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

Tawhidal Islam - tislam20@gmu.edu

Josh Yuen - jyuen2@gmu.edu

Pavan Kumar Dinesh - pdinesh@gmu.edu

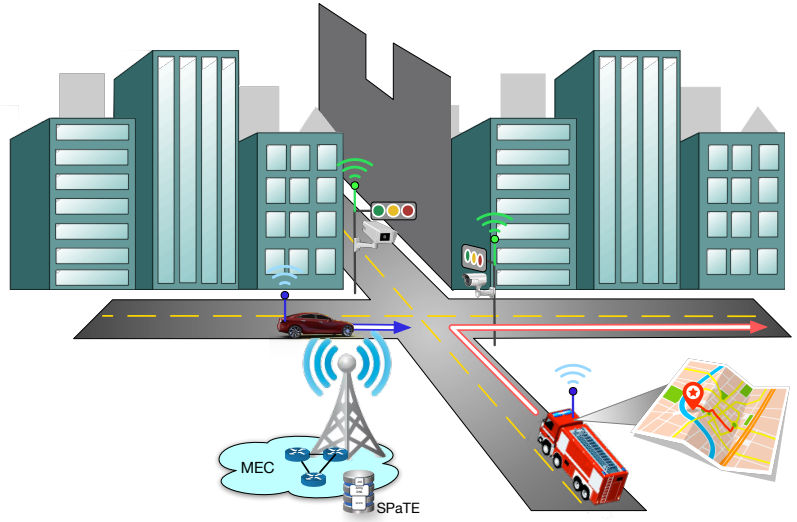
Tomofumi Okubo - tomofumi.okubo@digicert.com

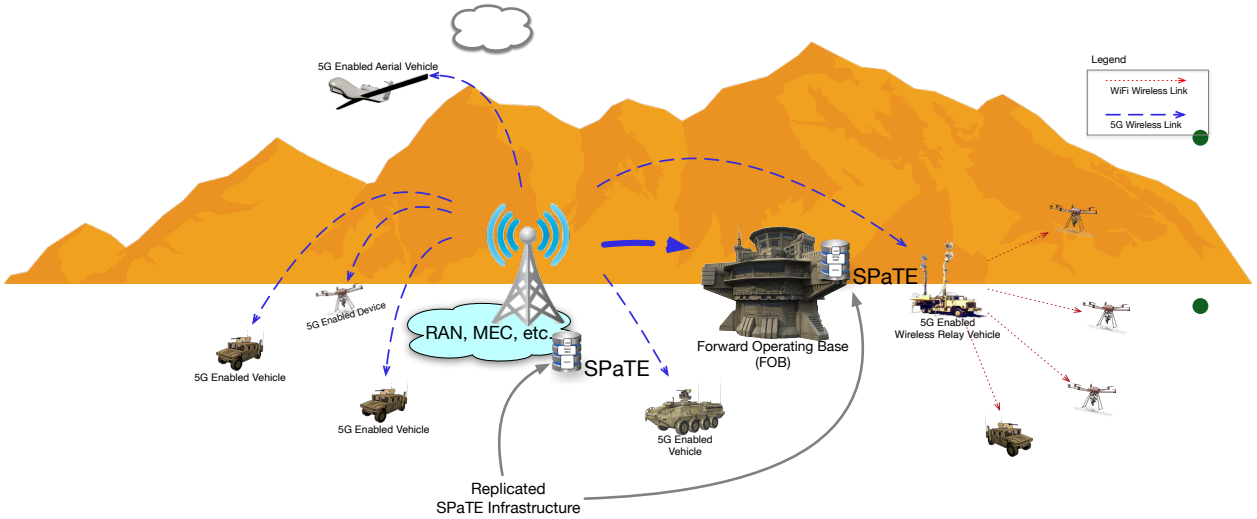
Eric Osterweil - eoster@gmu.edu

GEORGE MASON UNIVERSITY

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?





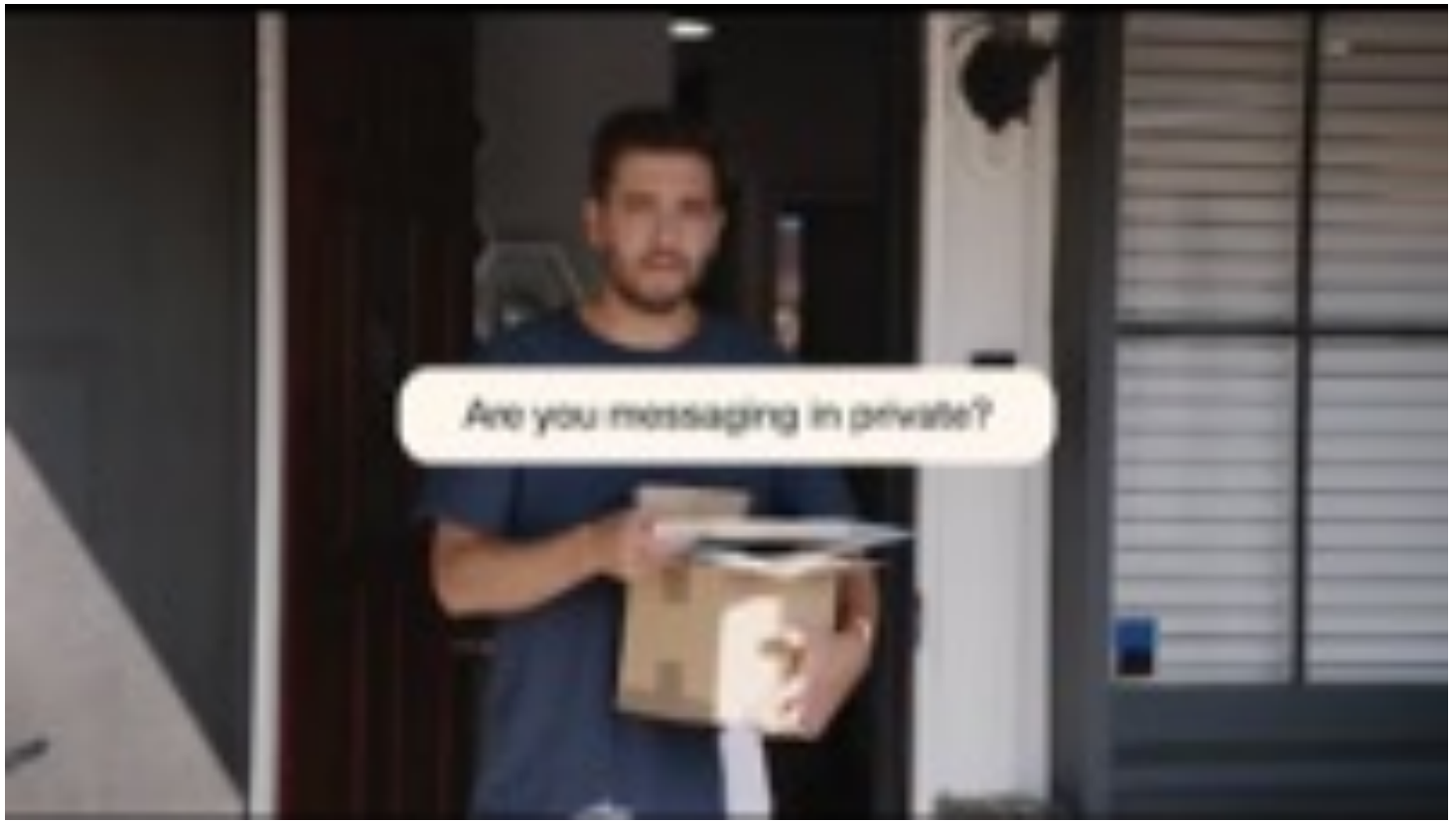
- Why do we need trusted network and transport layer protections to connect devices?
- Shouldn't the ***messages*** be protected too/instead?
- This is ***object-security***, it is different and more powerful

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*** 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

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

ARCHITECTURE FOR INTERNET OBJECT-SECURITY

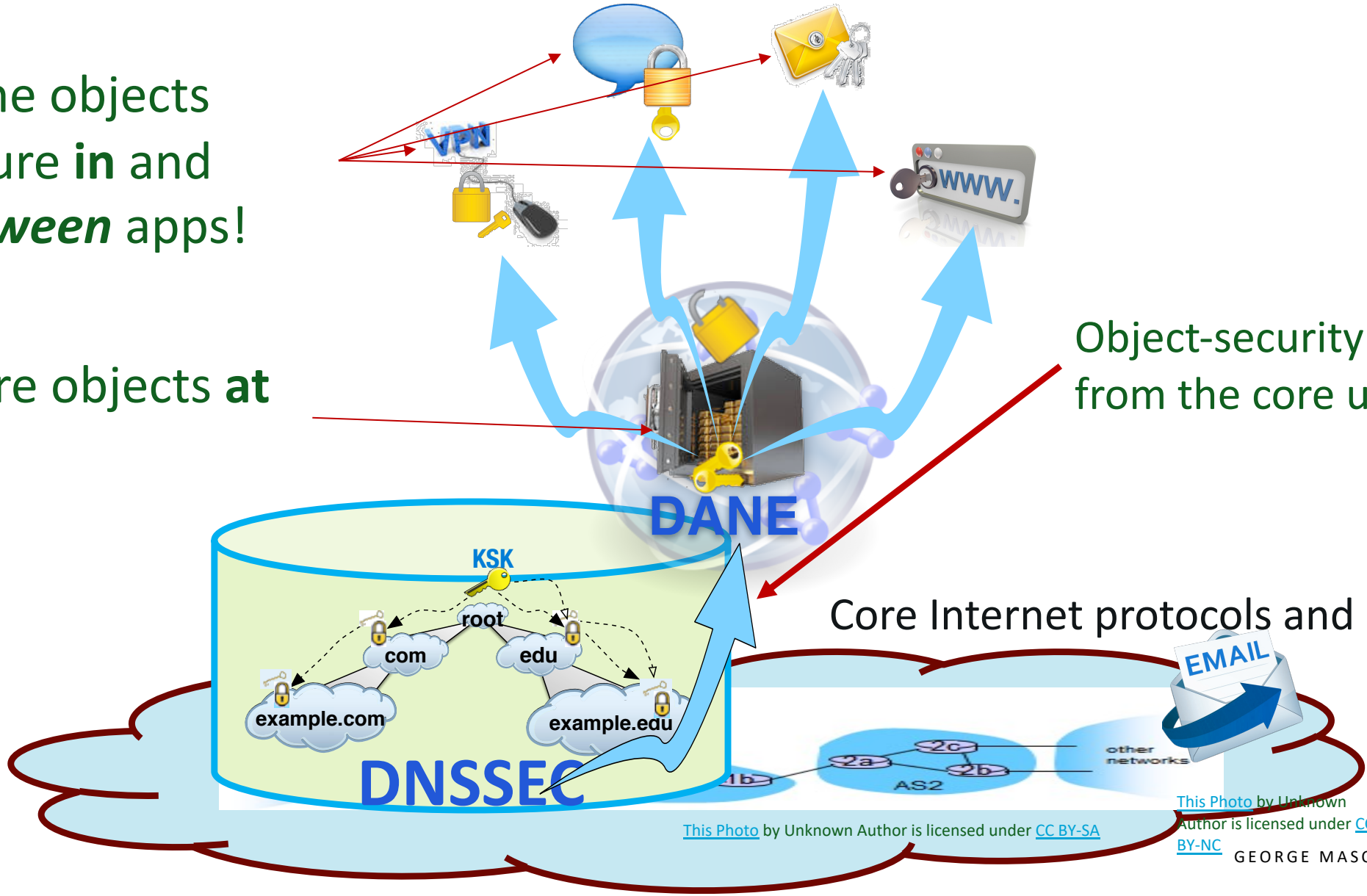
- Examples like IoT, mHealth, V2X, etc. show increasingly repeated requirements:
  - Inter-organizational (e.g., entity at University A to entity at company B)
  - Per-entity (e.g., device, user, etc.) E2E crypto at Internet-scale
  - Usable tools
  - Automation

- The foundations we need already operational in Internet's core
- The Domain Name System's Security Extensions (DNSSEC)
  - 16+ years, ~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!

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

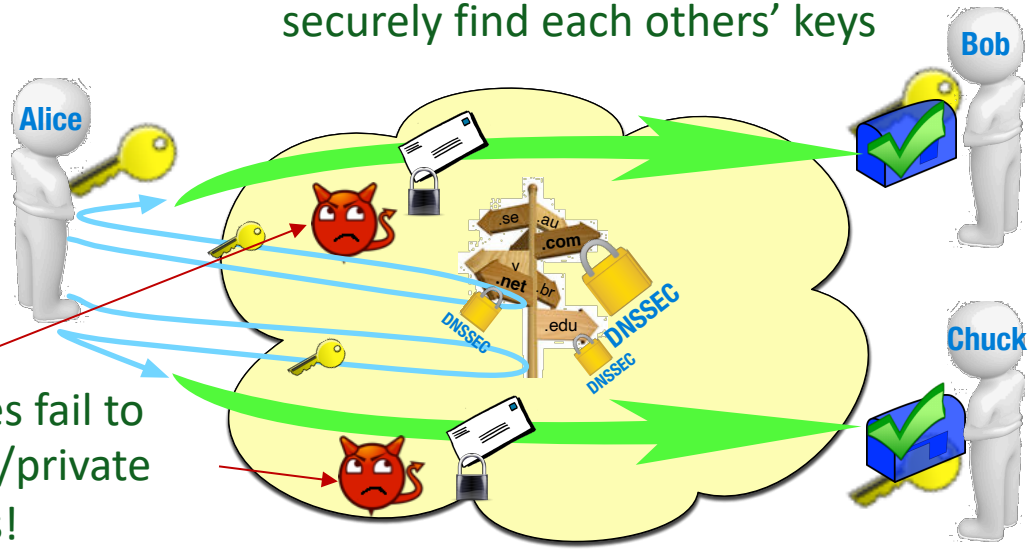
Adversary fails!

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?!?

INTRODUCING KURER AND DANEPORTAL.NET!

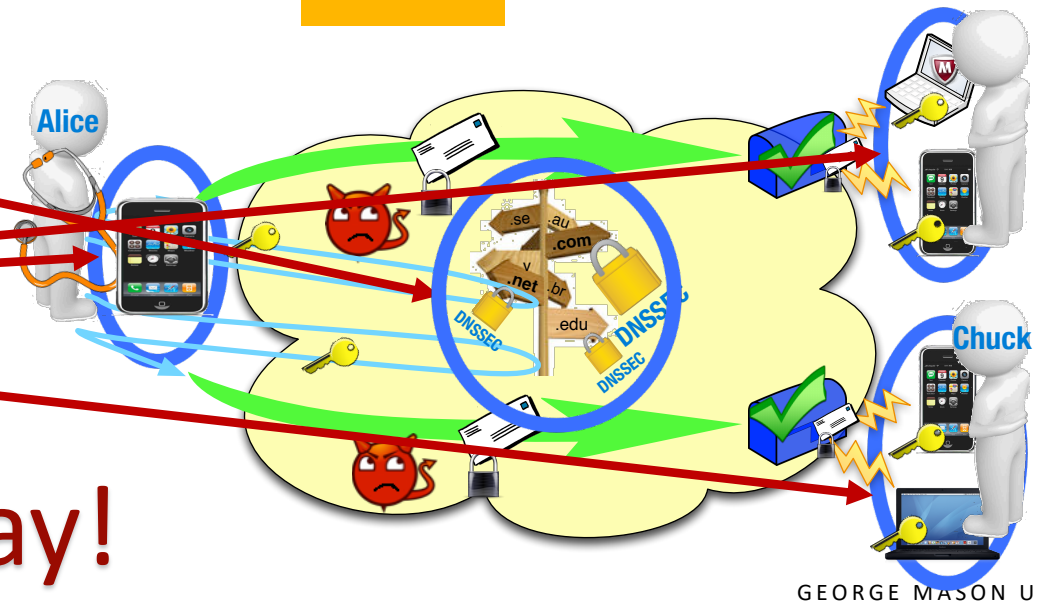
- To do that, we have built a ***live*** experimental apparatus: secure email

- 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?

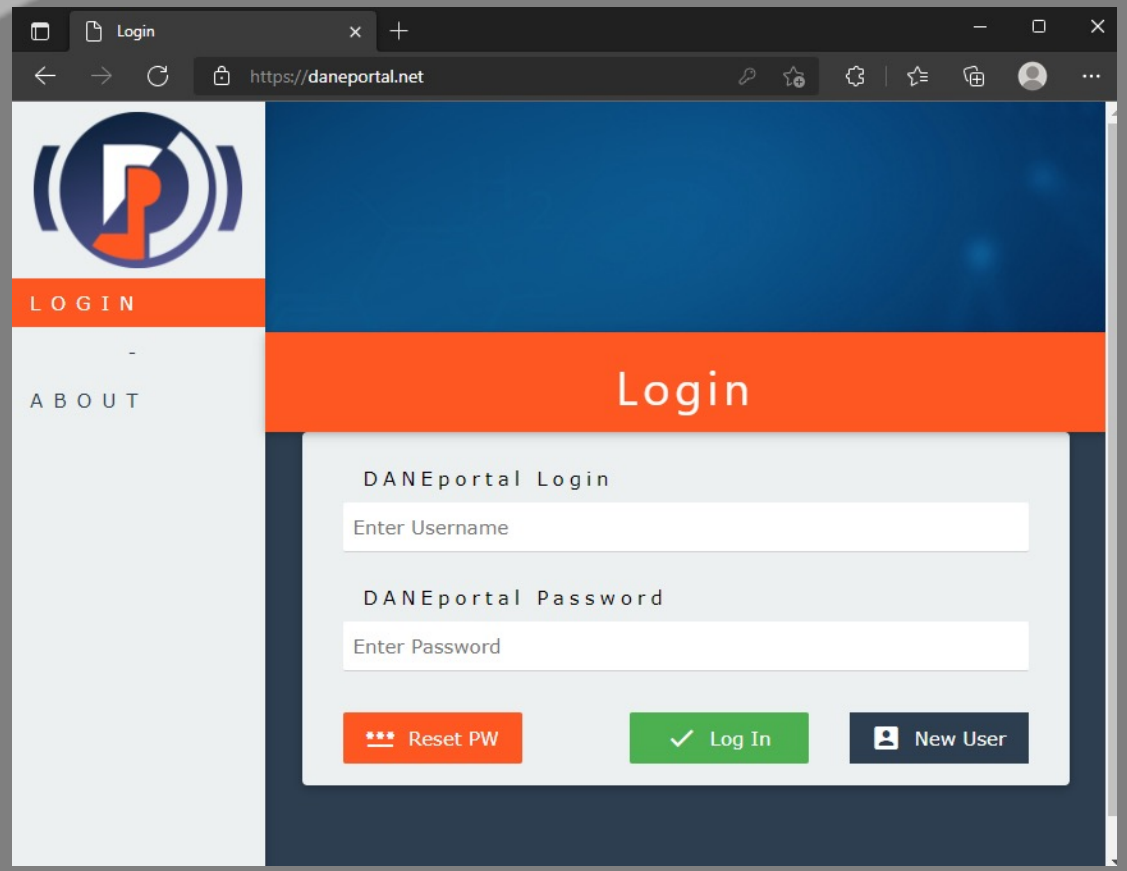
- DANEportal.net is where email users from any domain ("identity holders") can securely make their crypto keys *learnable*
  - Domain holders securely claim their zone (using ACME protocol)
  - DANE is managed for them
  - Email users, under a domain, create accounts and manage their own key life-cycles

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 extended further… more later

HTTPS://DANEPORTAL.NET/

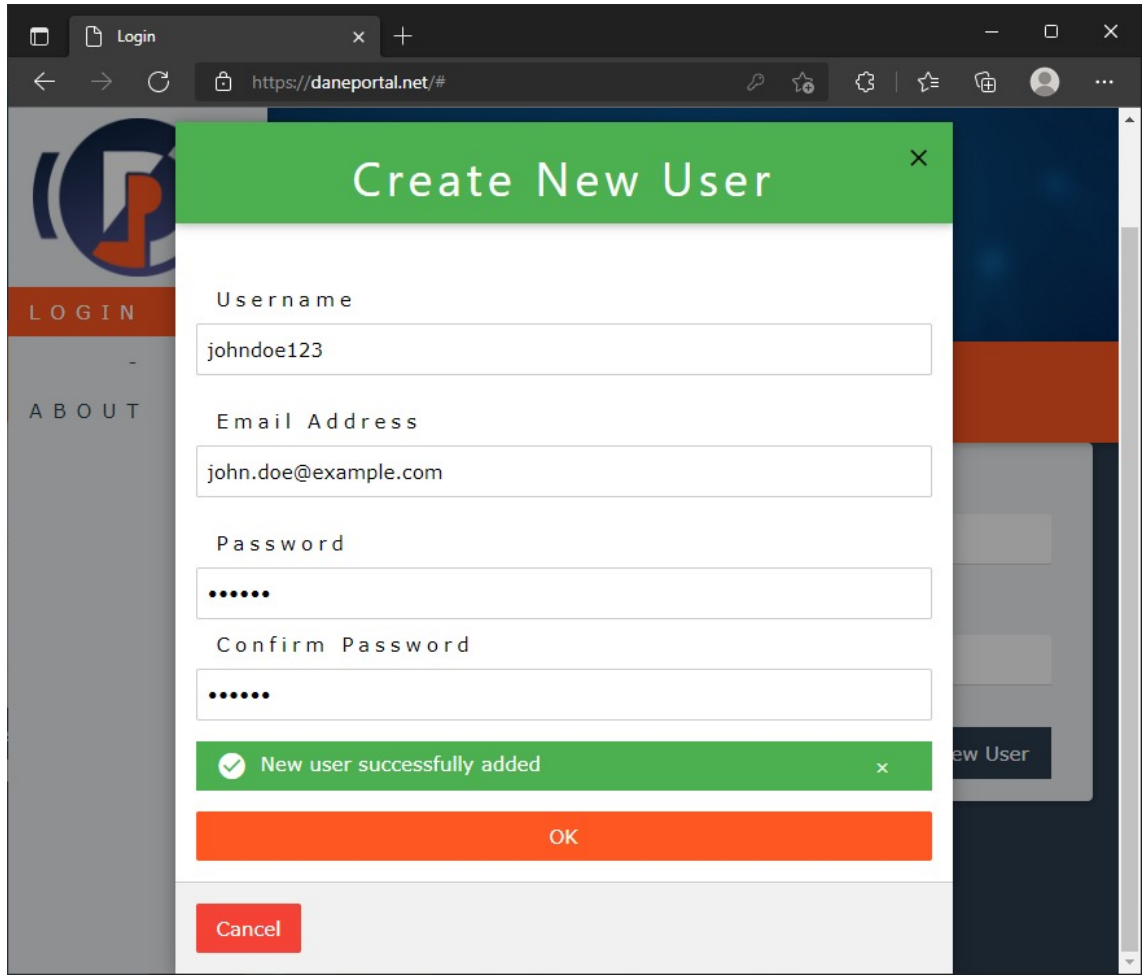
OVERVIEW, FULL GUIDE AVAILABLE ONLINE…



CREATE YOURSELF A USER ACCOUNT

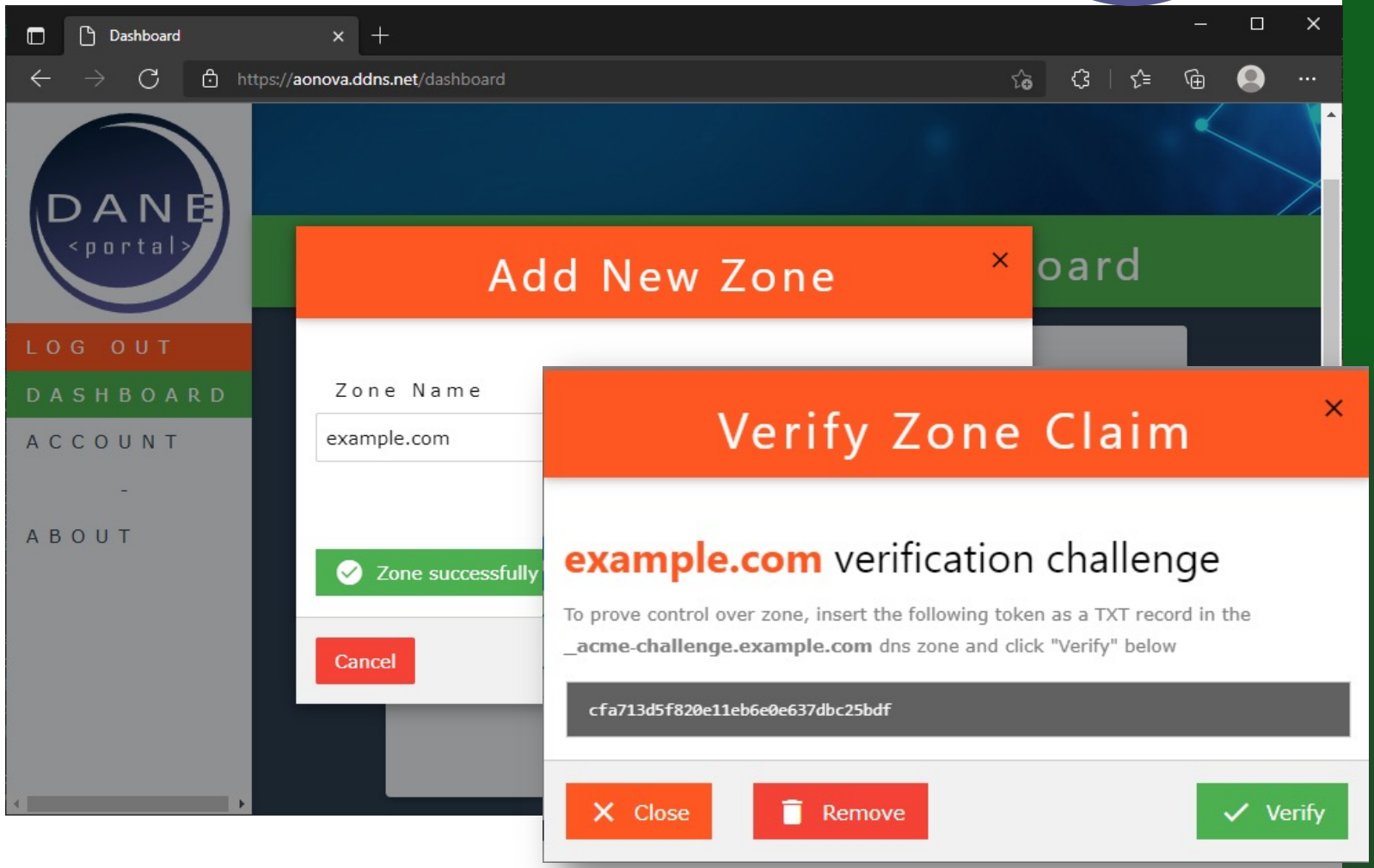
- Click [New User]
- Enter desired credentials
- Click [Create User]
- Click [OK] to close modal

- 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



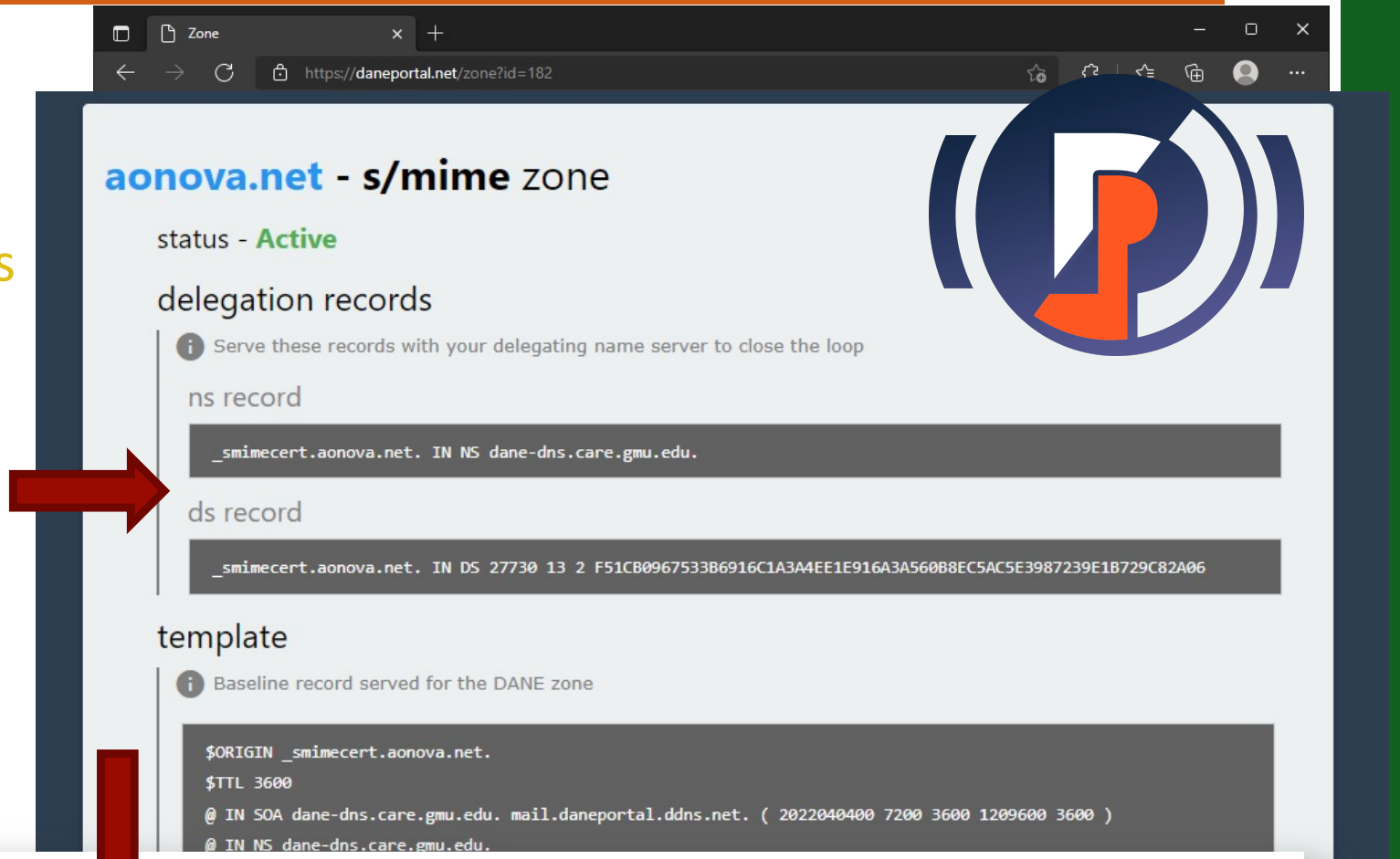
ADD YOUR OWN ZONE

- 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 DANEPORTAL 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



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.

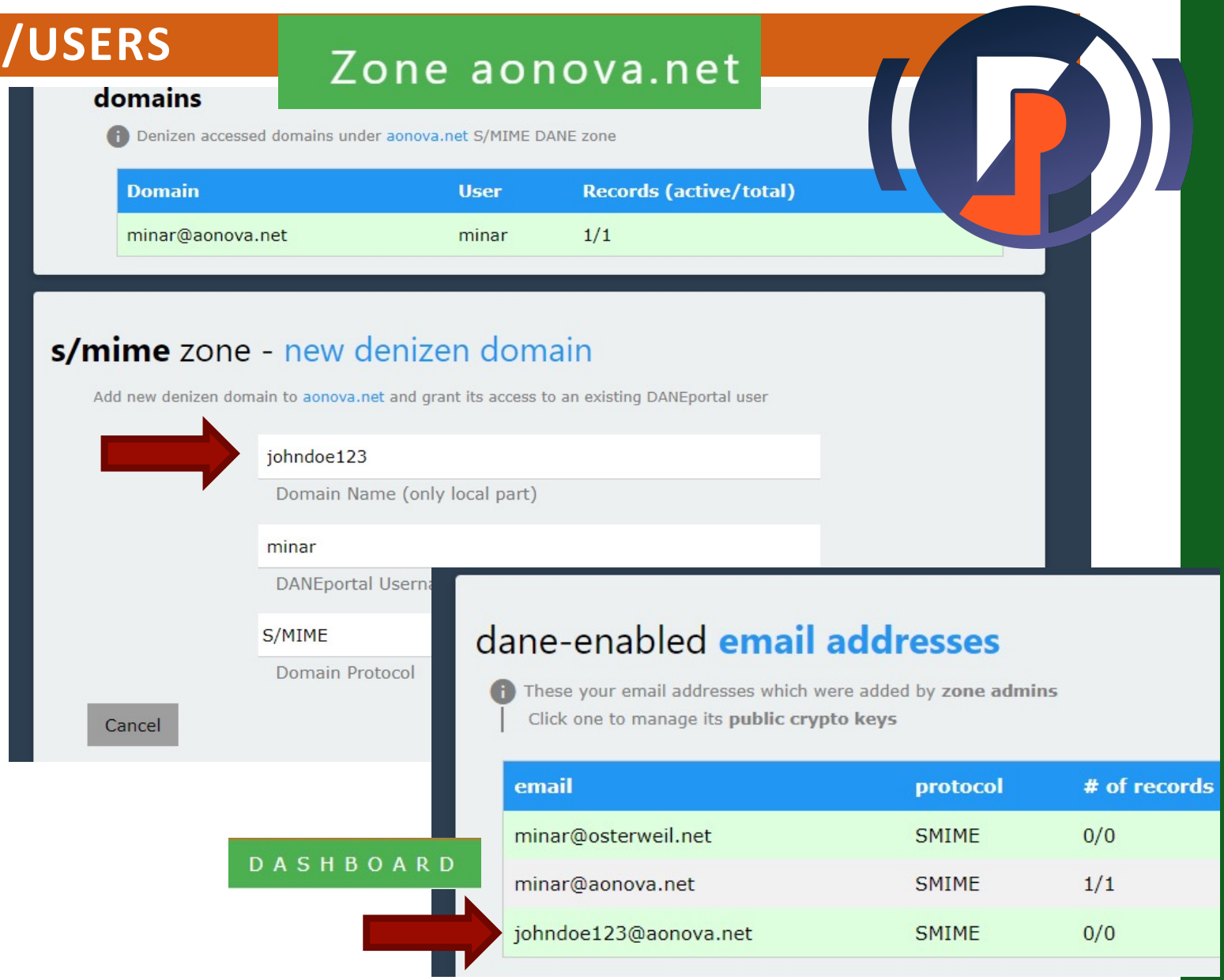
Google Domains

NOW, ADD EMAIL ADDRESSES/USERS

- **Denizen Users** email addresses under a zone, administered separately

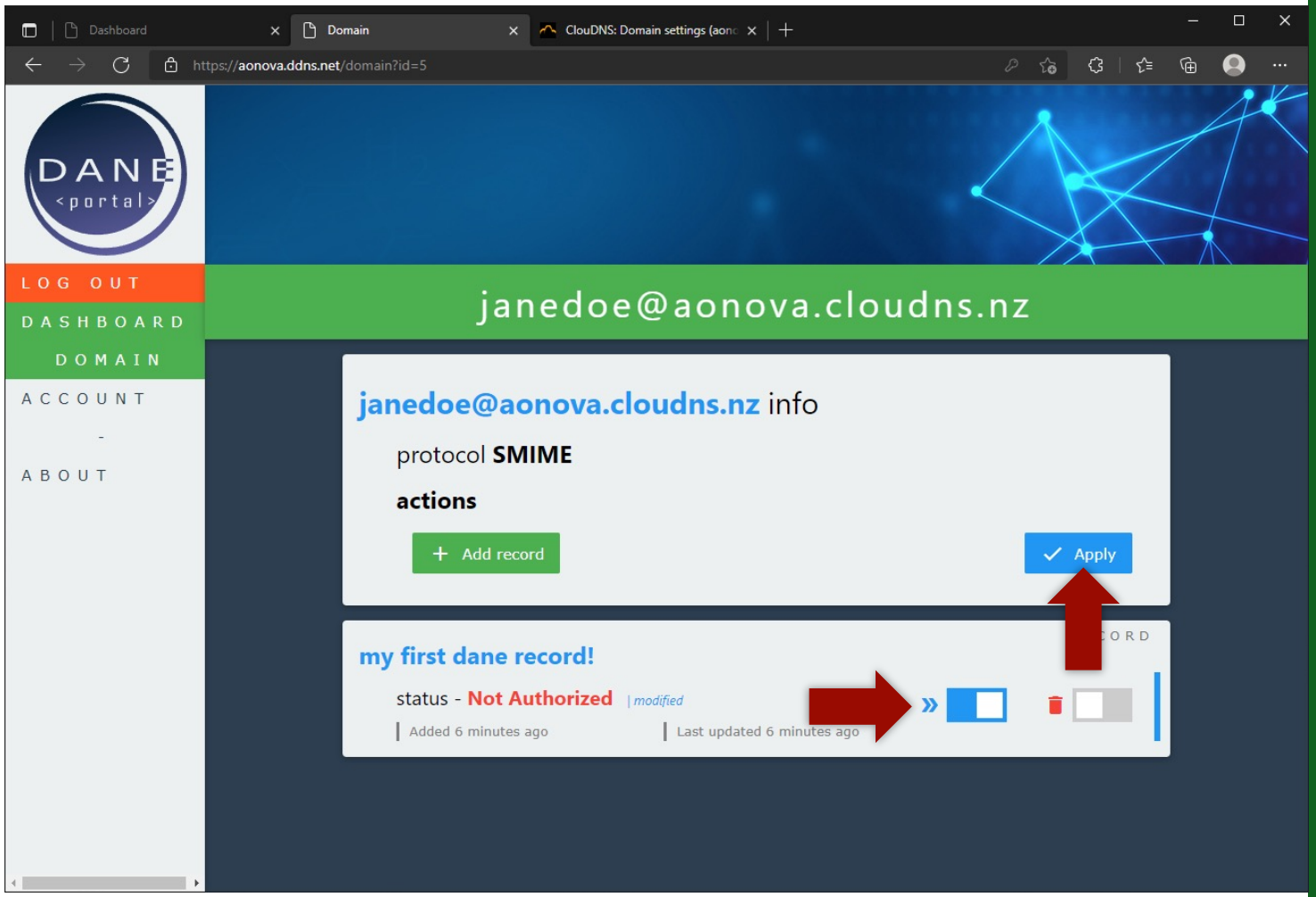
- In the context of DANE S/MIME, the **denizens are your email users**
  - DANEportal allows them to add their S/MIME records to **your** DANE zone without you losing any of your control as zone admin

- Click [Add domain] to open the form

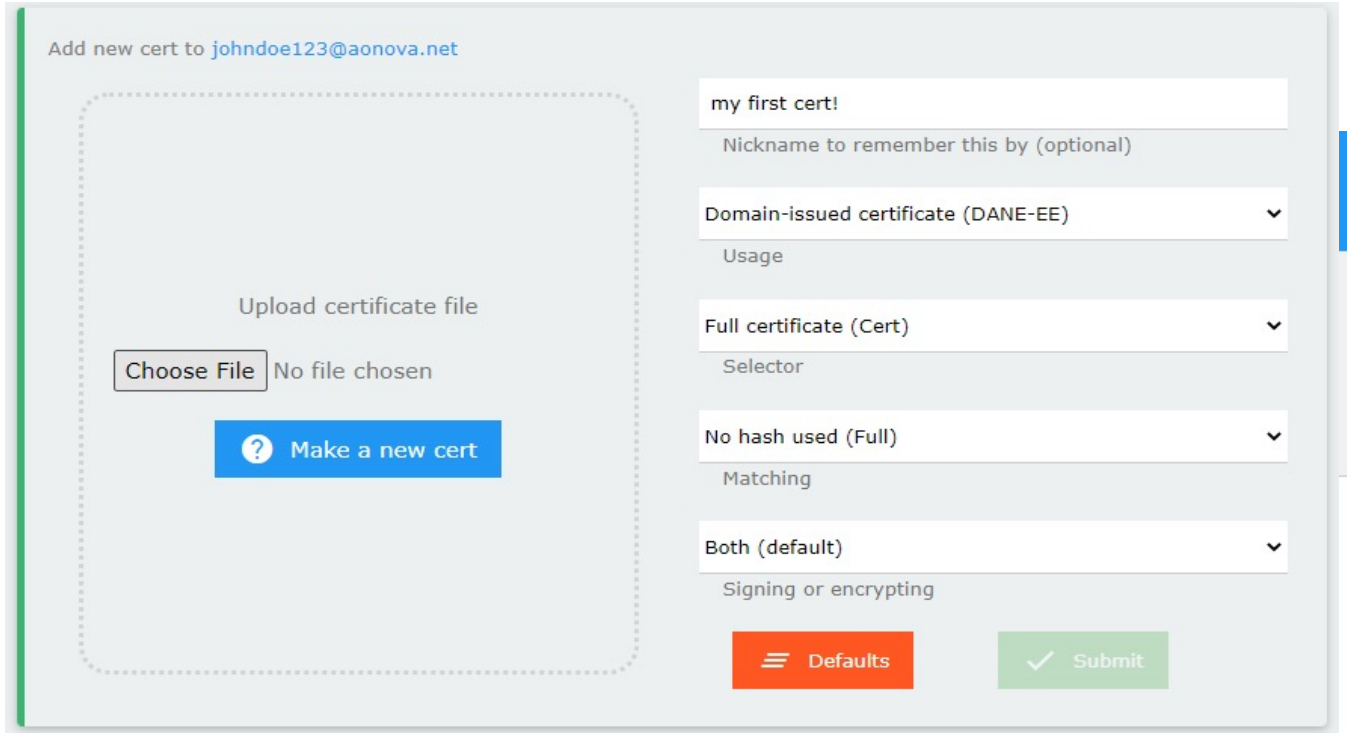


NOW, ADD EMAIL ADDRESSES/USERS

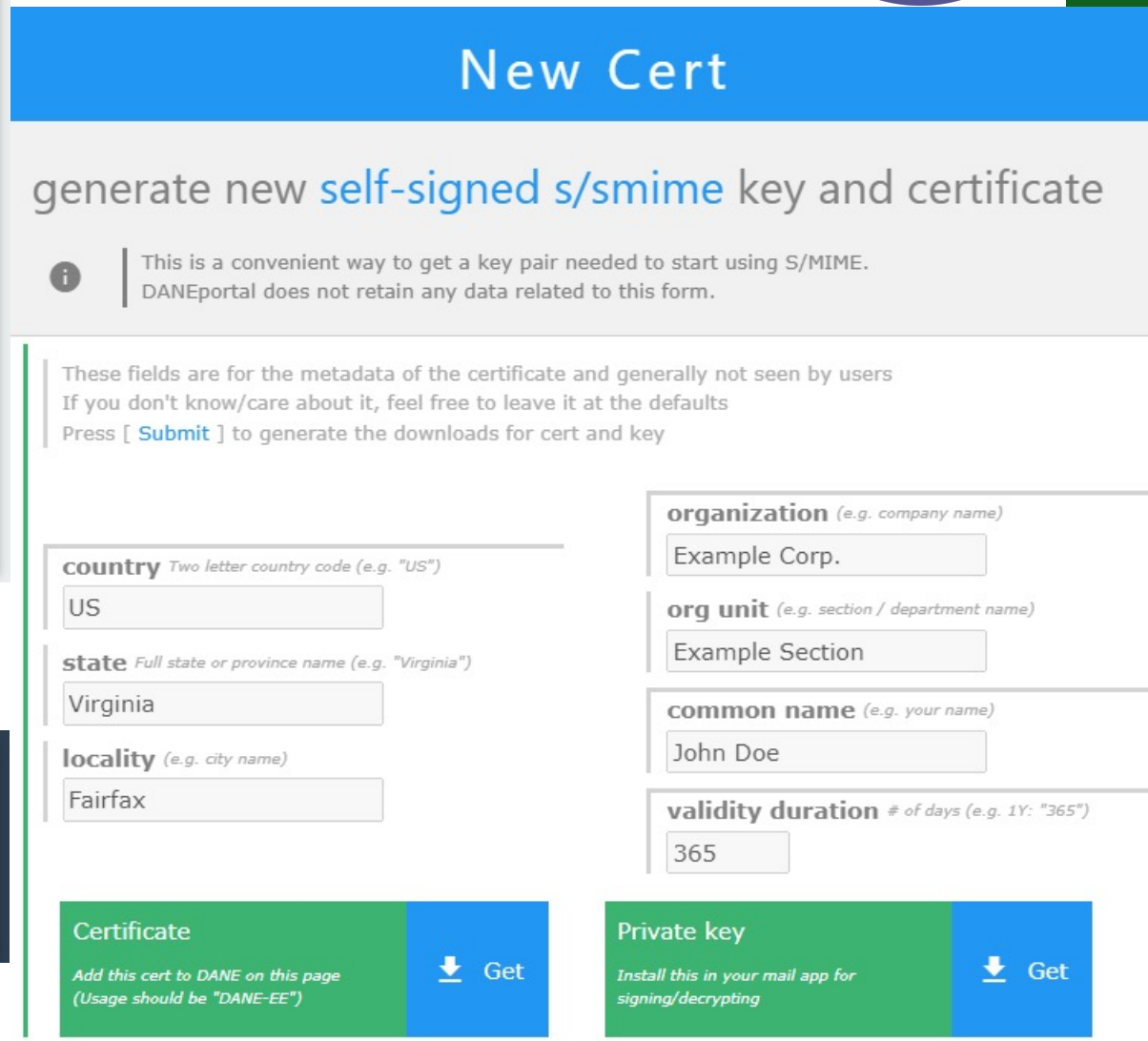
- You should now see a **card representing the record you just added**
- Manage records by toggling its authorization state or deleting it permanently
- For now, toggle the **authorize** switch to the right and click [Apply]



EMAIL USERS CAN MANAGE THEIR OWN CERTIFICATES



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



KURER: SECURE EMAIL FOR EVERYONE!

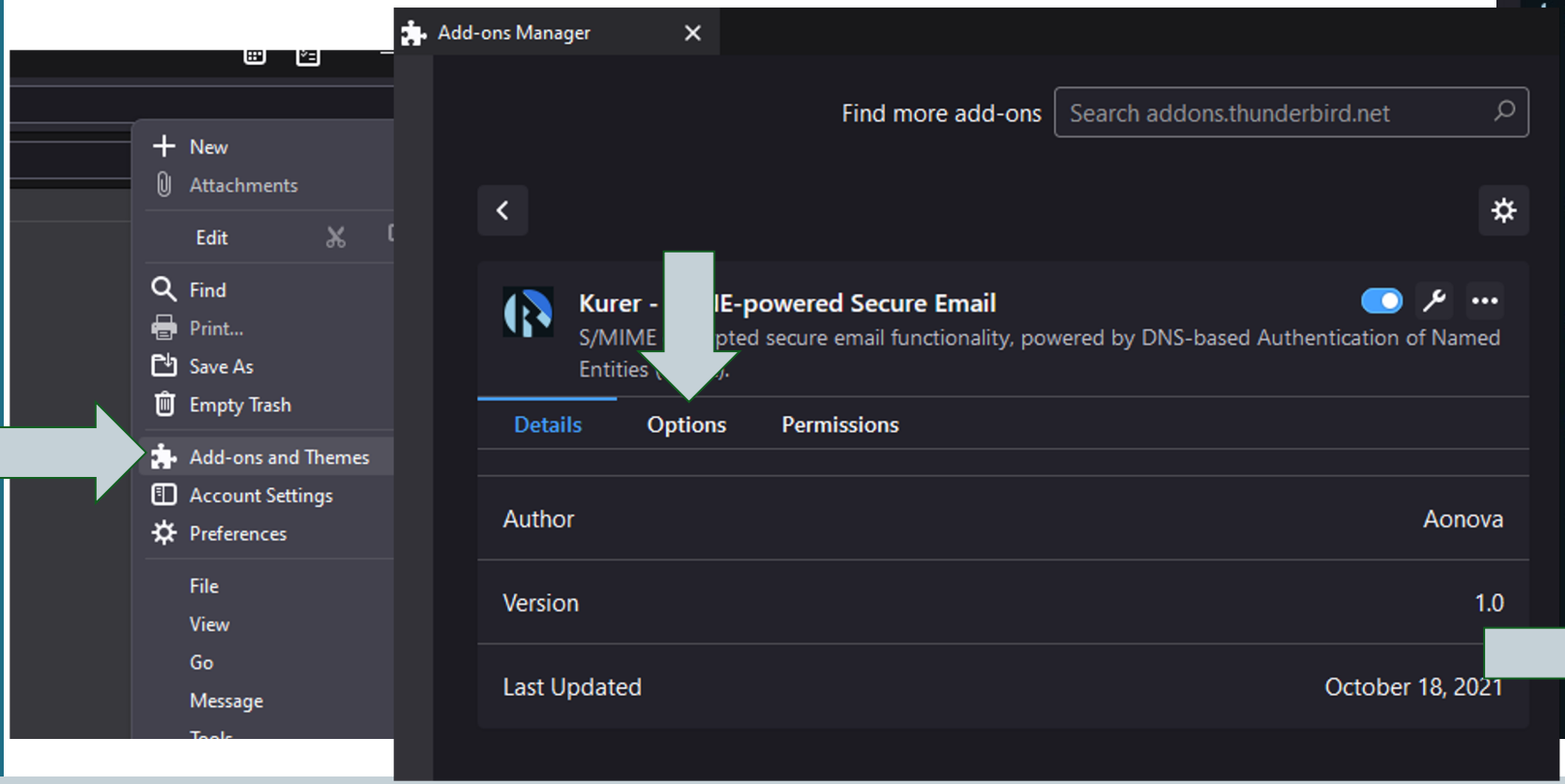
KURER FOR THUNDERBIRD

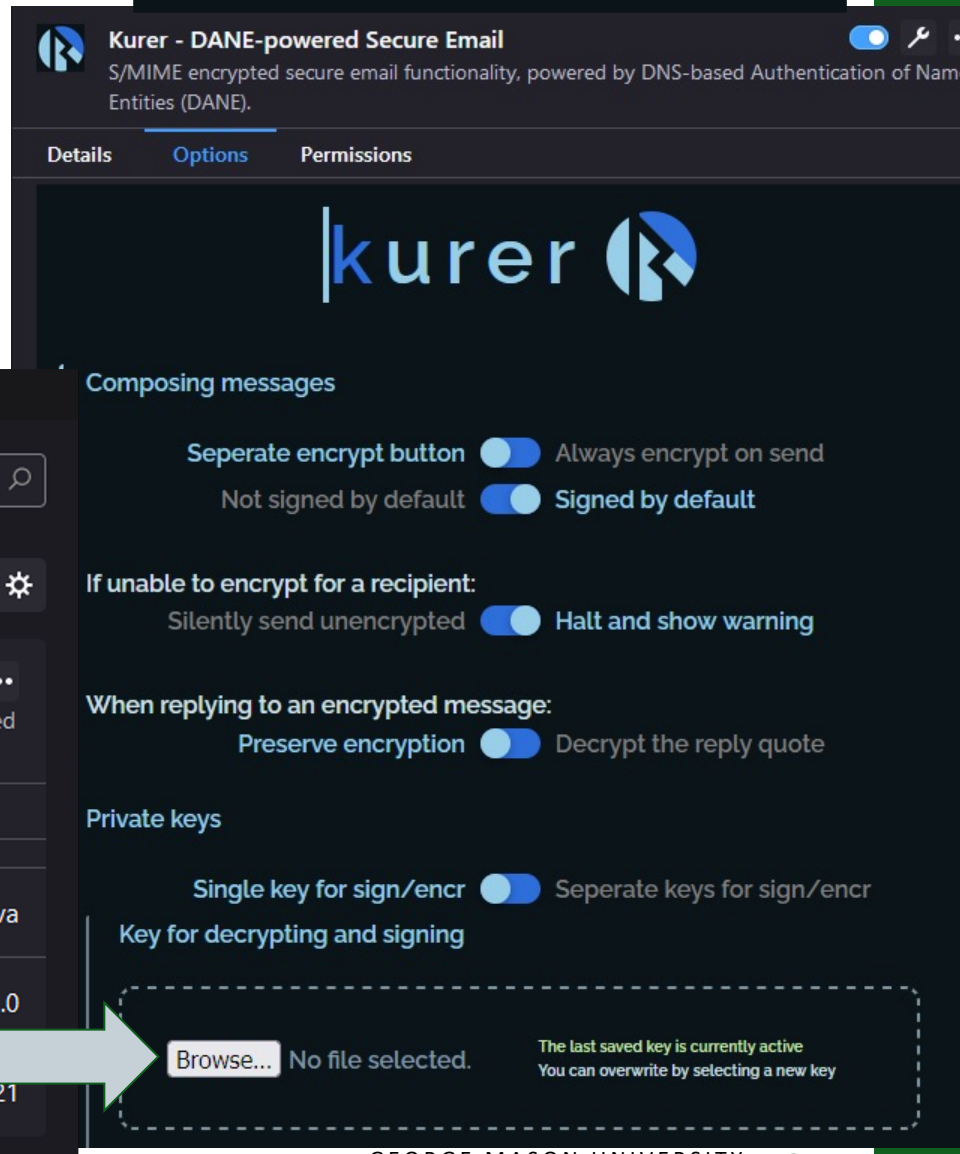
No-click solution for seamless DANE S/MIME

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

Only one setting is really needed for now:

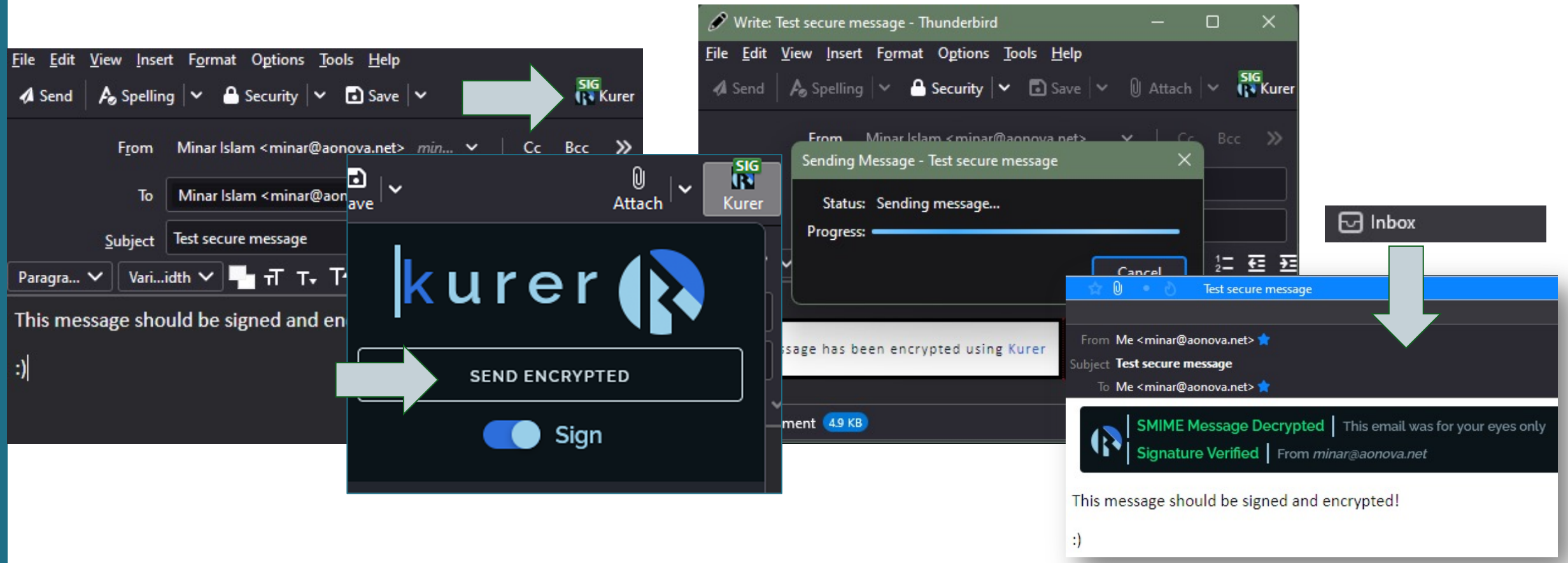
- Enter your private key and sending email address to allow signing your email





JUMP RIGHT IN TO SENDING SECURE EMAIL

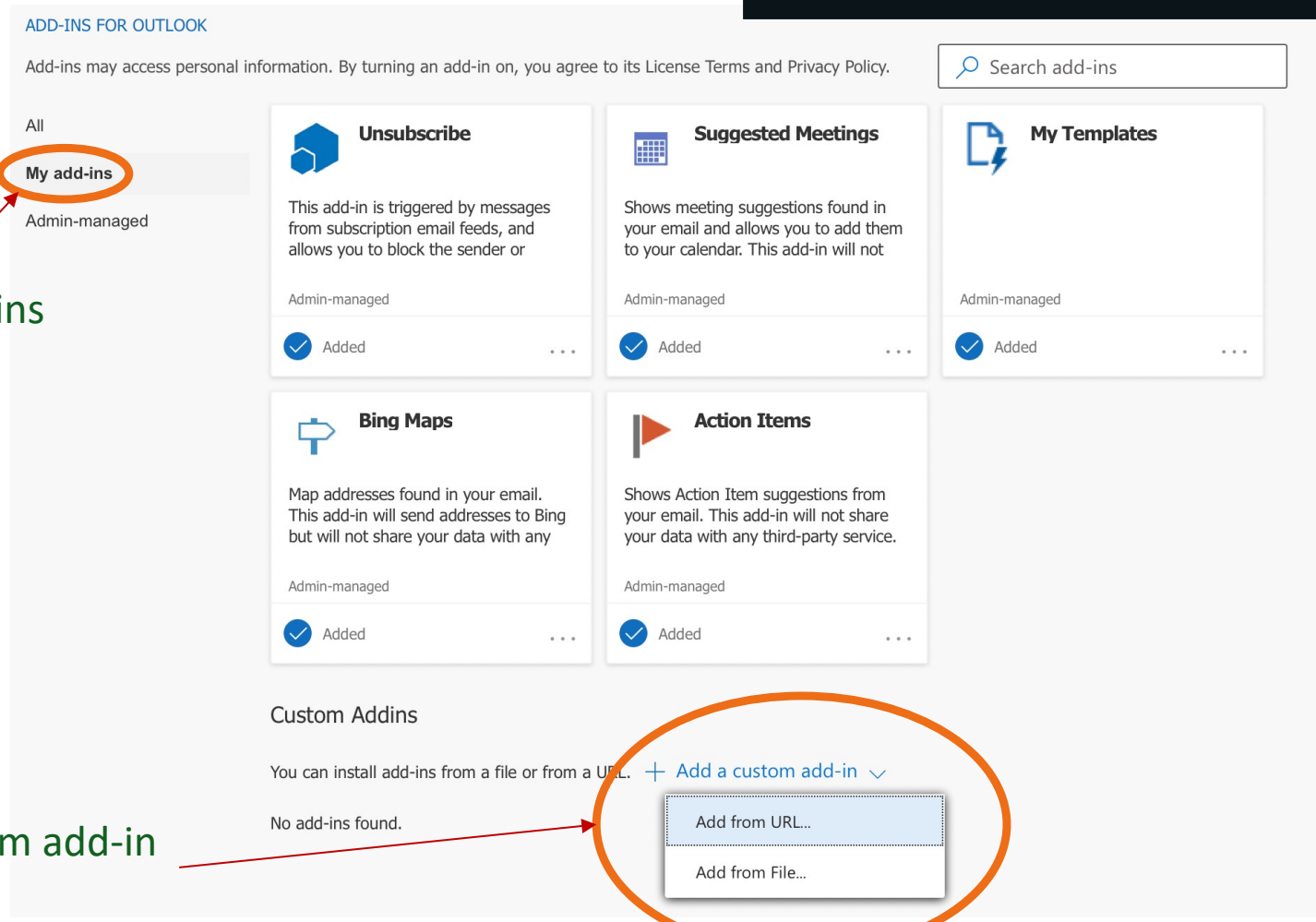
- Use the Kurer popup to toggle signing and click send encrypted
  - The SIG tag on the icon means the email will be signed when sending



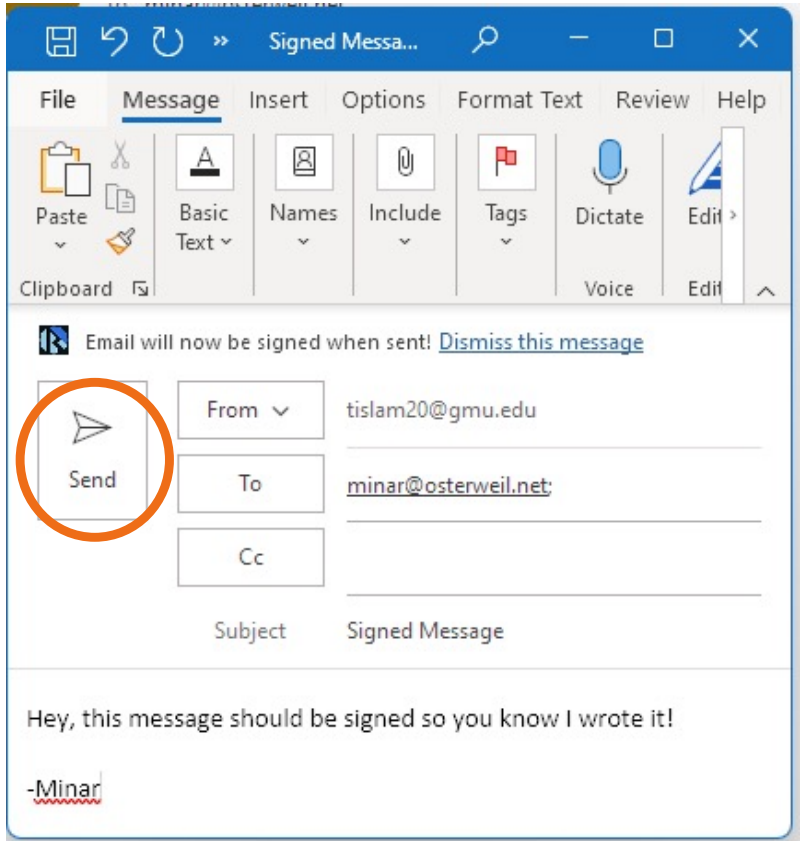
GETTING KURER ON OUTLOOK IS A SNAP!

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

My add-ins

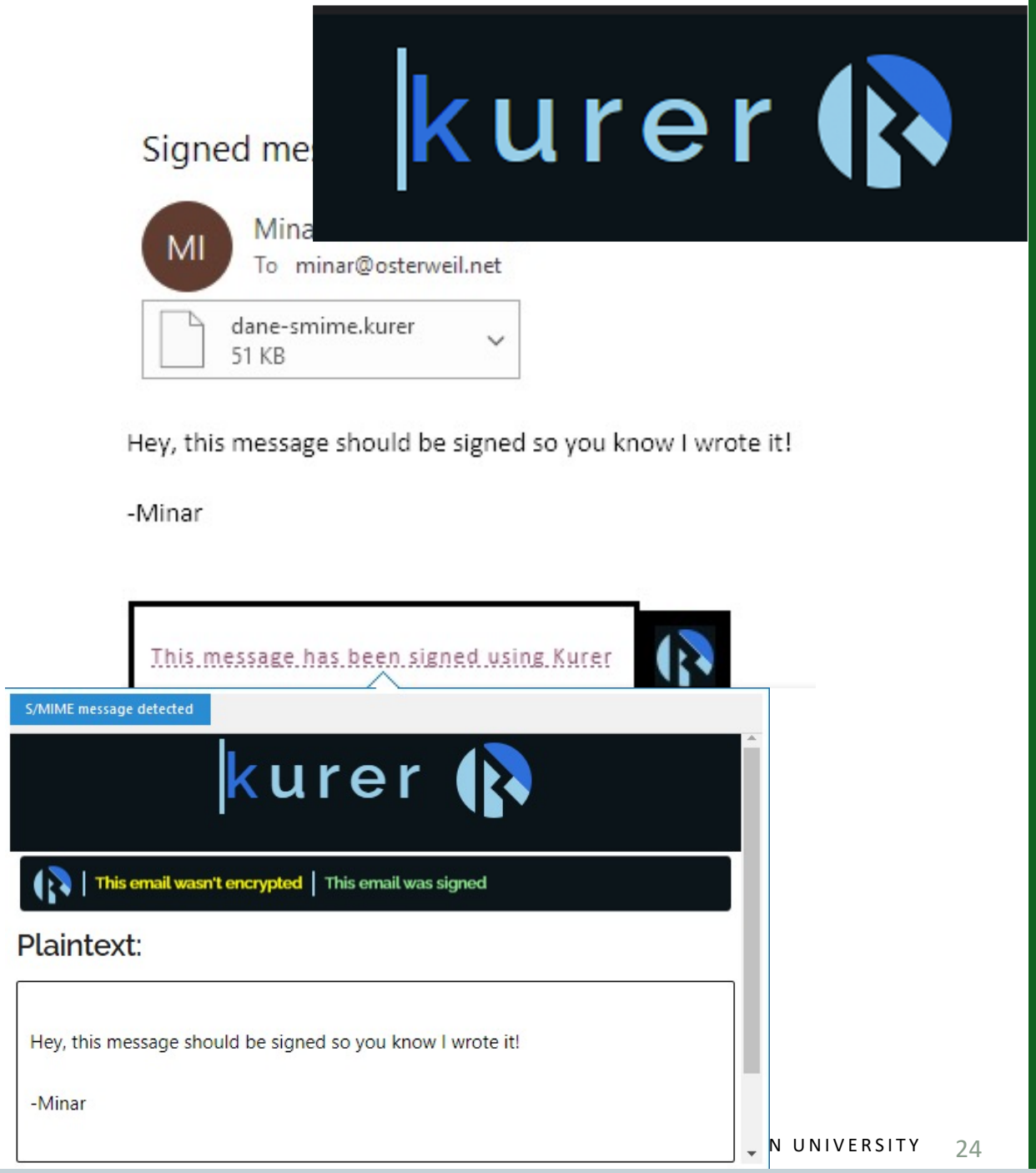


Add a custom add-in from URL:

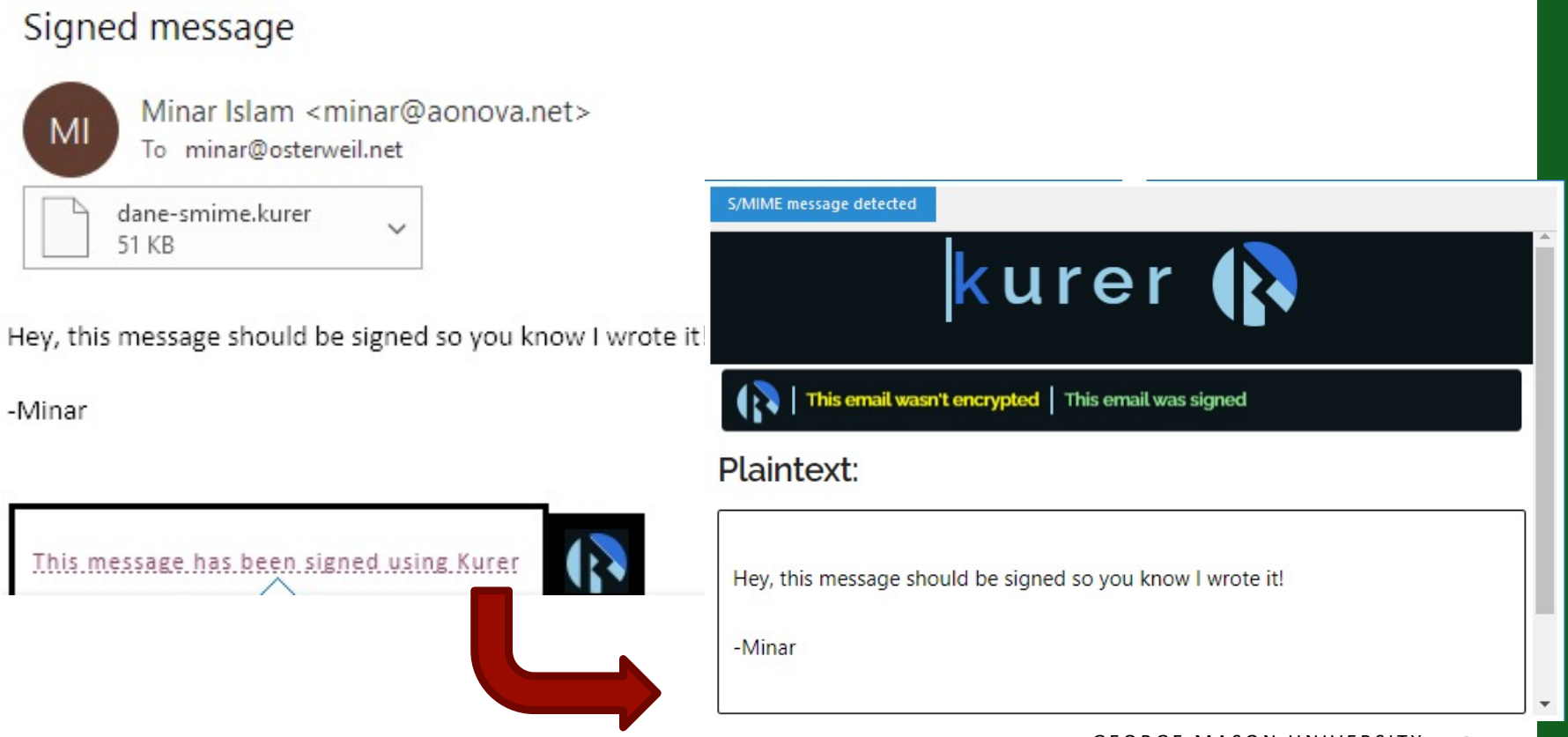


Sending

Receiving



- 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



STATUS

- DANEportal.net is live, today

  http://daneportal.net/

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

  https://kurer.daneportal.net/install

DISCUSSION

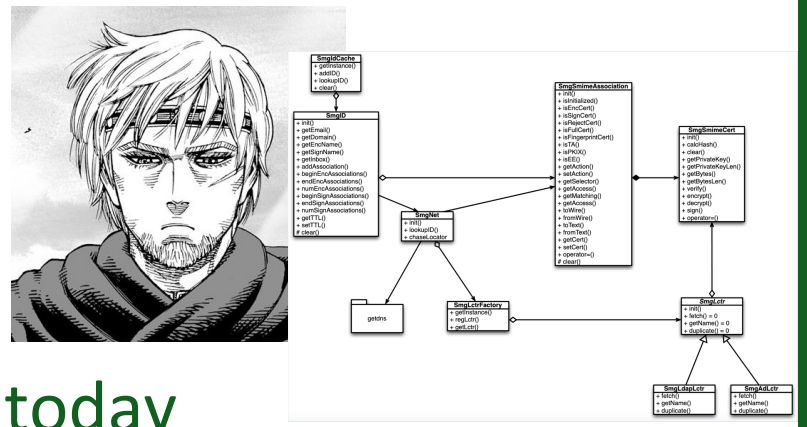
- Why not build cybersecurity / privacy protections from the top down?
  - Secure messaging works, right?
  - Why not build on blockchain?
  - Why not something else that fills a need?
- Internet needs an architecture for ***cross-app*** object-security
- Internet continuously proves things that "work"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

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

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



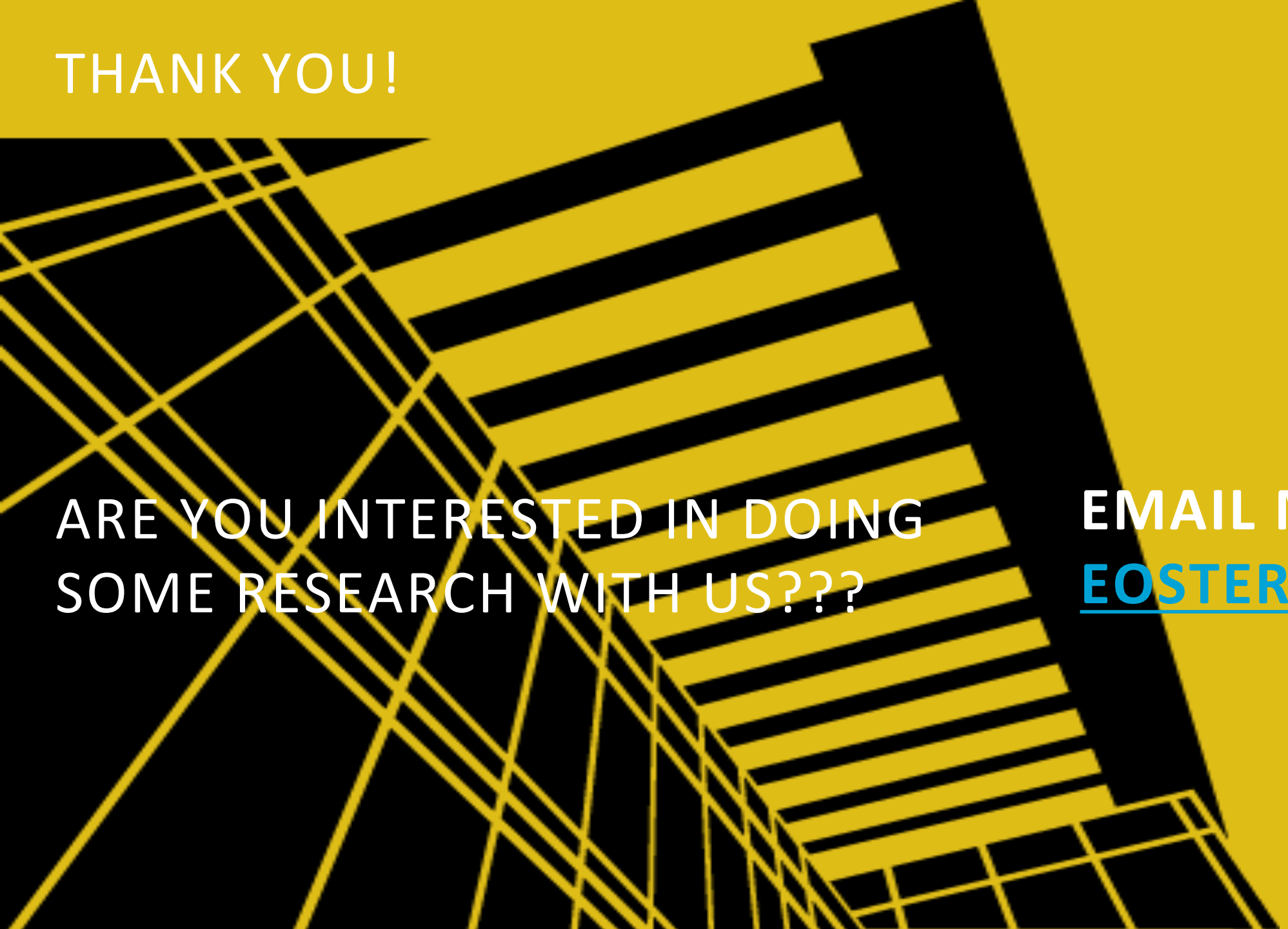
- DANEportal.net and Kurer will let you get started today

kurer

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 was 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!



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

EMAIL ME:
EOSTER@GMU.EDU

BACKUP