Email encryption finally going mainstream

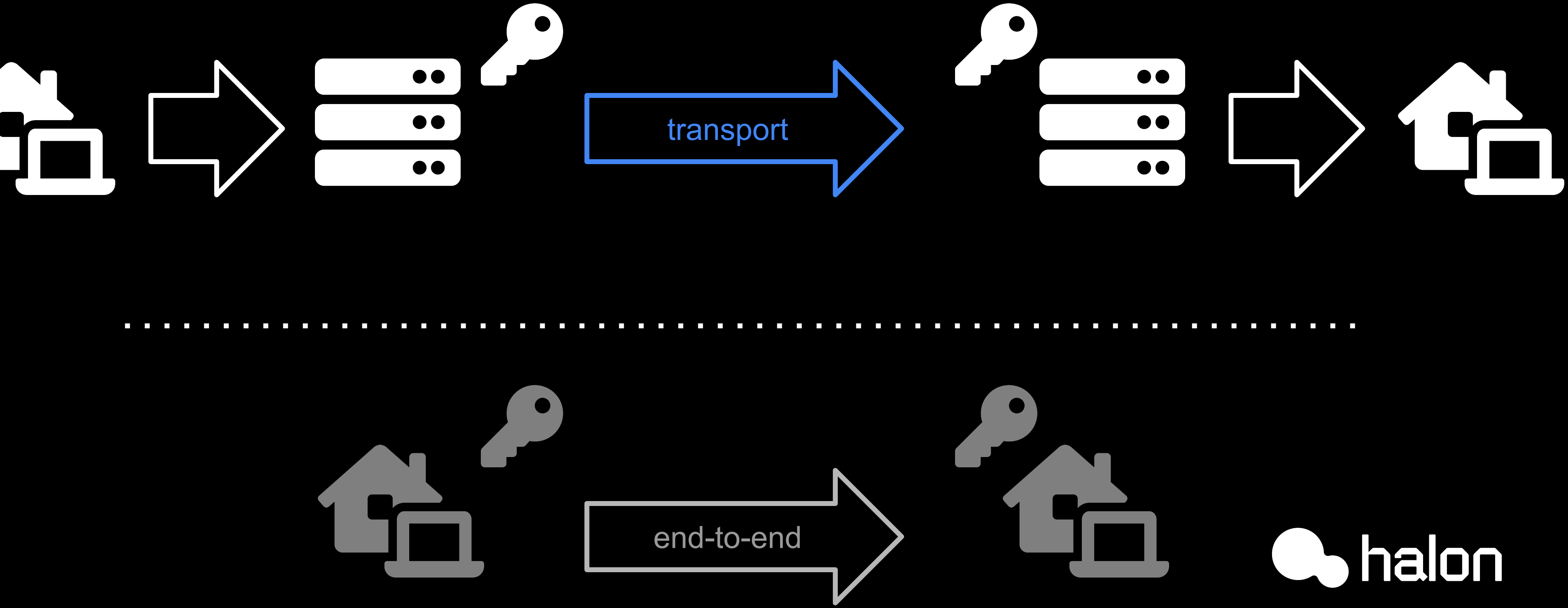
Anders Berggren

Halon Security co-founder

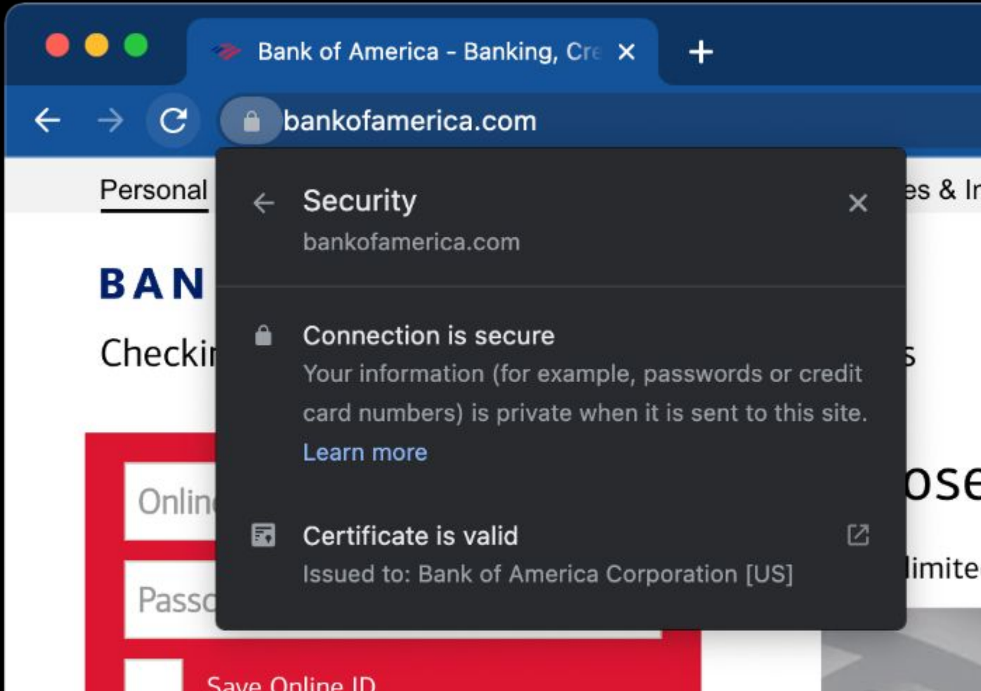
M3AAWG Data & Identity Protection co-chair

halon

Transport encryption for email exchange



TLS, the de-facto transport encryption protocol



Security

bankofamerica.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Issued to: Bank of America Corporation [US]

What’s the problem, we already use STARTTLS for email?

halon

What’s the problem, we already use STARTTLS for email?

- Enforced?
- Authenticated?

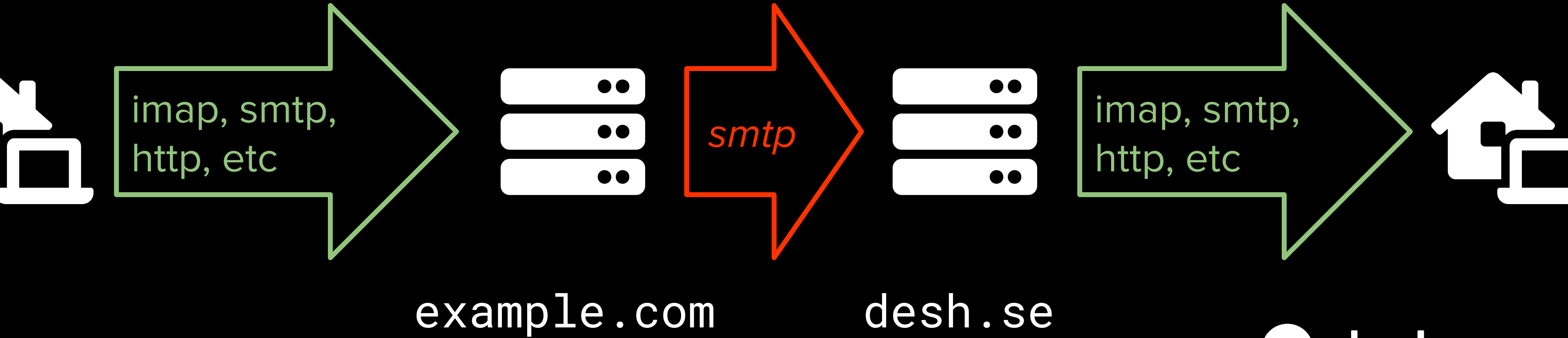
What’s the problem, we already use STARTTLS for email?

● Enforced?	*Downgrade!*
● Authenticated?	*Man-in-middle!*

What's the problem, we already use STARTTLS for email?

Enforced, authenticated TLS

Opportunistic, unauthenticated TLS



halon

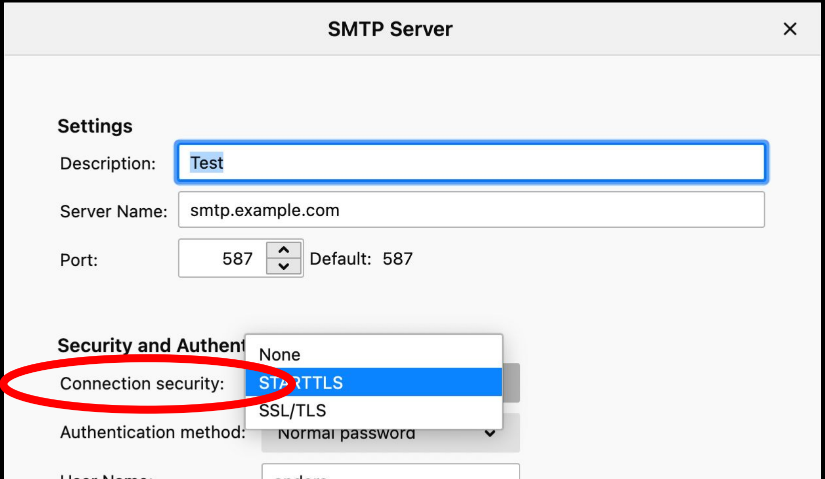
But why wasn’t this solved long ago?

But why wasn’t this solved long ago?

Not as straightforward to implement for email exchange, as for other use cases?

But why wasn’t this solved long ago?

Not as straightforward to implement for email exchange, as for other use cases?



SMTP Server

Settings

Description: Test

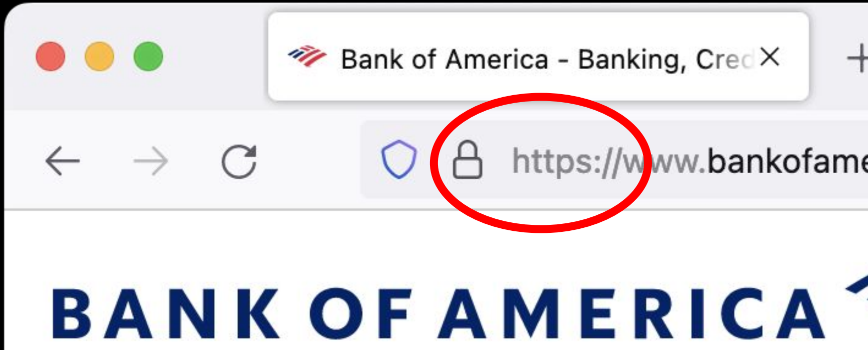
Server Name: smtp.example.com

Port: 587 Default: 587

Security and Authent

Connection security: STARTTLS

Authentication method: Normal password



Bank of America - Banking, Cred

https://www.bankofame

DANE and MTA-STS solves this problem

- Receiving organization (recipient domain) *signals* if TLS should be enforced, and how to authenticate the certificate
- Basically invisible to end-users

DANE and MTA-STS solves this problem

- Receiving organization (recipient domain) *signals* if TLS should be enforced, and how to authenticate the certificate
- Basically invisible to end-users

- **DANE**: using DNSSEC
- **MTA-STS**: using HTTPS and trust-on-first-use

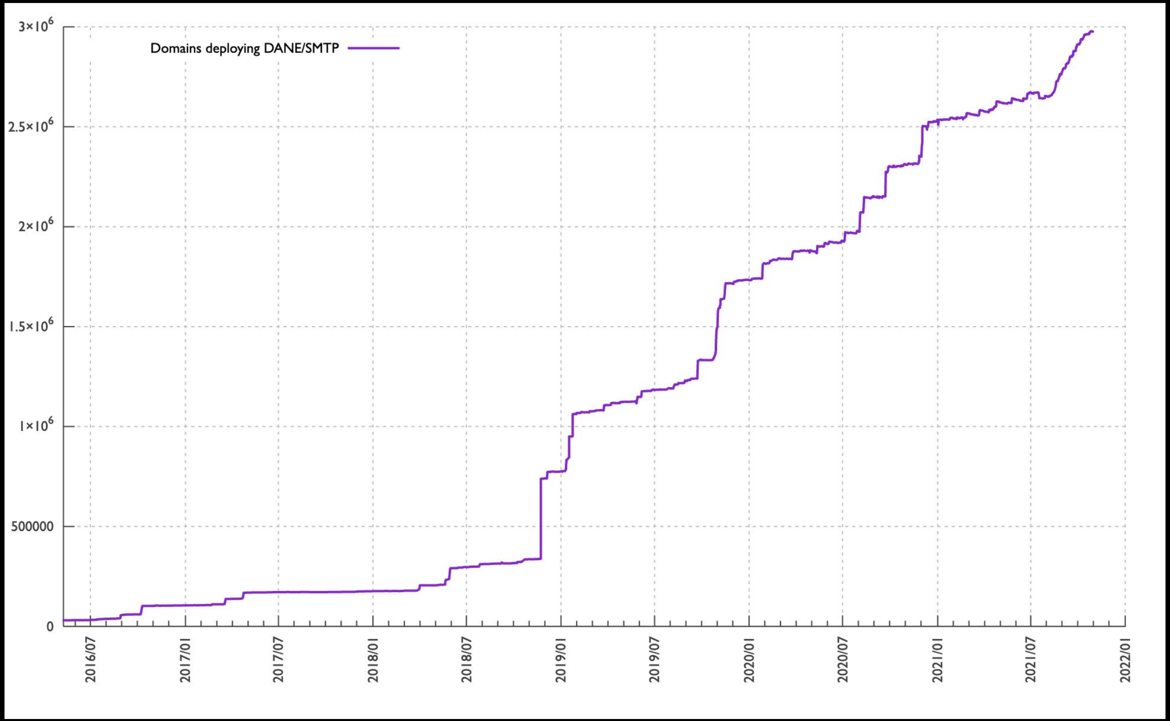
DANE

- Sending
  - Support in all major MTAs, since quite some time
  - Initially some delivery problems due to DNS issues
  - **Should be safe to enable in your outbound MTA**
- Receiving
  - Requires no MTA support, but DNSSEC on domain
  - Can be very convenient for hosters with tons of domains

DANE

```
% dig ietf.org mx +short
0 mail.ietf.org.
% dig _25._tcp.mail.ietf.org tlsa +short
3 1 1 0C72AC70B745AC19998811B131D662C9A...
```

Number of domains with DNSSEC and DANE on MX



https://stats.dnssec-tools.org/

MTA-STS

- RFC in 2018, support in some MTAs
- Doesn’t require DNSSEC; uses trust-on-first-use
  - HTTPS endpoint for each domain
- Enabled for @gmail.com and @outlook/hotmail/live.com

MTA-STS

```
% dig _mta-sts.example.com txt +short
"v=STSv1; id=20211101T010101;"
% curl https://mta-sts.example.com/.well-known/mta-sts.txt
version: STSv1
mode: enforce
mx: alt1.aspmx.l.google.com
mx: alt2.aspmx.l.google.com
mx: ...
max_age: 86400
```

A few best practices

- When using DANE and for example Let’s Encrypt, reuse the key to avoid having to update TLSA RRs
- For DANE key rotation; automate the process, pre-publish TLSAs in advance, and stagger rollovers to avoid single point of failure
- Take a look at RFC 8460 (TLS-RPT) for reporting, and point it at a separate domain
- Make sure you have working contacts in WHOIS, SOA and postmaster@

Some thoughts

- Is DNSSEC the main barrier for adoption?
  - Monetary incentives for registrars seem to drive adoption?
- What’s the overall, global attitude towards DNSSEC?
  - Fear of “going dark” because of misconfiguration?
  - mx1-4.smtp.goog are signed, DANE on the radar?
- Will “dual-stack” verification with both DANE and MTA-STS be the norm?

halon

Questions?

NOT SURE IF WE DID A GREAT JOB...
...OR NO ONE PAID ATTENTION
makeameme.org

halon