① End-to-end Security and Privacy — What's the big deal?

- **E2E Security** is **NOT a "default"** on the Internet -- despite **decades of maturity**

-- if it were, we could have:

- **Internet-scale Object Security**: IOT devices, mHealth, Smart-city infra.
- **Legal standards**: easy compliance — HIPAA, GDPR
- **Adaptive security**: Enforcement on receiver — *ETLP*
- **Cyber Threat Intelligence**: secured sharing

S/MIME spec written **20 years ago**

Active research (CCI-funded) — ***Invisible Security***

Imagine the Internet before *https* ... **that is where we stand** for E2E

- **Secure Email** is the launchpad to bring **ubiquity** to **E2E security**

email: the grandfather of messaging

- **everyone uses it**
- **barely anyone secures it**

why?
- technical: **usage limited** to organizational **boundaries**
- human: **annoying to use** for the everyday individual

Solution – **give email users a simple "ON switch" for secure email**

with Cert Management System and MUA add-on

daneportal.net — **Kurer**

Commonwealth Cyber Initiative

② Secure Internet-scale Key-learning

biggest limitation: Can't cross organizational bounds

why? security by **public-key cryptography**, but we can't learn the **public keys**!

Solution: allow ***anyone*** to find ***any*** **cert** by putting them on:

DNS (Mature, robust, and decentralized) + DNSSEC (record authenticity)

Made possible using the protocol **DANE**

DNS-based Authentication of Named Entities (RFC 6698)

Challenge — **Using DANE can be complicated**

- How to operate the DANE zone?
- Users have many emails addresses!
- What if email users want to use their own key?

The DANE key-learning solution

- **One-click:** Creates and serves DANE zone for zone admins
- **Streamlined front-end** lets users to add S/MIME certs

DANE <portal>

Key Design

Delegation of responsibility:
- **Admins** manage their zones and users
- **Email users** manage their own certs

Operational issues stymie interest and uptake

Overcoming them is **daneportal.net**

Learn more

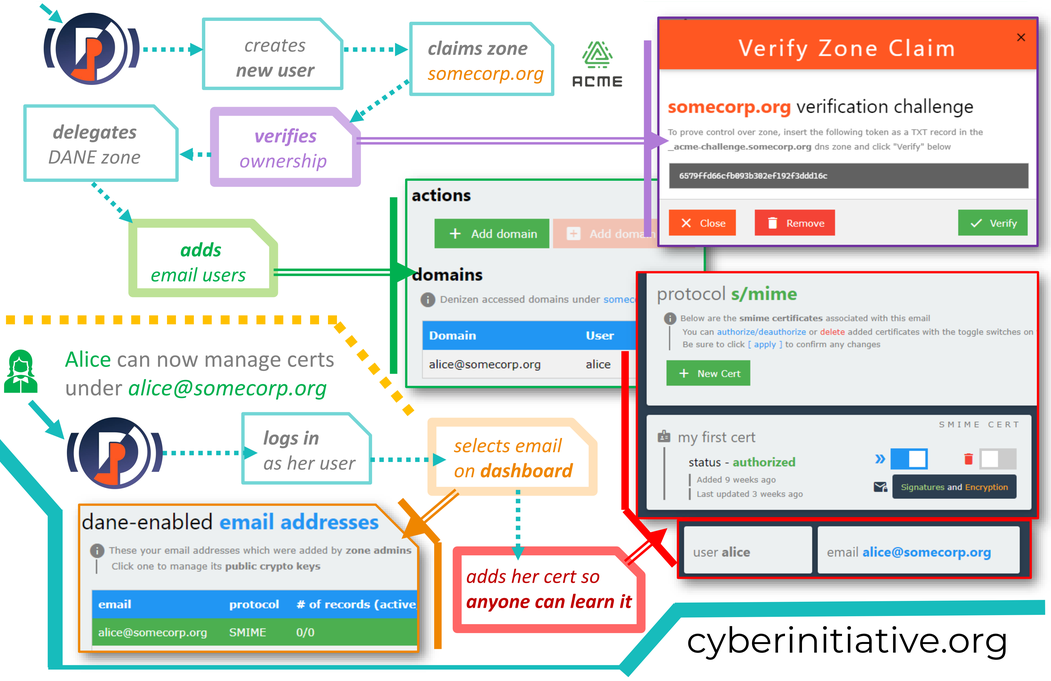
③ Getting DANE right now — USE CASE -- daneportal.net

Chuck administers *somecorp.org*

wants to let users to handle their own certs on DANE

Alice is a user: *alice@somecorp.org*

has a DANE portal user account

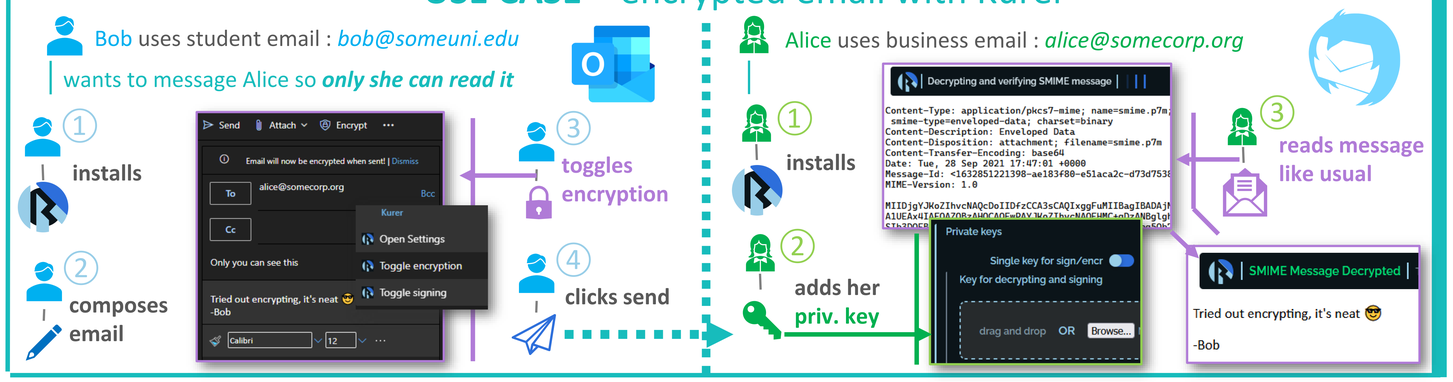


④ Secure Email — Augmented with — Human-usable S/MIME + DANE

kurer — Open-source add-on for popular MUAs

Outlook (Web/Client) and **Thunderbird**
- **S/MIME** signing and encryption
- **DANE** auto cert. discovery

USE CASE – encrypted email with Kurer



Title: **Kurer and DANEportal:**

True Democratized End-to-end Security and Privacy for End-users

Authors: **Tawhidul Minar Islam, Joshua Yuen, Pavan Kumar Dinesh, Tomofumi Okubo, Eric Osterweil**

Affiliation: **Measurable Security Lab, CS Dept., George Mason University**

cyberinitiative.org