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 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 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](http://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](http://DANEportal.net)

- Using certs from DANE needs integration with users’ mail clients
  - MUA add-on [Kurer](http://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

- 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
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.
Anyone can add a zone claim to their dashboard.
But to actually **create the DANE zone** and **admin it** they will need to **verify** their claim.
Dashboard: verify a claim

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

Any DNS provider will work as long as they allow those
Let’s see a real delegation

Once verified, daneportal will create the DANE zone for you
Zone management: delegation

Once verified, daneportal will create the DANE zone for you

Just complete the delegation to hook it up
Zone management: delegation

- ds record
  `_smimecert.aonova.net. IN DS 27730 13 2 f51cb0967533b6916c1a3a4ee1e916a3a560b8ec5ac5e3987239e1b729c82a06`

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

- Host name: `_smimecert.aonova.net`
  - Type: DS
  - TTL: 1 hour
  - Data: 27730 13 2 f51cb0967533b6916c1a3a4ee1e916a3a560b8ec5ac5e3987239e1b729c82a06

- Host name: `_smimecert.aonova.net`
  - Type: NS
  - TTL: 1 hour
  - Data: dane-dns.care.gmu.edu.
Zone management: active

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

Your DANE zone is now live with DNSSEC

Confirm it checks out: secspider.net
Zone management: add new email

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

- **john.doe**
  - Domain Name (only local part)
- **johndoe1**
  - DANEportal Username
- **S/MIME**
  - Domain Protocol

[Submit]
Zone management: add new email
Dashboard: email user

Now let's see how that newly added email user can manage their certs on DANE under your zone.
Email data: add new cert
Email data: add new cert
Email data: create a new cert
Email data: create a new cert

New Cert

generate new self-signed s/smime key and certificate

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.

20220721T114153618Z_cert.pem
Open file

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

Installation for your mail app for signing/decrypting
Email data: create a new cert

Protocol s/mime

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.

- New Cert

Certificate added successfully

Status: not authorized
Added just now
Last updated just now
Signatures and Encryption
Email data: configure and activate

Protocol s/mime

- Below are the s/mime 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.

New Cert

Apply

My first dane cert!

Status - not authorized | modified

- Added just now
- Last updated just now

Encryption only
Email data: configure and activate

**protocol s/mime**

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.

+ New Cert

**my first dane cert!**

- **status**: authorized
- Added 26 hours ago
- Last updated just now

Encryption only
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 dets: [https://daneportal.net/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](http://DANEportal.net)
We saw the first half:

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

Now for the other half:

- Using certs from DANE needs integration with users’ mail clients
  - MUA add-on [Kurer](http://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
One click secure send
Read it on the other end

Hey check this out

Minar Islam <minar@aonova.net>
To: Pavan Kumar

This message has been encrypted using Kurer

Reply Forward
Quick security details
Easily start reply
I heard you liked cats 😻

-Minar

Compose your reply below this line—everything above it will be automatically removed.

Much Appreciated, Thank you! 😊

From: Minar Islam <minar@aonova.net>
Sent: Thursday, July 21, 2022 9:50 PM
To: Pavan Kumar <pavan@itspavan.dev>
Subject: Hey check this out
Much Appreciated, Thank you! 😊

From: Minar Islam <minar@aonova.net>
Sent: Thursday, July 21, 2022 9:50 PM
To: Pavan Kumar <pavan@itspavan.dev>
Subject: Hey check this out

This message has been encrypted using Kurer

Toggle signing
Read the reply

This message has been encrypted using Kurer
Seamless secure convo

Subject: Re: Hey check this out
To: Minar Islam <minar@aonova.net>
Sent: Thursday, July 21, 2022 9:50 PM

I heard you liked cats 😸

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

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](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 do 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 do 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
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
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)
Invisible Security: nitty gritty

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