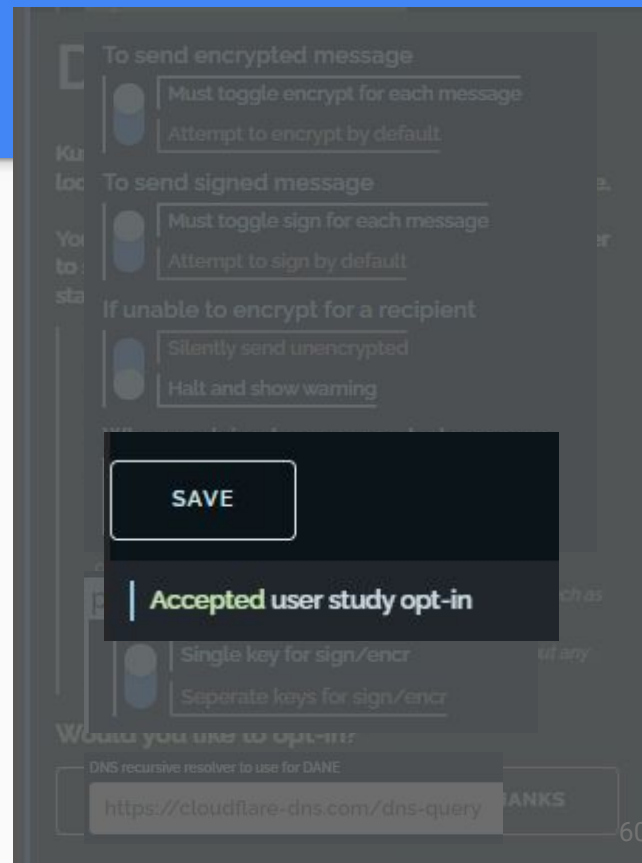
Education

59

Send anonymous config preferences to help us make Internet crypto more usable

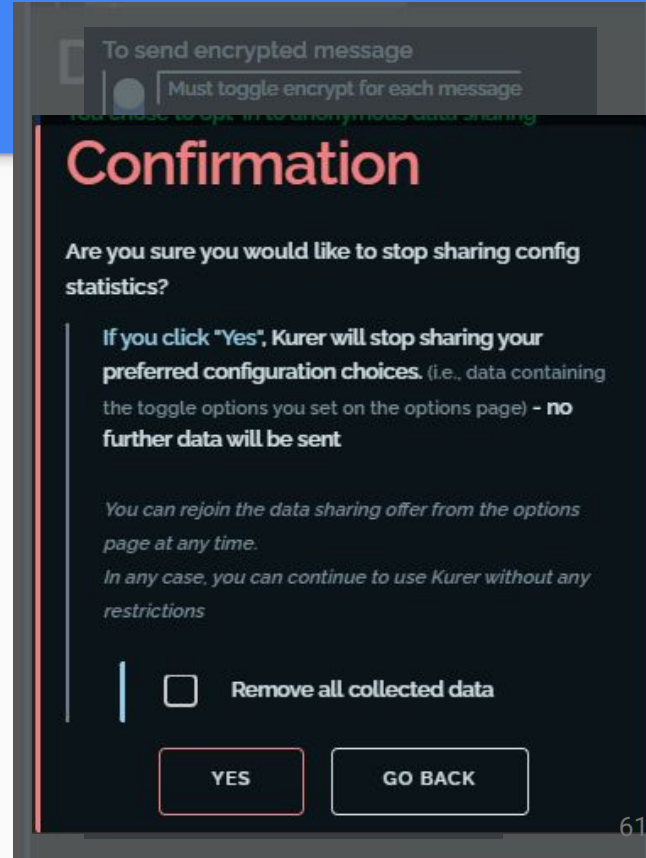
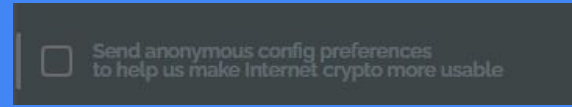
Invisible Security: nitty gritty

- Does **not** invade your privacy:
 - **Telemetry is only shared** when clicking “save” on the settings page after opting-in the user study
 - We **never** track or care about your emails, only noting the set default configs



Invisible Security: nitty gritty

- You have the **right to be forgotten**
 - Users can **toggle off** their participation at any time
 - On top of sent data being anonymous, users can also **request all the data** ever sent from their current install **to be purged**



Send anonymous config preferences to help us make Internet crypto more usable

We can't do it alone

We would greatly value your participation!

- Help us **produce the results** that show what people need, to automate and enable *invisible security* on the Internet

Did you know?

Kurer is an [open-source project](#) and part of a study looking at cryptography designed for everyday people.

You can help us make it more usable by allowing Kurer to securely share anonymous configuration (only) statistics

If you accept, Kurer will share your preferred configuration choices anonymously. (i.e., data containing the toggle options you set on the options page)

This is only sent when clicking "Save".

Kurer will never track any email activity when reading or composing emails.

Kurer will also never send any other written input fields such as your keys or passwords, etc.

You are free to decline and continue to use Kurer without any restrictions

Would you like to opt-in?

ACCEPT

NO THANKS

Big picture

- **DANE** as an architecture lets us make E2E security more seamless for the everyday person on the Internet
- In the past the IETF made a push for “HTTPS everywhere” - and we now live in a world where Internet-scale transport security is the default
 - We believe that sort of ubiquity should be the case for E2E: *Internet-scale Object Security*
- We start with tools for email security — but this is the proving grounds
 - Try them out, and help us **to see what users need**
 - Further our research on using DANE advance CTI, mHealth, SCC, etc, **to be what users actually need**

Thank you