



## ILLUSTRATING AN ARCHITECTURE FOR INTERNET-SCALE OBJECT-SECURITY: SECURE MESSAGING FOR TODAY AND TOMORROW

Tawhidal Islam - [tislam20@gmu.edu](mailto:tislam20@gmu.edu)

Josh Yuen - [jyuen2@gmu.edu](mailto:jyuen2@gmu.edu)

Pavan Kumar Dinesh - [pdinesh@gmu.edu](mailto:pdinesh@gmu.edu)

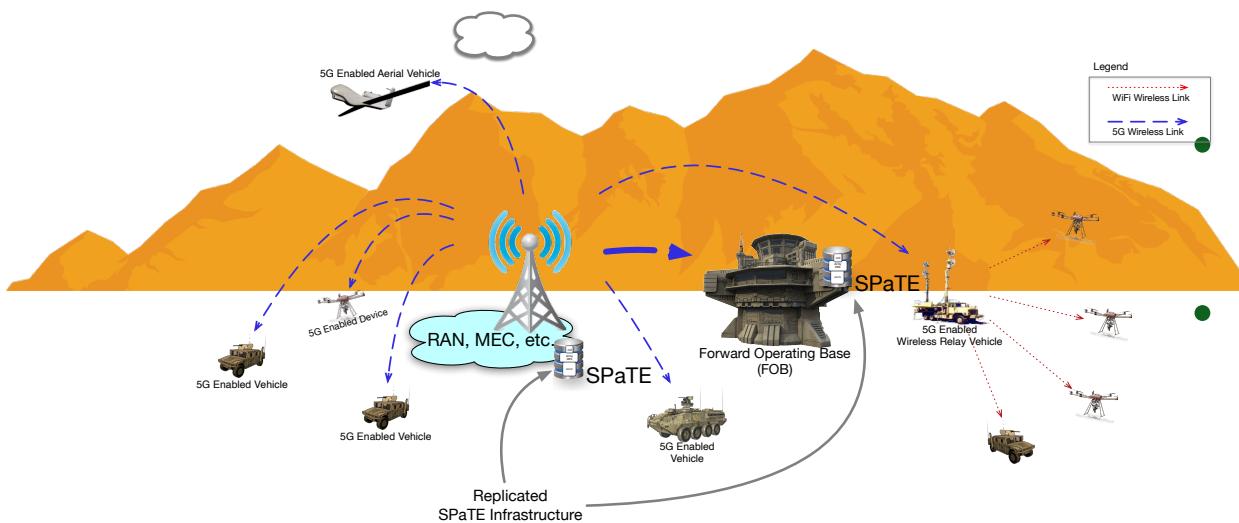
Tomofumi Okubo - [tomofumi.okubo@digicert.com](mailto:tomofumi.okubo@digicert.com)

Eric Osterweil - [eoster@gmu.edu](mailto:eoster@gmu.edu)



# WHAT ARE WE AIMING AT?

- What has made things so difficult in transacting securely/privately between, say, a fire engine, a municipal traffic signal, and my POV Tesla?
- How can independent devices/entities authenticate and encrypt their **messages** to each other with zero trust?



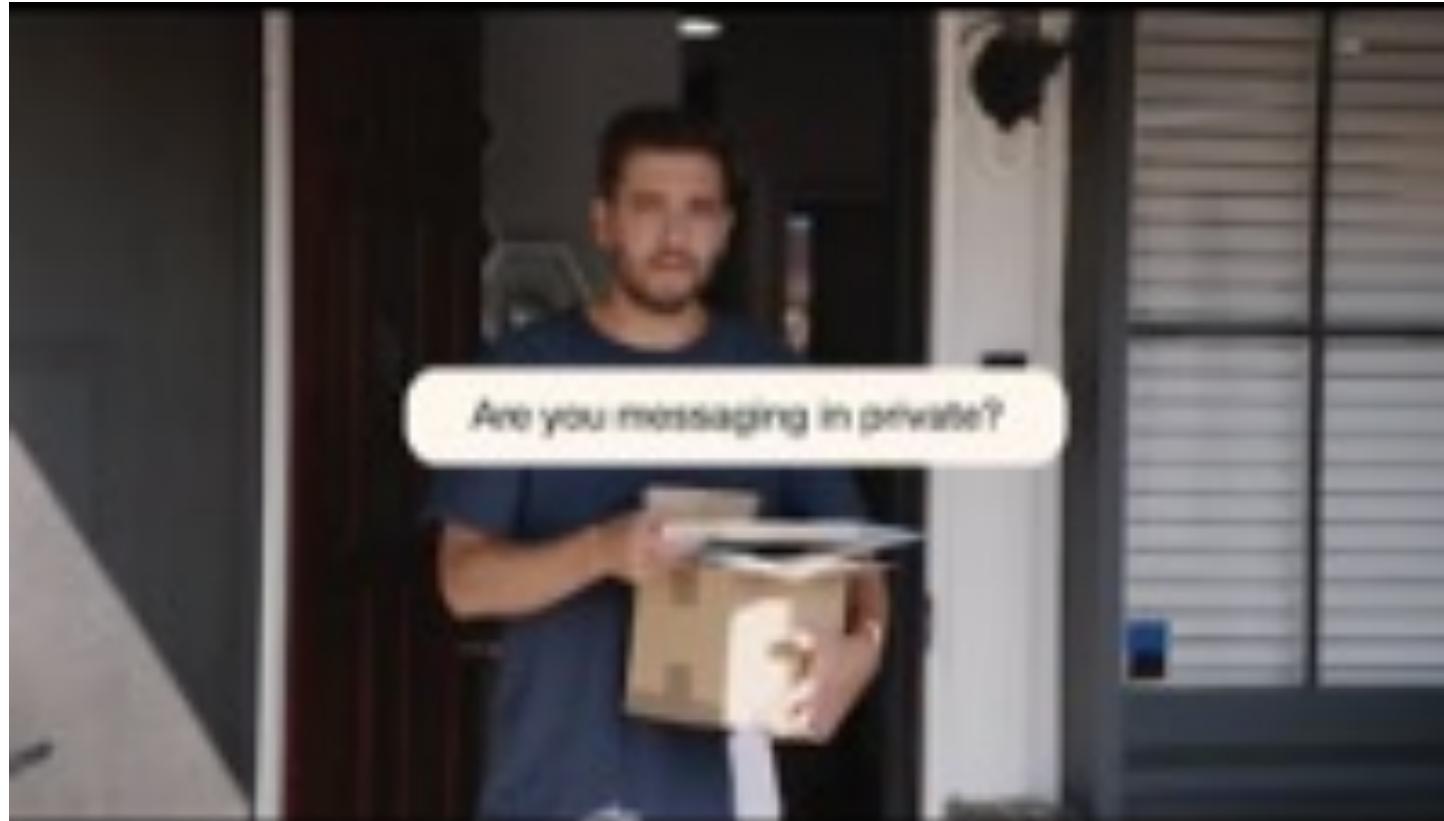
- Why do we need trusted network and transport layer protections to connect devices?
- Shouldn't the **messages** be protected too/instead?
- This is **object-security**, it is different and more powerful

# WHAT IS “OBJECT-SECURITY?”

- Well, first, what is a digital “object,” on the Internet?
  - It could be        ...  
an image    a file    a message    an email    sensor reading
- The security/privacy we need for objects is different
  - “Objects” exist/persist “at rest,” i.e. beyond “in flight”
  - Example: I create a document, send it over WhatsApp to a friend, and then email it to a colleague
  - If the WhatsApp msg is encrypted, does that protect the doc at rest on my computer, or over email?
- Securing objects will unlock protections for mHealth, V2X, Smart Cities, and more
- In this talk, we propose tomorrow’s object-security foundation should be built from the Internet’s core, upward
- But, the Internet doesn’t have a built-in way to do that today (i.e., an architecture)
  - Why can’t we encrypt objects to anyone or authenticate signed objects, regardless of where they’re from except by using a platform (e.g., WhatsApp, Signal, etc.)?
- But, first we might ask...

## SECURE/PRIVATE COMMUNICATIONS ON THE INTERNET, TODAY

- Are our communications and data private on the Internet?
- Well, maybe you've heard, no:



**And so are your EMAILS!**

## TAKE AWAY FROM THAT...

- What did we see there (besides a mixed metaphor of mail vs. messaging)?
  - Privacy: People expect that even snail-mail, in meat-space, is private
- What did we **not** see there?
  - Authenticity: no one expected to verify the of **sources** of mail
  - Cybersecurity and privacy on the Internet should be **more** advanced and automated than in meat-space
    - Drones & automobiles should be able to transact with each other
    - Doctors should be able to send health records to patients
    - ...
  - The Internet should enable this, but fundamental requirements have **not** been met

## THE FOUNDATION MUST SUIT ITS PURPOSE

- To know what Internet-scale object-security *needs to be*, we need to *evaluate why* object-security is doesn't yet exist
- So, “why?” We’ve had mature crypto protections for *years*: S/MIME, PGP, etc.
  - These are so “mature,” they ought to be in *nursing homes* by now!

What we already know:

our protections have been stymied by a simple limitation:

Our software can’t securely (inter-admin) learn the crypto keys

What we *still* need to know:

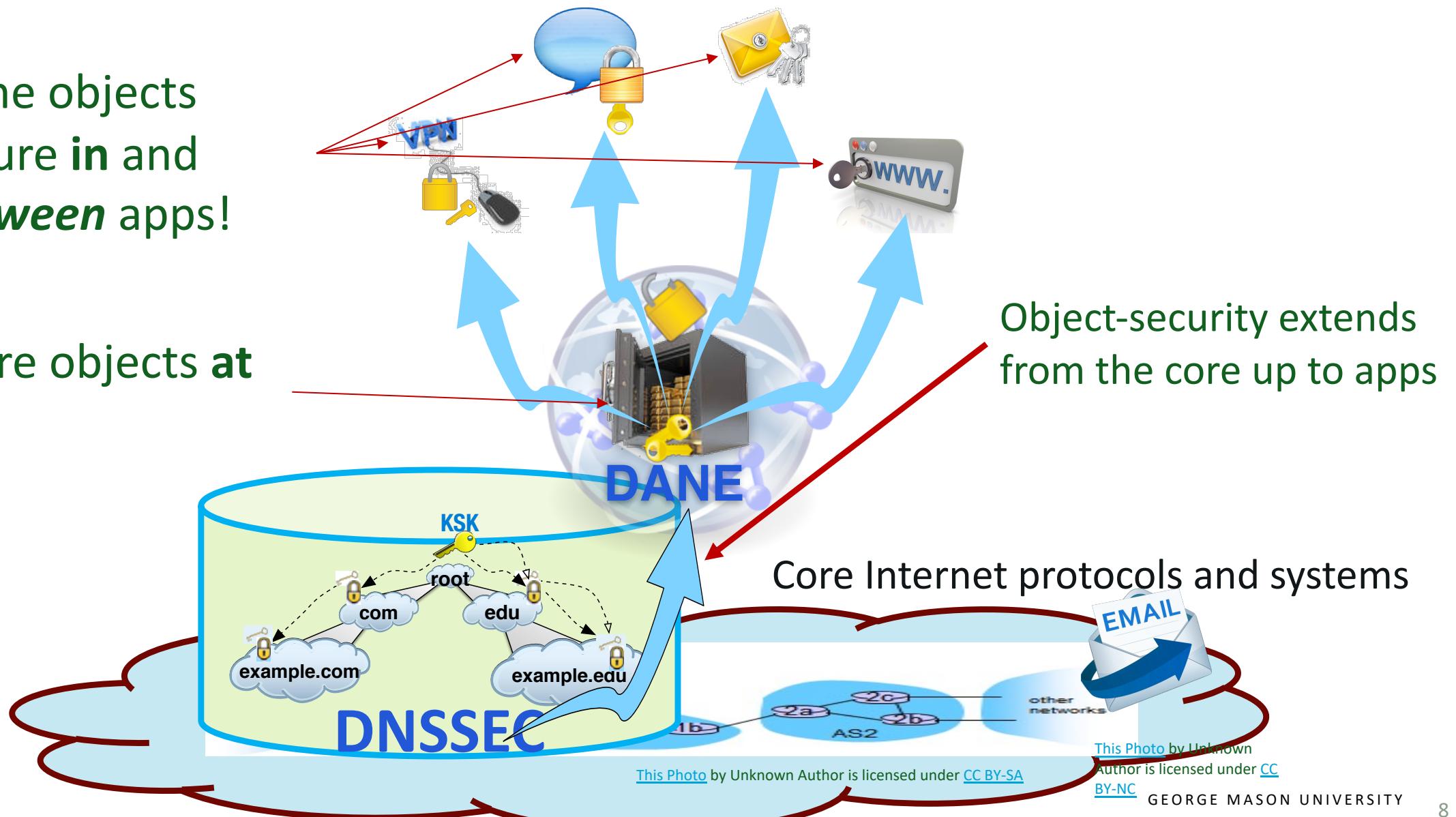
To be sure foundation will bear the Internet’s weight, need to understand and evaluate what are the *fundamental* needs + obstacles

- Examples like IoT, mHealth, V2X, etc. show increasingly repeated requirements:
  - Inter-organizational (e.g., entity at University A to entity at company B)
  - Per-entity (e.g., device, user, etc.) E2E crypto at Internet-scale
  - Usable tools
  - Automation
- The foundations we need already operational in Internet's core
- The Domain Name System's Security Extensions (DNSSEC)
  - 16+ years,  $\sim 10^7$  global zones, inter-org loosely-federated, etc.
- DNS-based Authentication of Named Entities (DANE)
  - General object-security, ~10 years, per-entity crypto, etc.

## “CORE TO TABLE” CYBERSECURITY: RESOURCE CERTIFICATION

Same objects  
secure **in** and  
*between* apps!

Secure objects **at**  
rest!



## FOR EXAMPLE: SENDING MESSAGE OBJECTS

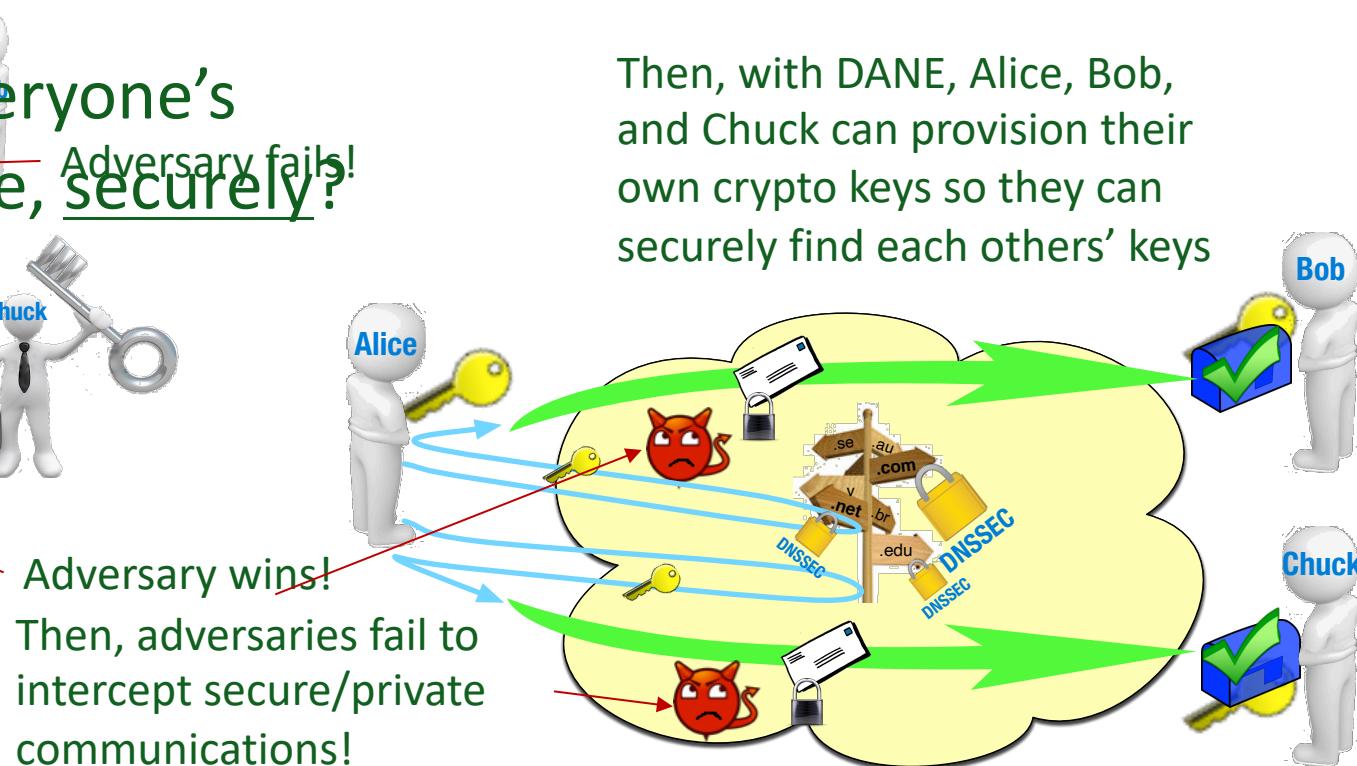


If Alice, from Example U., can get Bob's key, from Company B, she can transact with him at will!

If Alice, Bob, and Chuck can securely find each others' crypto keys, they can all communicate securely/privately!



But, even if Chuck has a key, Alice cannot securely/privately communicate with him!



But, how?!?

## INTRODUCING KURER AND DANEPORTAL.NET!

- To do that, we have built a *live* experimental apparatus: secure email
- Securing email will vault cybersecurity forward, but more than that it will prove the utility of the underlying architecture
  - An email add-on called **Kurer** and a management portal at **DANEportal.net**
- These will let us *evaluate the fundamental* needs of Internet-scale security and privacy of *digital objects* (e.g., messages, files, etc.), at scale

# INTERNET-SCALE OBJECT SECURITY REQUIREMENTS

- Recall our fundamental requirements (messaging platform, aside):

- Inter-organization key learning



S/MIME with DANE

- Per-user crypto key enrollment



DANEportal.net

- Human-usable tools for e2e protections



Kurer MUA plugins

- Framework to enable security-automation

NEXT UP

Invisible Security

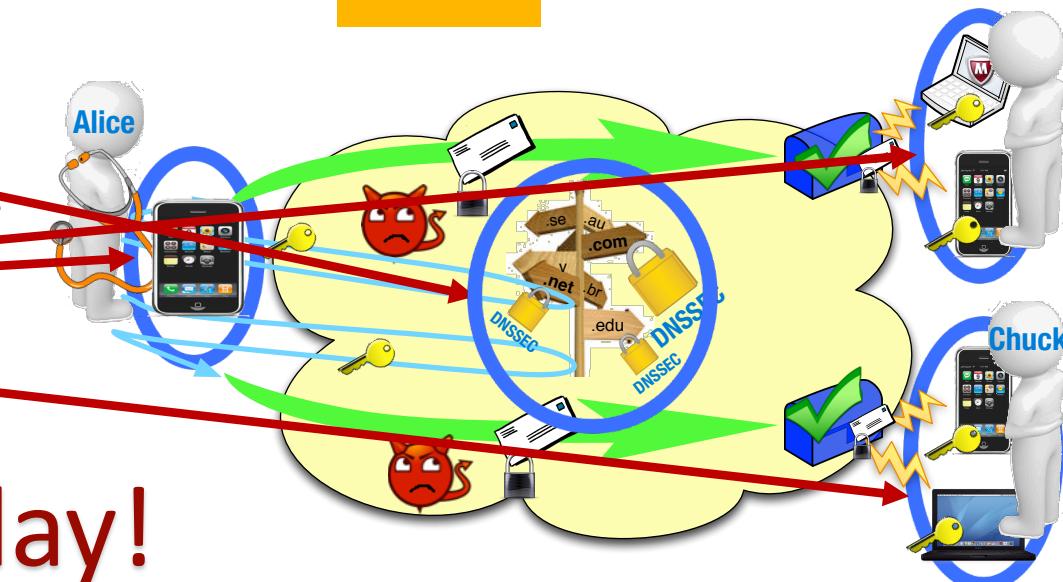
- DANEportal.net

- Management of users' DANE keys

- Kurer

- User-side DANE software

Tools you can use, today!



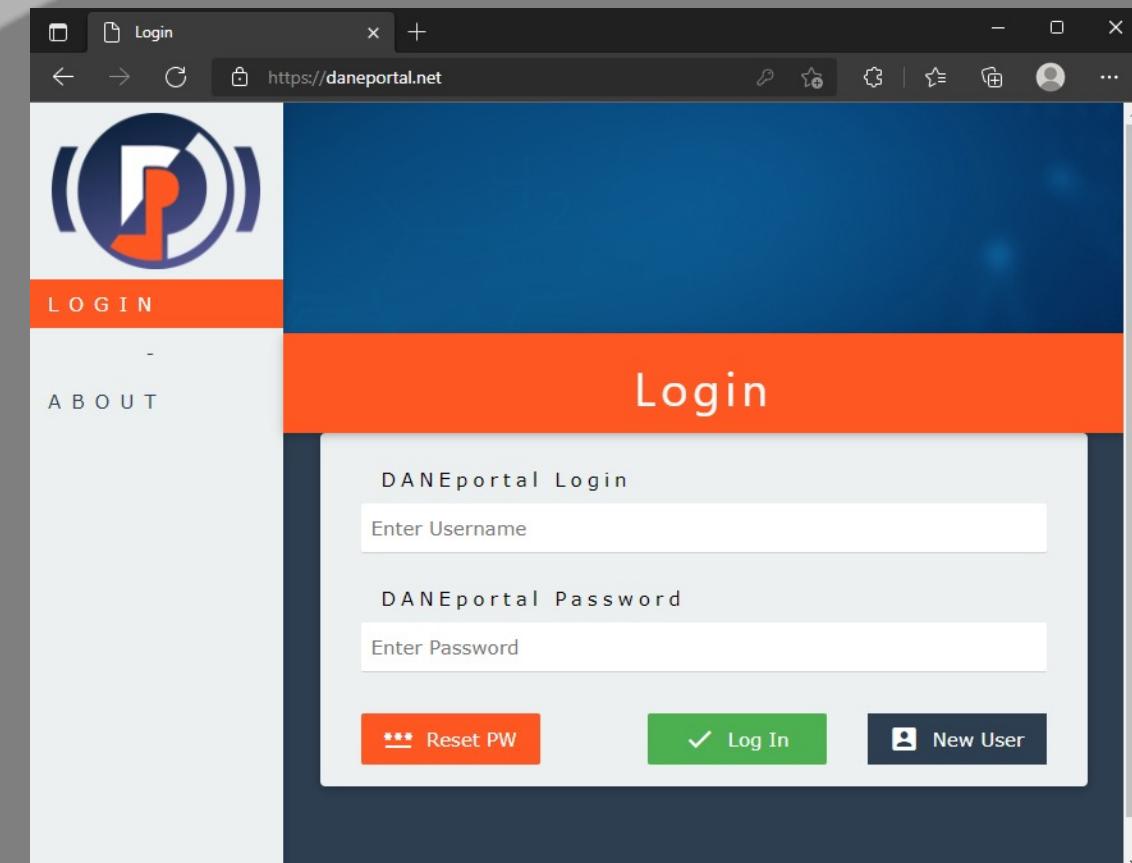
## WHAT ARE DANEPORTAL.NET AND KURER?

- DANEportal.net is where email users from any domain (“identity holders”) can securely make their crypto keys *learnable*
  - Domain holders securely claim their zone (using ACME protocol)
  - DANE is managed for them
  - Email users, under a domain, create accounts and manage their own key life-cycles
- <http://daneportal.net/>
- Kurer is an add-on/plugin for Mail User Agents (MUAs, Outlook and Thunderbird)
  - Email users install Kurer
  - Configure their crypto keys
  - And go secure... To anyone, anywhere, anytime
- Observation: secure email builds from core Internet security up to users
  - Ideally positioned to extend further... more later





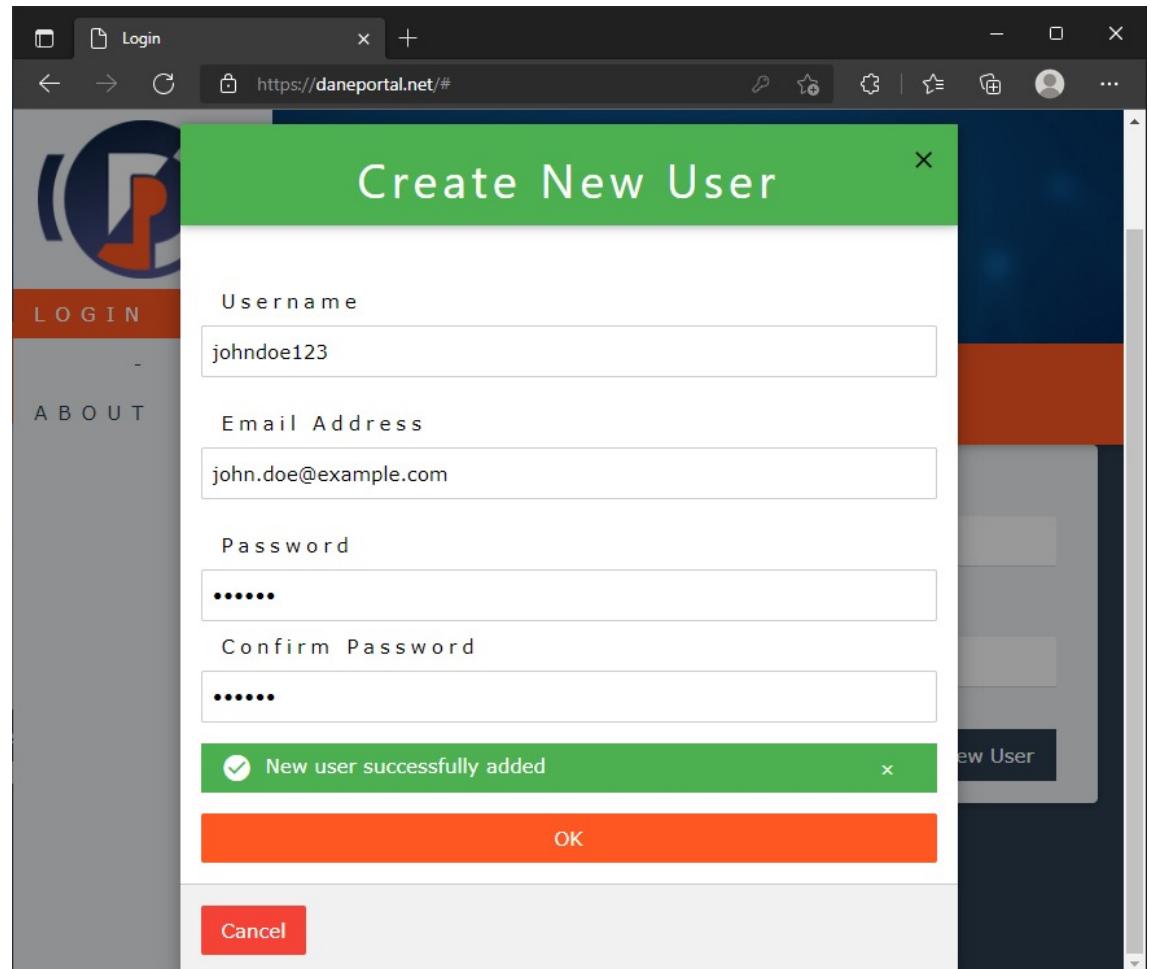
**HTTPS://DANEPORTAL.NET/**  
OVERVIEW, FULL GUIDE AVAILABLE ONLINE...



# CREATE YOURSELF A USER ACCOUNT



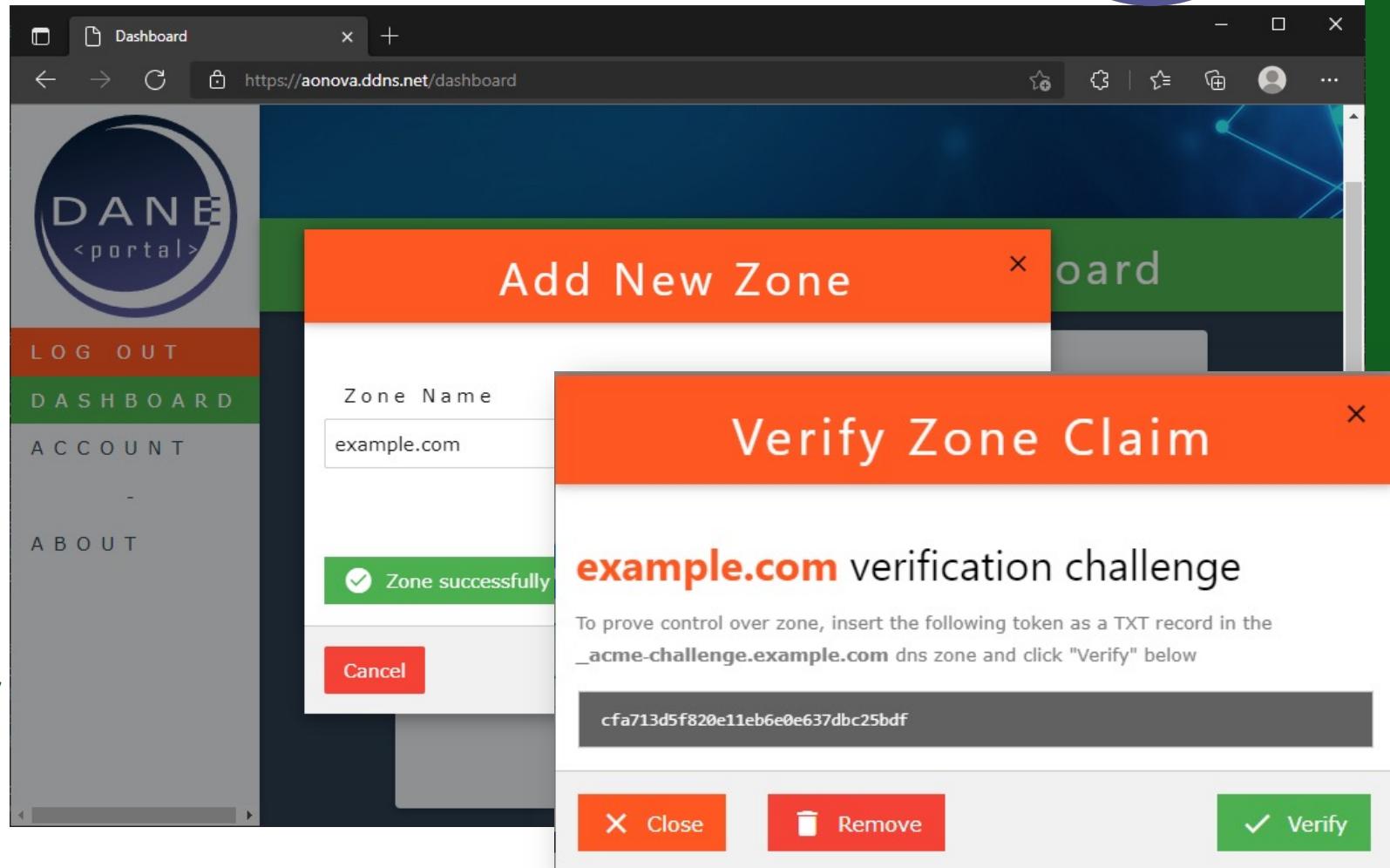
- Click [ New User ]
  - Enter desired credentials
  - Click [ Create User ]
  - Click [ OK ] to close modal
- 
- This will be your portal/management account
  - Every email user will need their own login
    - Third-party OAuth logins are a planned feature, as is automated bulk account creation



## ADD YOUR OWN ZONE



- Enter the *Fully Qualified Domain Name* of your zone
- Click [ Submit ] to add the zone *on a claimed basis*
- Click [ Return ] to close the modal and see the newly added zone claim
- Use ACME protocol to verify administration of zone



# DELEGATE FROM DANEPORAL TO YOUR ZONE

- To serve, complete the delegation of the DANE zone.
- This involves adding two records (NS and DS) to your zone using your zone management tools.
  - Both can be found on the page we are looking at
- Specifics differ by registrar / MDNS interface
  - The following pictures are just for reference

The screenshot shows a web browser window displaying the Daneportal.net interface for managing a zone. The title bar says "Zone" and the URL is "https://daneportal.net/zone?id=182". The main content area is titled "aonova.net - s/mime zone" with a status of "Active". It shows "delegation records" which include an "ns record" and a "ds record". A red arrow points from the text "Both can be found on the page we are looking at" to the "ns record" section. Another red arrow points from the text "The following pictures are just for reference" to the "ds record" section. To the right of the "ns record" is a large circular logo with a stylized "D" and "P". Below the delegation records is a "template" section with baseline records. At the bottom, there is a table showing two entries:

Host name	Type	TTL	Data
_smimecert.aonova.net	DS	1 hour	27730 13 2 f51cb0967533b6916c1a3a4ee1e916a3a560b8ec5ac5e3987239e1b729c82a06
_smimecert.aonova.net	NS	1 hour	dane-dns.care.gmu.edu.

At the bottom left is a "Google Domains" logo.

## NOW, ADD EMAIL ADDRESSES/USERS

- Denizen Users email addresses under a zone, administered separately
- In the context of DANE S/MIME, the denizens are your email users
  - DANEPortal allows them to add their S/MIME records to your DANE zone without you losing any of your control as zone admin
- Click [ Add domain ] to open the form

The screenshot illustrates the DANEPortal interface for managing email addresses and S/MIME records.

**Zone aonova.net**

**domains**

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

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

**s/mime zone - new denizen domain**

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

john doe123

Domain Name (only local part)

minar

DANEPortal Username

S/MIME

Domain Protocol

Cancel

**DASHBOARD**

**dane-enabled email addresses**

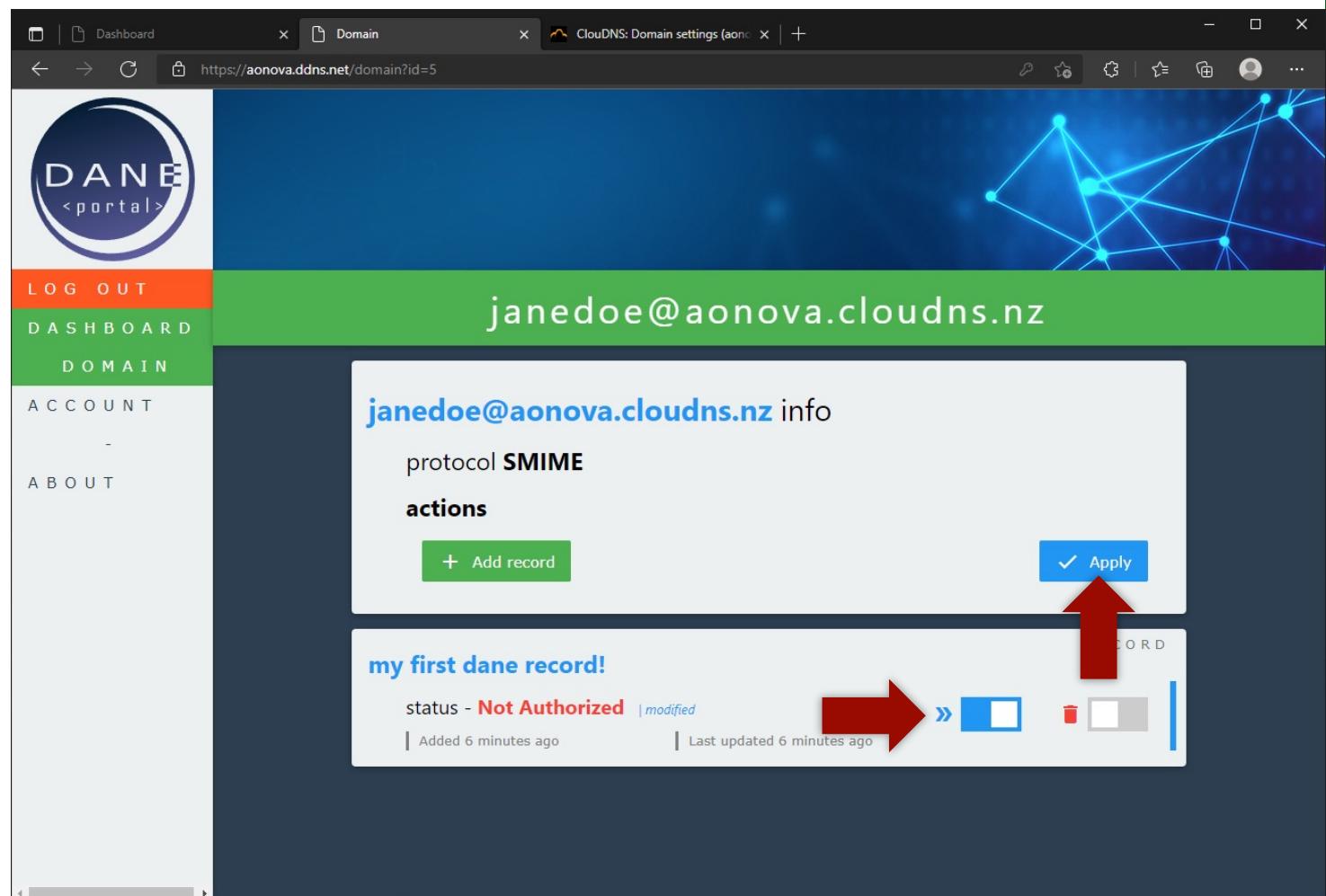
These are your email addresses which were added by **zone admins**. Click one to manage its **public crypto keys**.

email	protocol	# of records
minar@osterweil.net	SMIME	0/0
minar@aonova.net	SMIME	1/1
john doe123@aonova.net	SMIME	0/0

## NOW, ADD EMAIL ADDRESSES/USERS



- You should now see a **card** representing the record you just added
- Manage records by toggling its **authorization state** or **deleting** it permanently
- For now, toggle the **authorize** switch to the right and click **[Apply]**



# EMAIL USERS CAN MANAGE THEIR OWN CERTIFICATES



Add new cert to johndoe123@aonova.net

Upload certificate file

No file chosen

[? Make a new cert](#)

my first cert!

Nickname to remember this by (optional)

Domain-issued certificate (DANE-EE)

Usage

Full certificate (Cert)

Selector

No hash used (Full)

Matching

Both (default)

Signing or encrypting

- For now, toggle the **authorize** switch to the right and click

my first cert!

status - **not authorized**

Added just now  
Last updated just now

SMIME CERT

»

Signatures and Encryption

## 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

organization (e.g. company name)  
Example Corp.

org unit (e.g. section / department name)  
Example Section

common name (e.g. your name)  
John Doe

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

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

Private key  
Install this in your mail app for signing/decrypting



KURER: SECURE EMAIL FOR EVERYONE!

## KURER FOR THUNDERBIRD

No-click solution for seamless DANE S/MIME

<https://github.com/gmu-msl/kurer-thunderbird>

Only one setting is really needed for now:

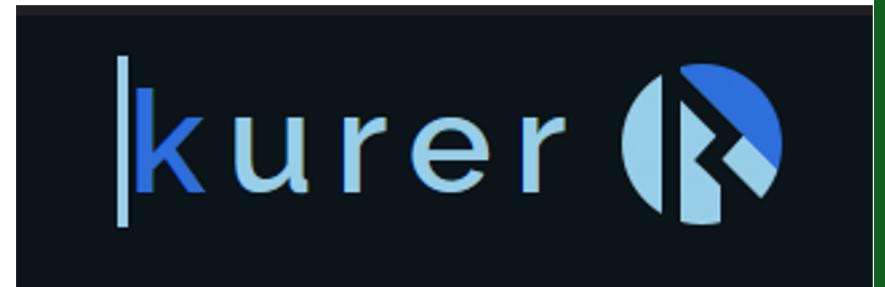
- Enter your private key and sending email address to allow signing your email

The screenshot shows the Mozilla Thunderbird Add-ons Manager window. On the left, a sidebar lists various options like New, Attachments, Edit, Find, Print..., Save As, Empty Trash, Add-ons and Themes, Account Settings, Preferences, File, View, Go, Message, and Tools. A large green arrow points from the bottom-left towards the 'Options' tab of the Kurer add-on's details page. The Kurer add-on card itself has a blue header with the logo and name, followed by a description: 'S/MIME encrypted secure email functionality, powered by DNS-based Authentication of Named Entities (DANE)'. It includes tabs for Details, Options (which is selected), and Permissions. Below the card, it shows the Author as Aonova, Version 1.0, and Last Updated as October 18, 2021. The main content area is titled 'Composing messages' and contains several configuration options with toggle switches:

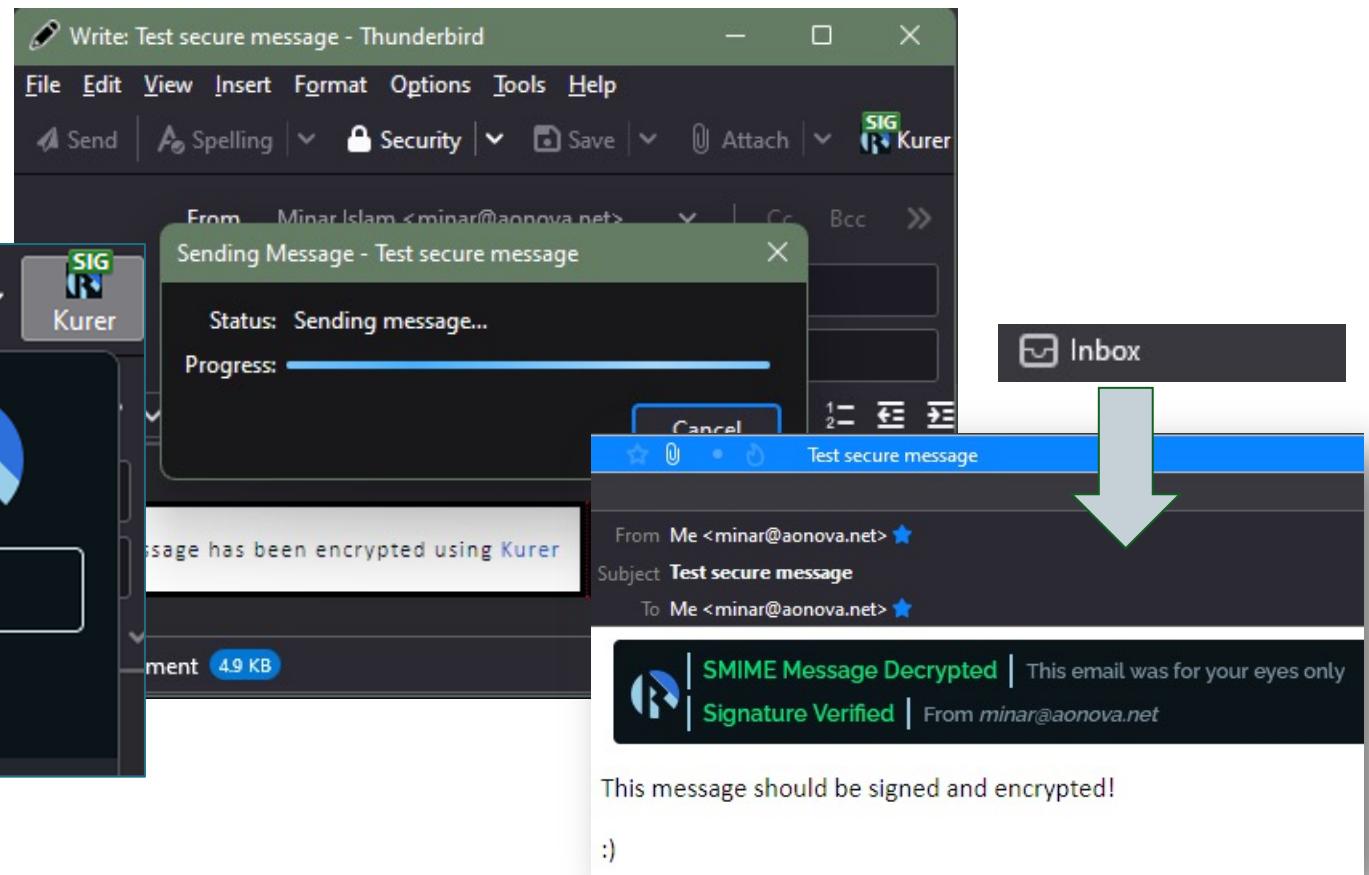
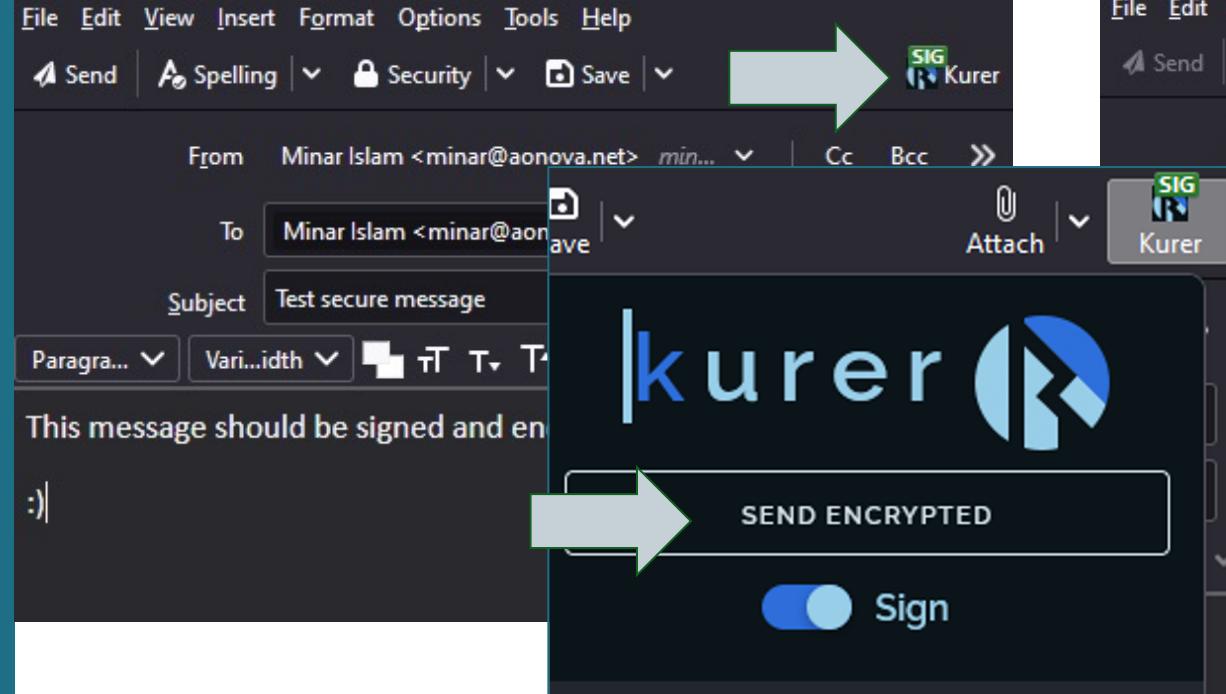
- Separate encrypt button (Always encrypt on send)
- Not signed by default (Signed by default)
- If unable to encrypt for a recipient:
  - Silently send unencrypted (Halt and show warning)
- When replying to an encrypted message:
  - Preserve encryption (Decrypt the reply quote)
- Private keys
  - Single key for sign/encr (Separate keys for sign/encr)
  - Key for decrypting and signing (Browse... No file selected. The last saved key is currently active. You can overwrite by selecting a new key)

A second green arrow points from the bottom-right towards the 'Browse...' button for selecting a private key.

JUMP RIGHT IN TO SENDING SECURE EMAIL

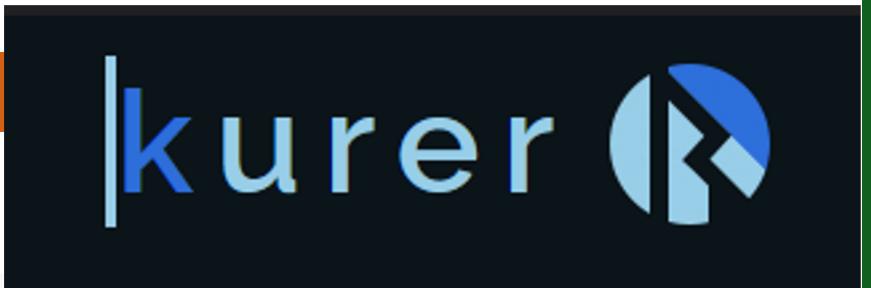


- Use the Kurer popup to toggle signing and click send encrypted
  - The SIG tag on the icon means the email will be signed when sending



# GETTING KURER ON OUTLOOK IS A SNAP!

Full install directions: <https://kurer.daneportal.net/install>

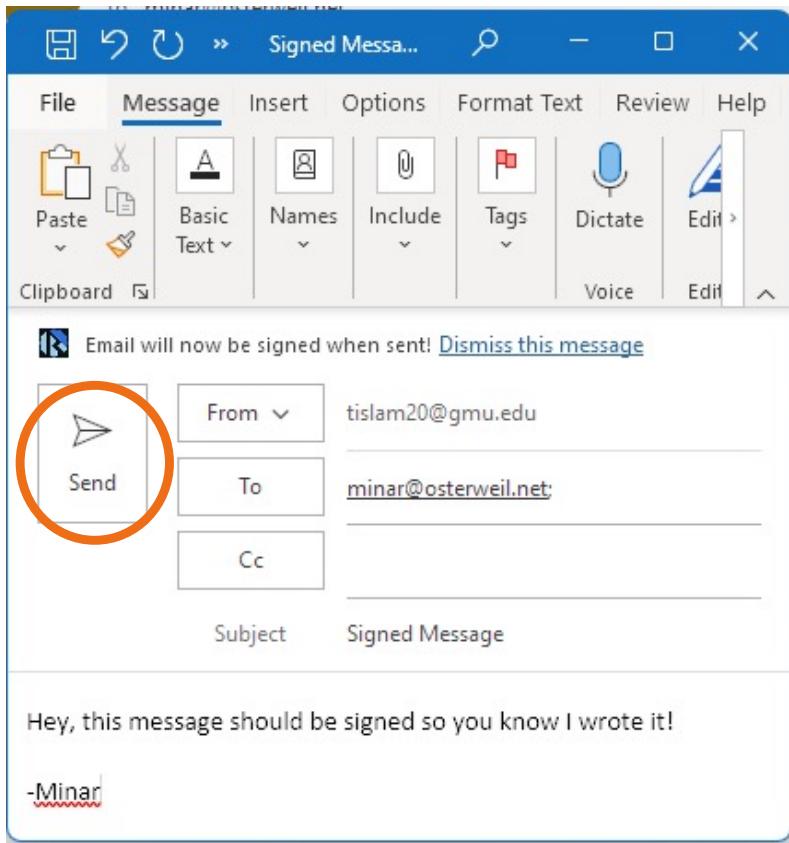


The screenshot shows the Microsoft Add-ins for Outlook interface. On the left, there's a sidebar with a "Get Add-ins" button. A large red arrow points from this button to the "My add-ins" section in the main pane. Below this, the text "My add-ins" is written in green. In the main pane, under "ADD-INS FOR OUTLOOK", there's a heading "All" and a sub-section "Admin-managed". Several add-ins are listed:

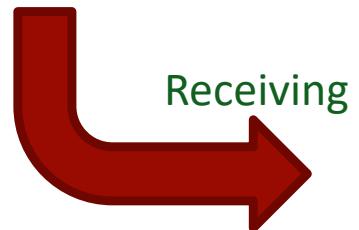
- Unsubscribe**: Admin-managed, Added
- Suggested Meetings**: Admin-managed, Added
- My Templates**: Admin-managed, Added
- Bing Maps**: Admin-managed, Added
- Action Items**: Admin-managed, Added

At the bottom, there's a section titled "Custom Addins" with the text "You can install add-ins from a file or from a URL." It shows "No add-ins found." and features a button labeled "+ Add a custom add-in ▾". A red arrow points from the text "Add a custom add-in from URL:" to this button. A large orange oval highlights the "Add from URL..." option in a dropdown menu that appears when the button is clicked.

Add a custom add-in  
from URL:



Sending



Receiving

Signed me

MI Minar  
To: minar@osterweil.net

dane-smime.kurer  
51 KB

Hey, this message should be signed so you know I wrote it!  
-Minar

This message has been signed using Kurer

S/MIME message detected

kurer

| This email wasn't encrypted | This email was signed

Plaintext:

Hey, this message should be signed so you know I wrote it!  
-Minar



- Automatically detect if incoming emails are encrypted or signed
- Simply click the text to automatically decrypt the email and view the plaintext
  - New reply buttons with additional functionality

Signed message



Hey, this message should be signed so you know I wrote it!

-Minar

This message has been signed using Kurer



Plaintext:

Hey, this message should be signed so you know I wrote it!

-Minar

## STATUS

- DANEportal.net is live, today

<http://daneportal.net/>

- Kurer is entering *alpha release*, for Outlook and Thunderbird

<https://kurer.daneportal.net/install>

## DISCUSSION

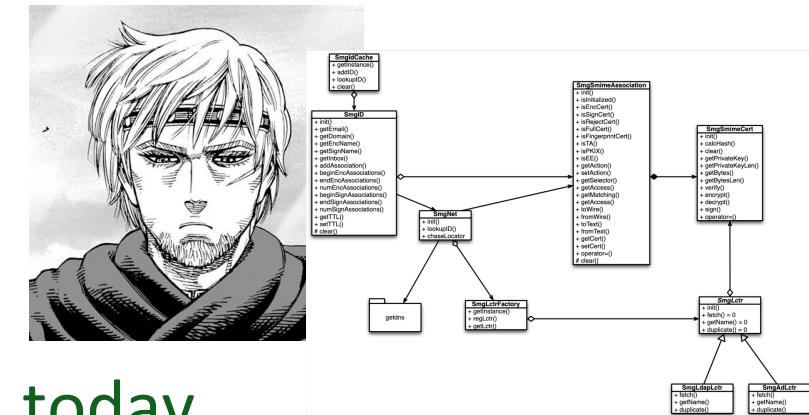
- Why not build cybersecurity / privacy protections from the top down?
  - Secure messaging works, right?
  - Why not build on blockchain?
  - Why not something else that fills a need?
- Internet needs an architecture for *cross-app* object-security
- Internet continuously proves things that “work” may not work *at scale*
- Internet’s needs *evolve*, and protections need to be *(re)evaluated*
- Building on Internet’s scalable core (protections) inherits versatility
  - DNSSEC has embodied scalable/usable protections for 16+ years
  - Email is inter-org, has been scalable/evolvable core protocol for decades, etc.
- S/MIME + DANE → scalable messaging and object security

# PLAY WITH DANE AND ITS TOOLS

- DANE has been used in CTF at M3AAWG
    - <https://www.m3aawg.org/>



- libCanute: a reference library for DANE protocols
    - <https://github.com/gmu-msl/canute>
  - DANEPortal.net and Kurer will let you get started



## WATERSHED MOMENT: MAKING INTERNET PROTECTIONS BEFIT SETTING

- This technology will secure digital objects throughout cyberspace:
  - Mobile Healthcare (**mHealth**), Smart and Connected Communities (**SCC**), **5G** Internet of Things (**IoT**) security, Vehicle-to-Everything (**V2X**) communications, and much more.
- Just like email, those disciplines will *also* need
  - Inter-organizational foundations
  - Per-user E2E crypto, Internet-scale
  - Human-usable tools
- Securing email with DANE paves the way to evolve protections from the Internet's core
  - This work will *evaluate* in order to *evolve* protections that fit
  - Deployable *immediately*
- Next: architecture for Security, Privacy and Trust Enrollment (SPaTE) at the Internet's scale, and beyond

THANK YOU!

The background features a complex geometric pattern composed of black and yellow lines. It includes several thick, diagonal yellow lines sloping upwards from left to right, and a grid of black lines forming a perspective-like structure that recedes towards the bottom right. A large, solid black triangle is positioned in the upper right quadrant.

ARE YOU INTERESTED IN DOING  
SOME RESEARCH WITH US???

EMAIL ME:  
[EOSTER@GMU.EDU](mailto:EOSTER@GMU.EDU)

BACKUP

