



USING DANE AS THE FIRST STEPS TOWARDS GENERALIZABLE INTERNET-SCALE OBJECT-SECURITY: SECURE MESSAGING FOR TODAY AND TOMORROW

Minar Islam - tislam20@gmu.edu

Josh Yuen - jyuen2@gmu.edu

Pavan Kumar Dinesh - pdinesh@gmu.edu

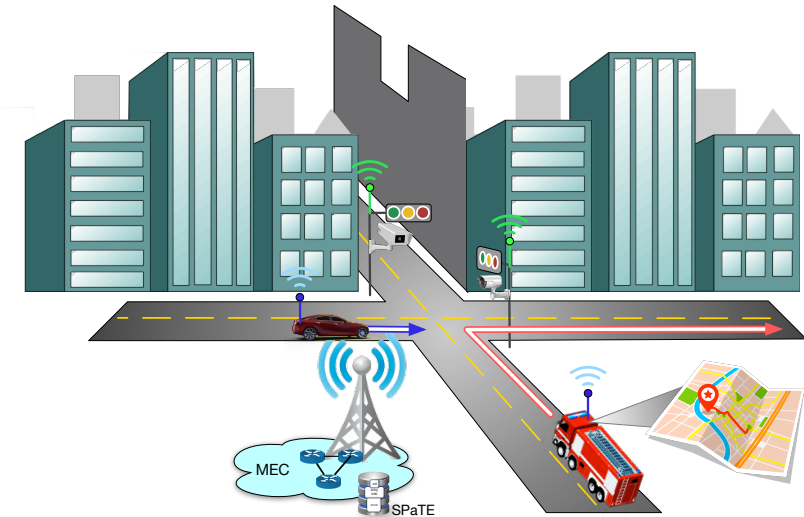
Tomofumi Okubo - tomofumi.okubo@digicert.com

Eric Osterweil - eoster@gmu.edu

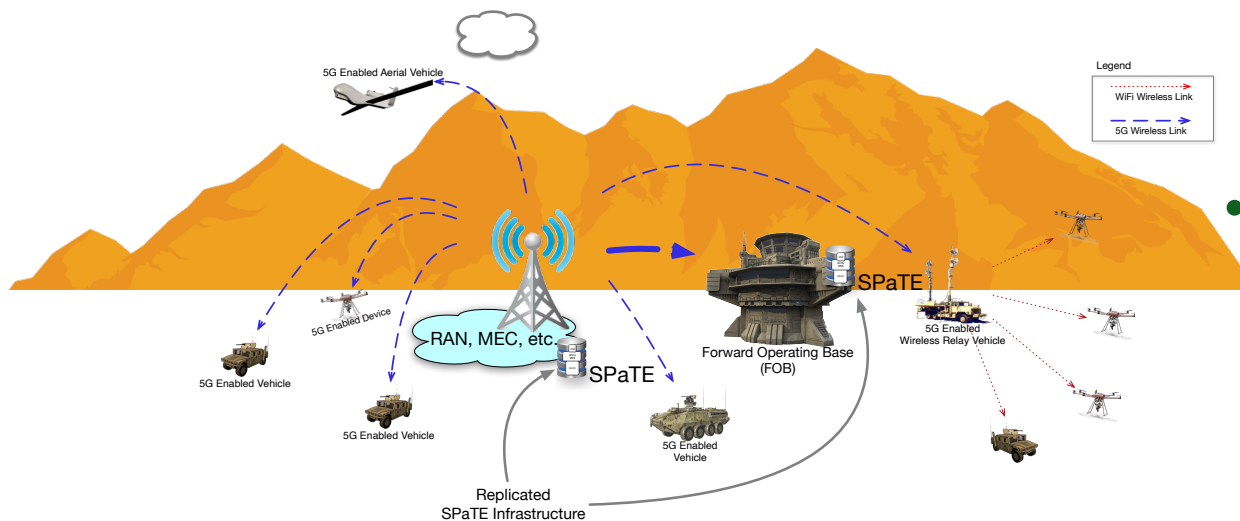


WHAT IS MOTIVATING OUR RESEARCH?

- Should we protect data in flight, at rest, or both?
 - Shouldn't, actions be taken based on data, not (just) who transmits it?
- Can independent devices/entities auth. and encr. their *messages* to each other with 0-trust?
 - Say, a fire engine to a municipal traffic signal, and that signal to my POV Tesla?



- Transport-layer protections do not protect data
 - Shouldn't the *messages* be protected too/instead?
- That is *object-security*, and it is different (and maybe more powerful) than transport-security



WHAT IS “OBJECT-SECURITY?”

- Well, first, what is a digital “object,” on the Internet?

- It could be



- 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?

- But, the Internet doesn’t have a built-in way to do that today (i.e., an architecture)

- Why can’t we encrypt/authenticate objects to anyone, except through WhatsApp, Signal, etc.?

WHAT IS “OBJECT-SECURITY?”

- In this talk, we propose that we already have tomorrow’s object-security foundation from the Internet’s core, and it’s time to build on it!

DANE

- An Internet-scale object-security **foundation** will unlock protections for mHealth, V2X, Smart Cities, and more

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 at scale
- 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:

what are the *fundamental* needs + obstacles;

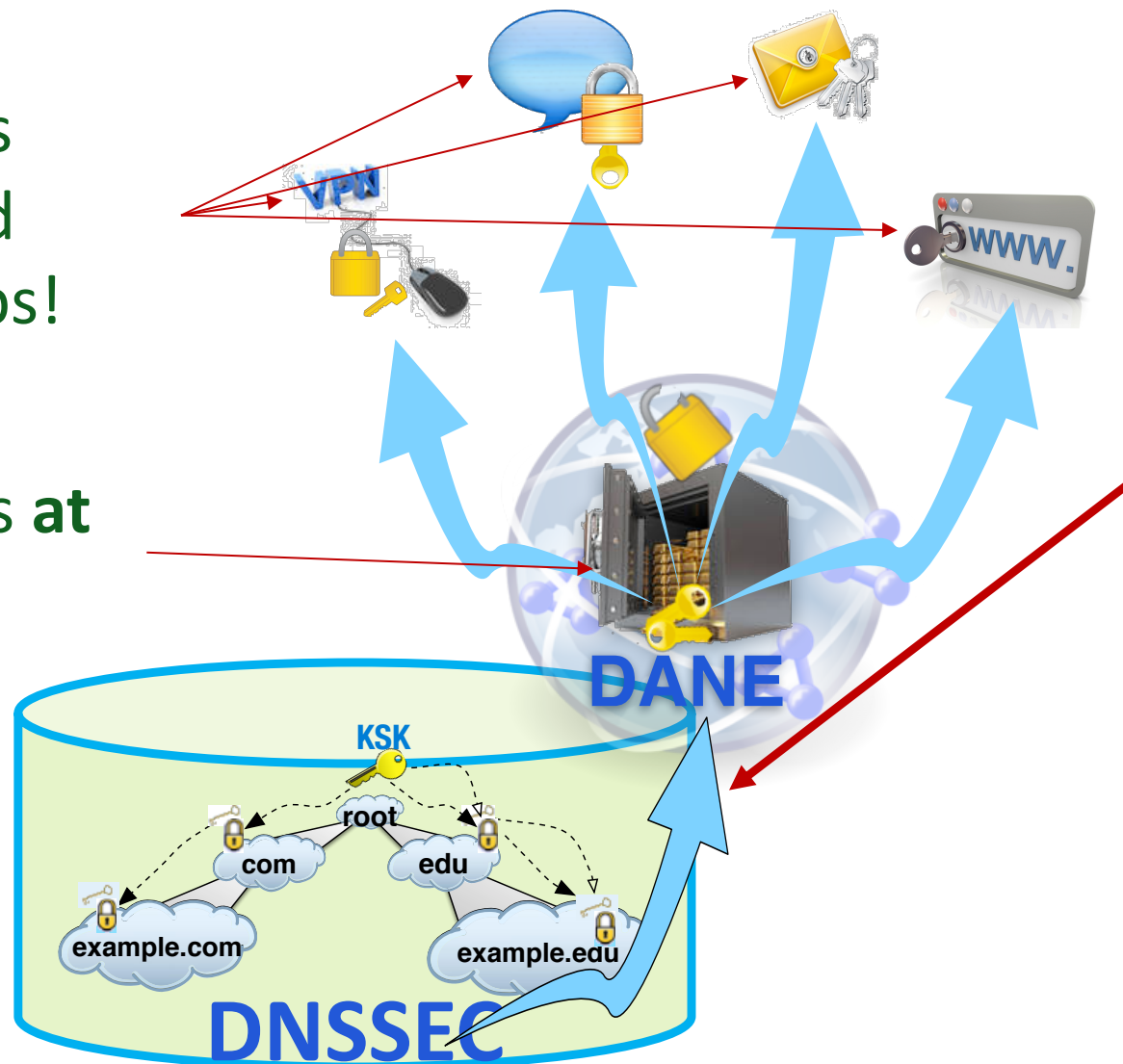
to be sure foundation will bear the Internet's weight

- 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
- An architecture should synthesize these

"CORE TO TABLE" CYBERSECURITY: RESOURCE CERTIFICATION

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

Secure objects **at
rest!**



Object-security extends
from the core up to apps

Core Internet protocol

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**
 - Object format for the Internet (using PKCS7)!
- 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

Entity-Security / “invisible security”

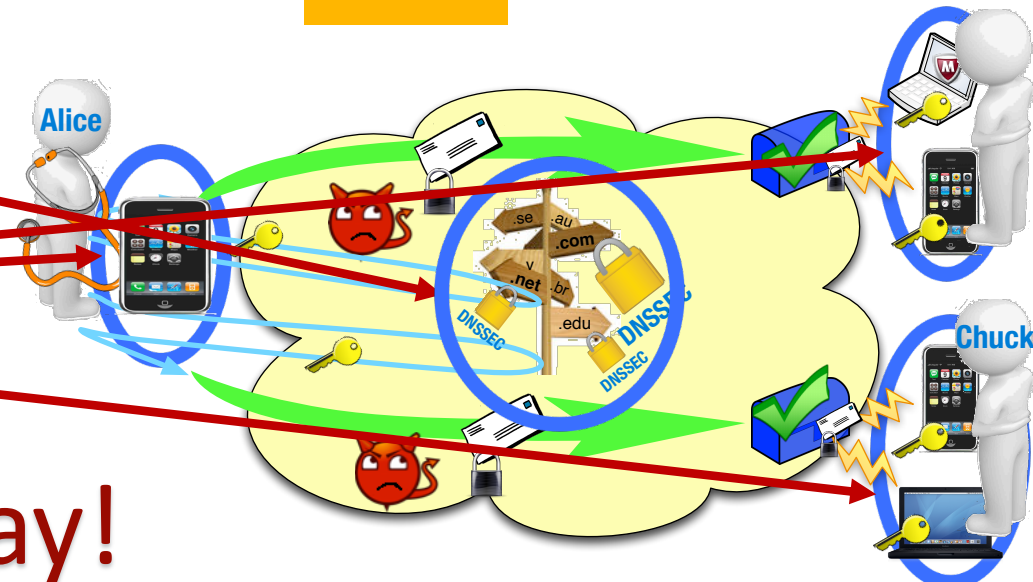
- DANEportal.net

- 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)

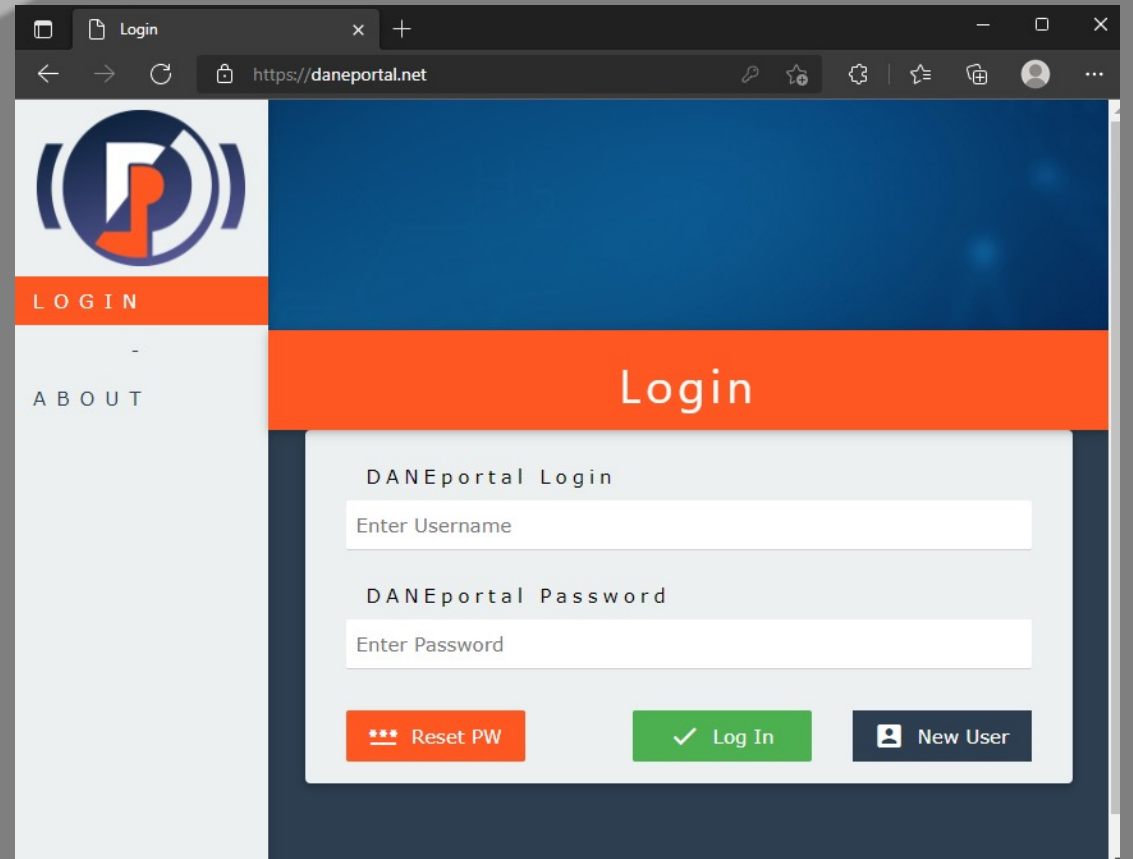
- Email users install Kurer
 - Configure their crypto keys
 - And go secure... To anyone, anywhere, anytime
- **Observation: secure email builds from core Internet security up to users**
 - Ideally positioned to extended further... more later





[HTTPS://DANEPORTAL.NET/](https://daneportal.net/)

OVERVIEW, FULL GUIDE AVAILABLE ONLINE...



ADD YOUR OWN ZONE



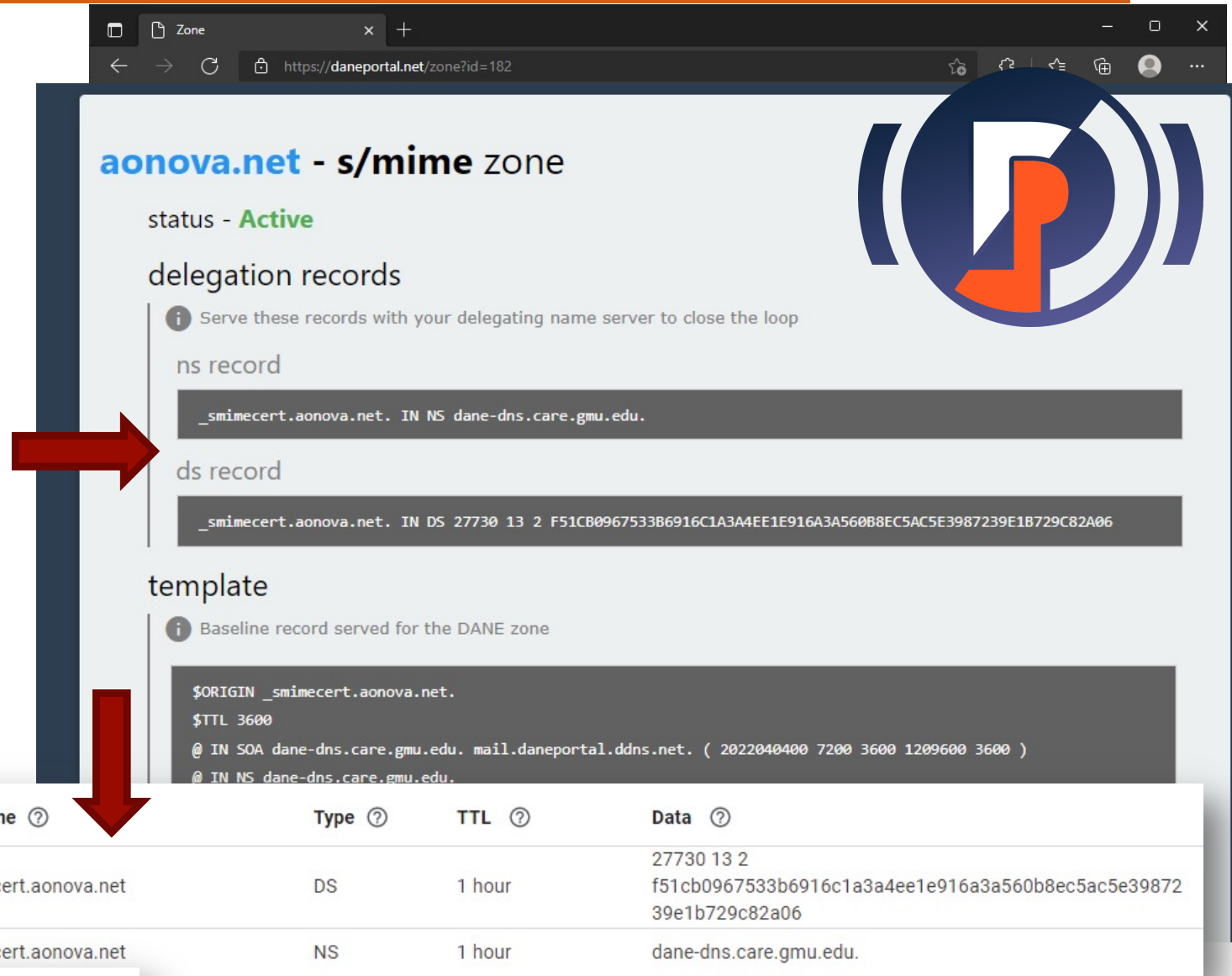
- Create a portal user account
- Add your zone
- Claim your zone using ACME protocol to verify proof of administration

The screenshot shows a web browser window at <https://aonova.ddns.net/dashboard>. The dashboard has a sidebar with the DANE <portal> logo and navigation links: LOG OUT, DASHBOARD, ACCOUNT, and ABOUT. Two modal windows are open:

- Add New Zone:** A form with the text "Zone Name" and the input field containing "example.com". Below the input is a green success message: "Zone successfully" with a checkmark icon. A red "Cancel" button is at the bottom.
- Verify Zone Claim:** A modal for "example.com verification challenge". It contains the text: "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 this is a text box containing the token: `cfa713d5f820e11eb6e0e637dbc25bdf`. At the bottom are three buttons: "Close" (orange), "Remove" (red), and "Verify" (green).

DELEGATE FROM YOUR ZONE TO DANEPORTAL

- Add NS and DS to your zone using your zone management tools
 - Zone cut at “_smimecert”



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

delegation records

ns record

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

ds record

```
_smimecert.aonova.net. IN DS 27730 13 2 F51CB0967533B6916C1A3A4EE1E916A3A560B8EC5AC5E3987239E1B729C82A06
```

template

Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022040400 7200 3600 1209600 3600 )  
@ IN NS dane-dns.care.gmu.edu.
```

| Host name | Type | TTL | Data |
|-----------------------|------|--------|--|
| _smimecert.aonova.net | DS | 1 hour | 27730 13 2 f51cb0967533b6916c1a3a4ee1e916a3a560b8ec5ac5e39872 39e1b729c82a06 |
| _smimecert.aonova.net | NS | 1 hour | dane-dns.care.gmu.edu. |

NOW, ADD USERS' EMAIL ADDRESSES

- Users create DANEportal accounts
- Zone admins authorize portal users as “denizens”
 - i.e., email addresses under a zone
- **Denizens** are your **email users**
 - Users add S/MIME records to **your** DANE zone
 - Admins do **not** lose any control

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

→ johndoe123
Domain Name (only local part)

minar
DANEportal User

S/MIME
Domain Protocol

Cancel

dane-enabled email addresses

These 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 |
| johndoe123@aonova.net | SMIME | 0/0 |

DASHBOARD →

EMAIL USERS CAN CREATE/MANAGE THEIR OWN CERTIFICATES



Add new cert to johndoe123@aonova.net

Upload certificate file

Choose 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

[Defaults](#) [Submit](#)

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

my first cert! SMIME CERT

status - **not authorized**

Added just now
Last updated just now

[»](#)

[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

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

US

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

Virginia

locality *(e.g. city name)*

Fairfax

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")

[↓ Get](#)

Private key

Install this in your mail app for
signing/decrypting

[↓ Get](#)

NOW, ADD EMAIL ADDRESSES/USERS



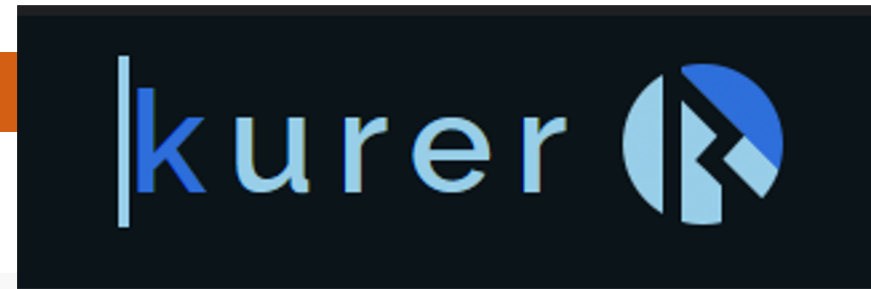
- Manage records by toggling its authorization state or deleting it permanently
- DANE allows “de-authorization” of keys
 - Not revocation, and faster
- For now, toggle the **authorize switch** to the right and click [Apply]

The screenshot shows a web browser window with the URL `https://aonova.ddns.net/domain?id=5`. The page header features the DANE <portal> logo and a user profile for `janedoe@aonova.cloudns.nz`. The main content area displays the configuration for a record with protocol **SMIME**. It includes an **actions** section with a green **+ Add record** button and a blue **✓ Apply** button. Below this, a record titled **my first dane record!** is shown with a status of **Not Authorized**. A red arrow points to the **Apply** button, and another red arrow points to the toggle switch for this record, which is currently in the 'Not Authorized' position.

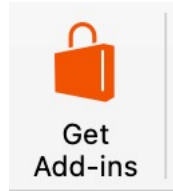


KURER: SECURE EMAIL FOR EVERYONE!

GETTING KURER ON OUTLOOK IS A SNAP!



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



My add-ins

ADD-INS FOR OUTLOOK

Add-ins may access personal information. By turning an add-in on, you agree to its License Terms and Privacy Policy.

Search add-ins

All

My add-ins

Admin-managed

Unsubscribe

This add-in is triggered by messages from subscription email feeds, and allows you to block the sender or

Admin-managed

✓ Added ...

Suggested Meetings

Shows meeting suggestions found in your email and allows you to add them to your calendar. This add-in will not

Admin-managed

✓ Added ...

My Templates

Admin-managed

✓ Added ...

Bing Maps

Map addresses found in your email. This add-in will send addresses to Bing but will not share your data with any

Admin-managed

✓ Added ...

Action Items

Shows Action Item suggestions from your email. This add-in will not share your data with any third-party service.

Admin-managed

✓ Added ...

Custom Addins

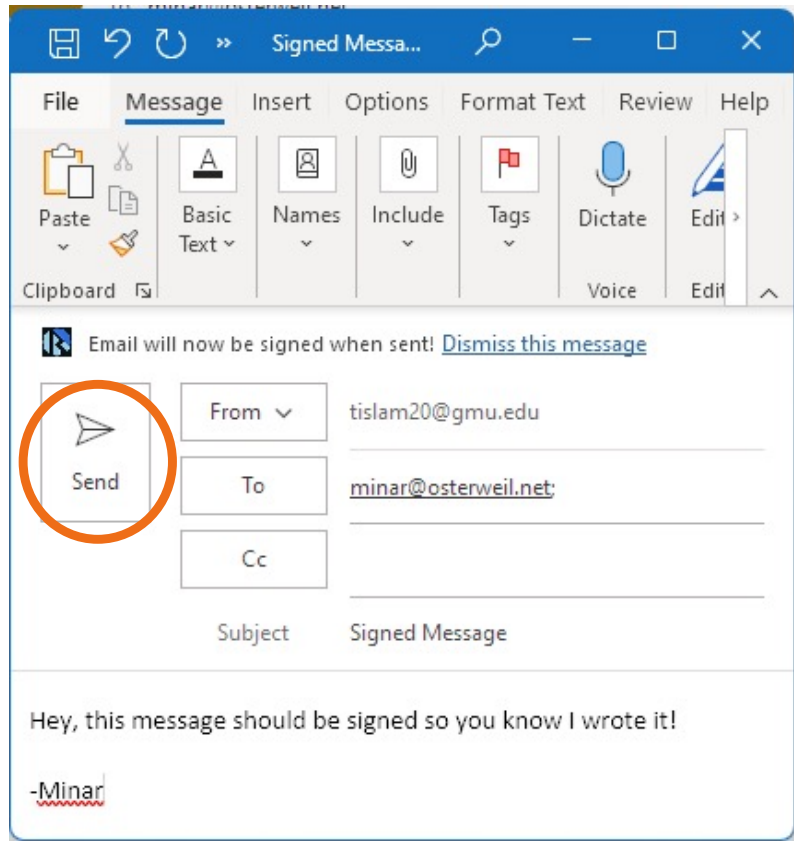
You can install add-ins from a file or from a URL. **+ Add a custom add-in** ▾

No add-ins found.

Add from URL...

Add from File...

Add a custom add-in from URL:

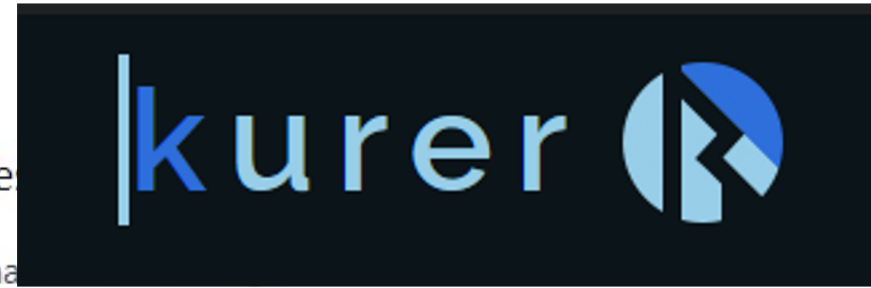


Sending



Receiving

Signed me



MI Mina
To minar@osterweil.net



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

-Minar





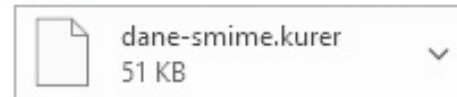
- Automatically detect if incoming emails are encrypted or signed
- Simply click the text to automatically decrypt the email and view the plaintext

- New reply buttons with additional functionality

Signed message



Minar Islam <minar@aonova.net>
To minar@osterweil.net



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

-Minar



S/MIME message detected

The Kurer logo is displayed at the top of the message preview window.

This email wasn't encrypted | This email was signed

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 in *alpha release*, for Outlook and Thunderbird

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

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: Entity-Security... Developing a tool for Security, Privacy and Trust Enrollment (SPaTE)

THANK YOU!

EOSTER@GMU.EDU

BACKUP



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* we 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

ARCHITECTURE FOR INTERNET OBJECT-SECURITY

- 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.

DISCUSSION

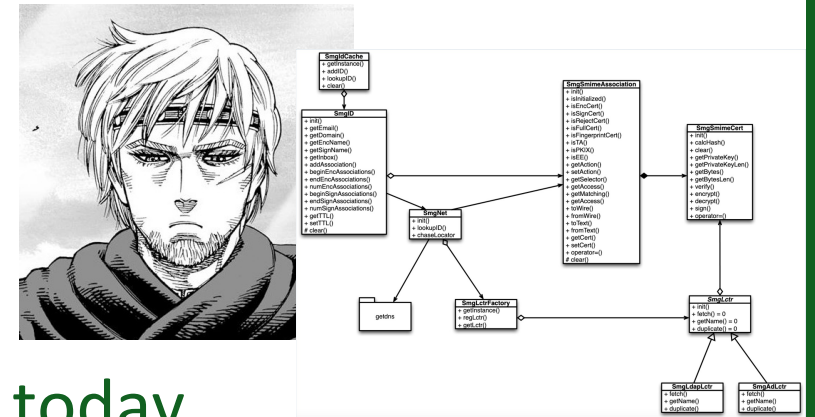
- Why not build cybersecurity / privacy protections from the top down?
 - Secure messaging works, right?
 - Why not build on blockchain?
 - Why not something else that fills a need?
- Internet needs an architecture for ***cross-app*** object-security
- Internet continuously proves things that “work” 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

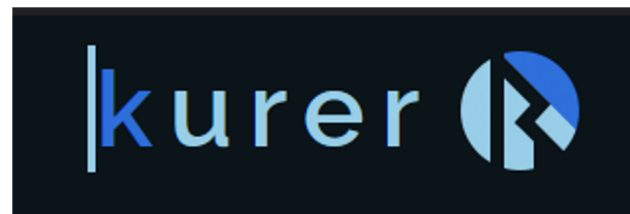
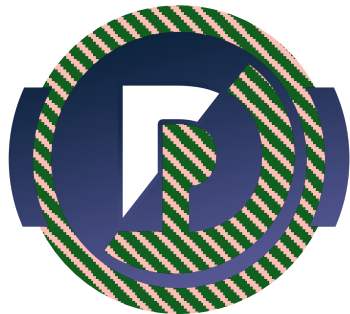
- DANE has been used in CTF at M3AAWG
 - <https://www.m3aawg.org/>



- libCanute: a reference library for DANE protocols
 - <https://github.com/gmu-msl/canute>



- DANEportal.net and Kurer will let you get started today



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!



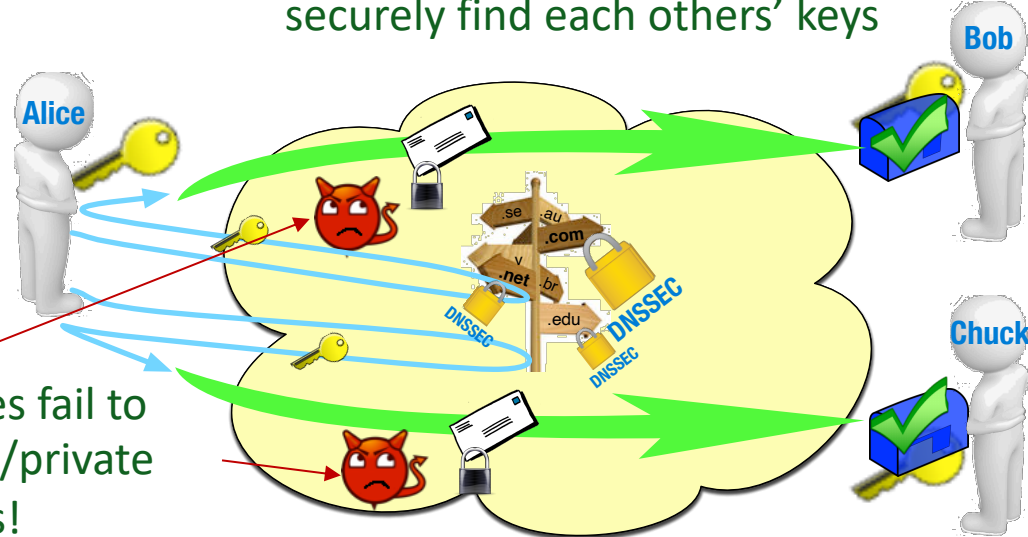
How can we make everyone's keys globally learnable, securely?

Adversary fails!

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

Adversary wins!
Then, adversaries fail to intercept secure/private communications!

Then, with DANE, Alice, Bob, and Chuck can provision their own crypto keys so they can securely find each others' keys



First step: secure DNS with DNSSEC

But, how?!?

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

A screenshot of a web browser showing a 'Create New User' modal form. The browser address bar shows 'https://daneportal.net/#'. The modal has a green header with the title 'Create New User' and a close button. Below the header are four input fields: 'Username' (containing 'johndoe123'), 'Email Address' (containing 'john.doe@example.com'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). A green success message 'New user successfully added' is displayed below the fields. At the bottom of the modal are two buttons: 'OK' (orange) and 'Cancel' (red). The background shows a navigation menu with 'LOGIN' and 'ABOUT' options.

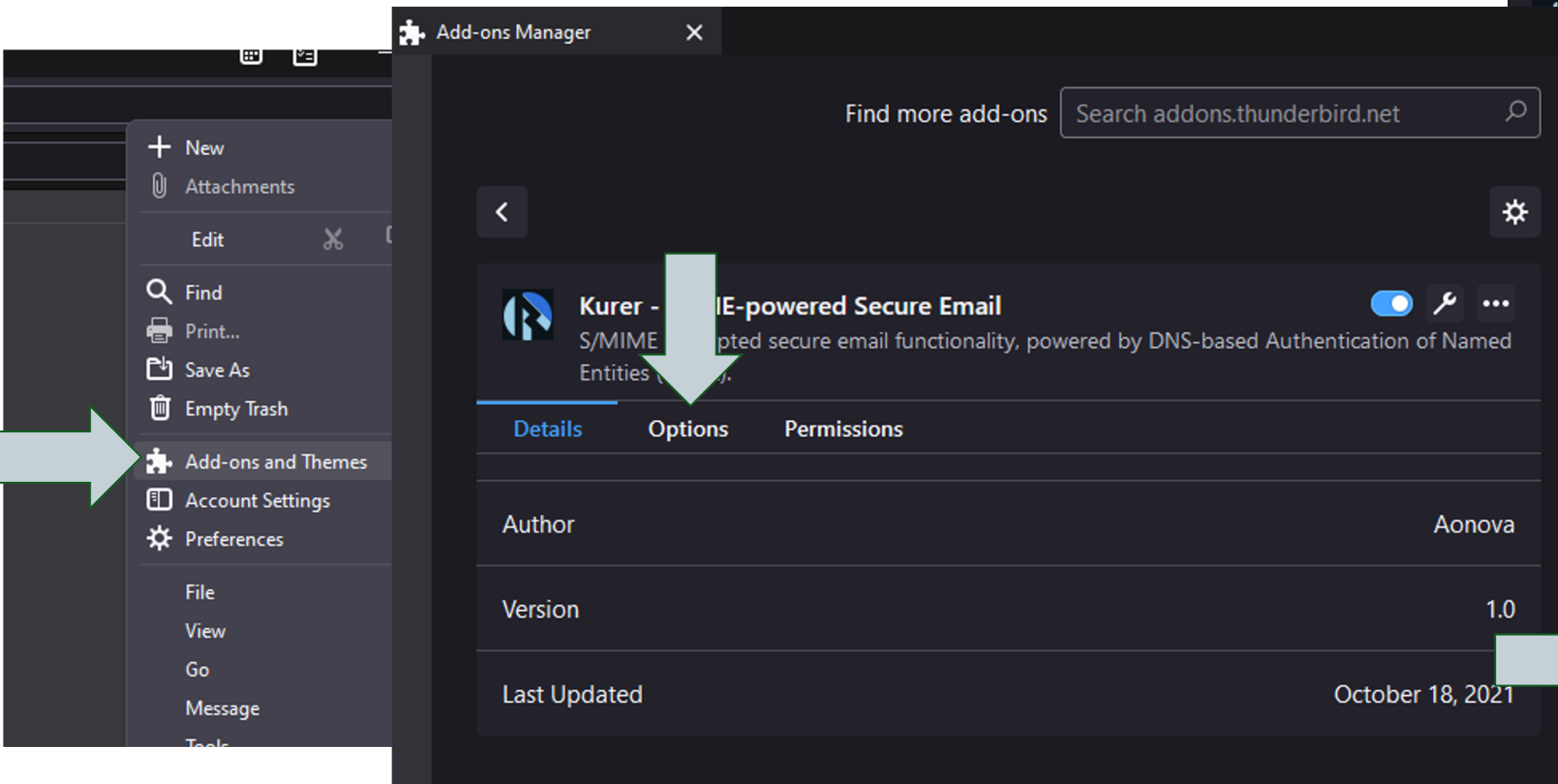
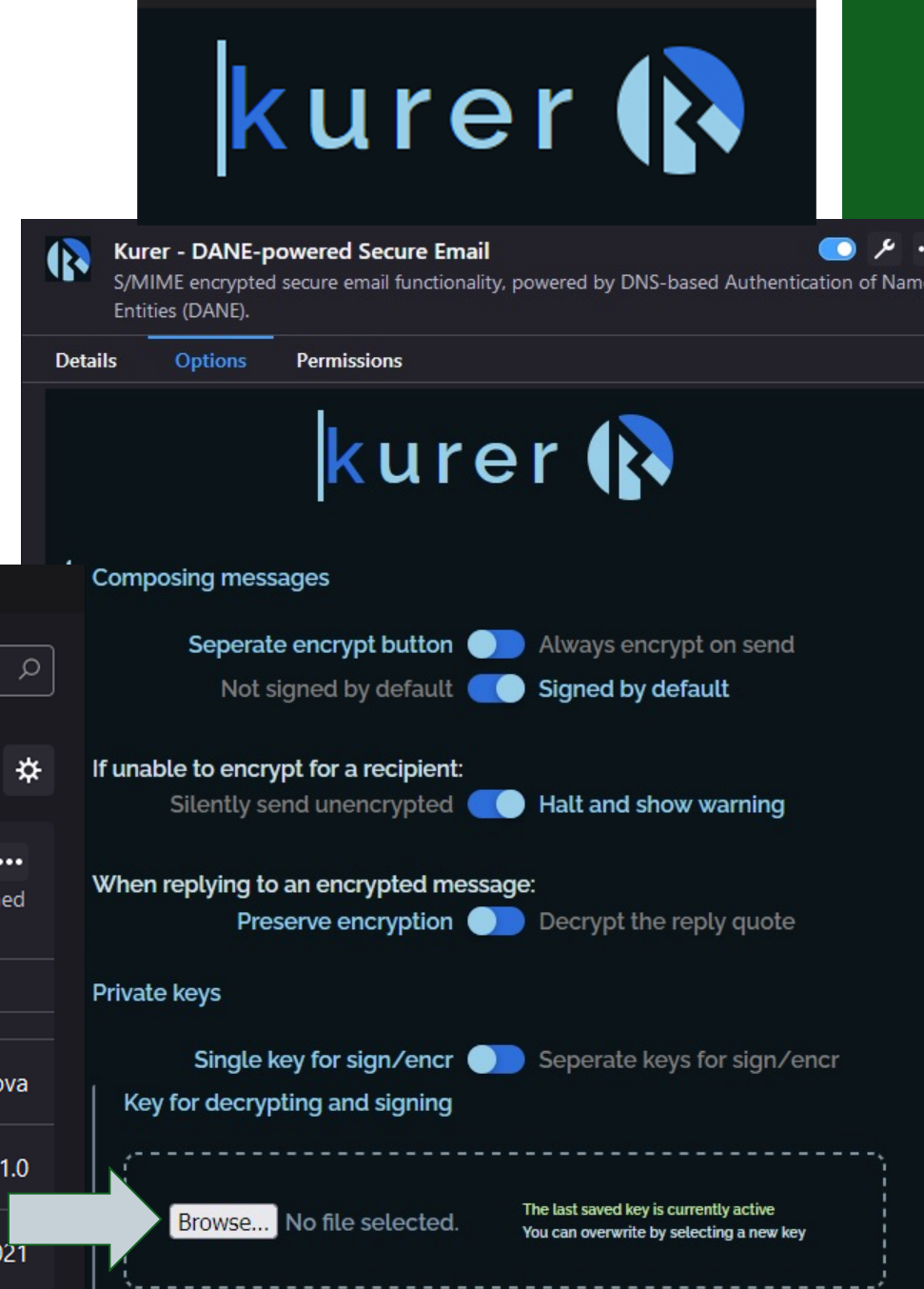
KURER FOR THUNDERBIRD

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



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

A composite screenshot illustrating the Kurer workflow in Thunderbird. The background shows the "Write: Test secure message" window with the "Security" menu open and the "Kurer" option selected. A "Sending Message" dialog box is overlaid, showing a progress bar. In the foreground, a large Kurer popup is shown with the "SEND ENCRYPTED" button highlighted by a grey arrow. Below the button is a "Sign" toggle switch, which is currently turned on. To the right, an "Inbox" view shows the sent email with a "SMIME Message Decrypted" notification bar at the top, indicating that the signature was verified and the message was encrypted. A grey arrow points from the "Inbox" area down to the notification bar.