TAMPEREEN TEKNILLINEN YLIOPISTO

Consider it DANE

Joona
Kannisto
TUT

DNSSEC and DANE?

- DNSSEC authenticates DNS records
  - Secure binding between name and IP
- DANE binds TLS certificates and keys to service names (TLSA record type)
  - Authentic self signed certificates, restrict allowed CA certs, TLS exists in this port…
- Authenticating names, not a trustworthiness assesment – Not replacing CAs then?

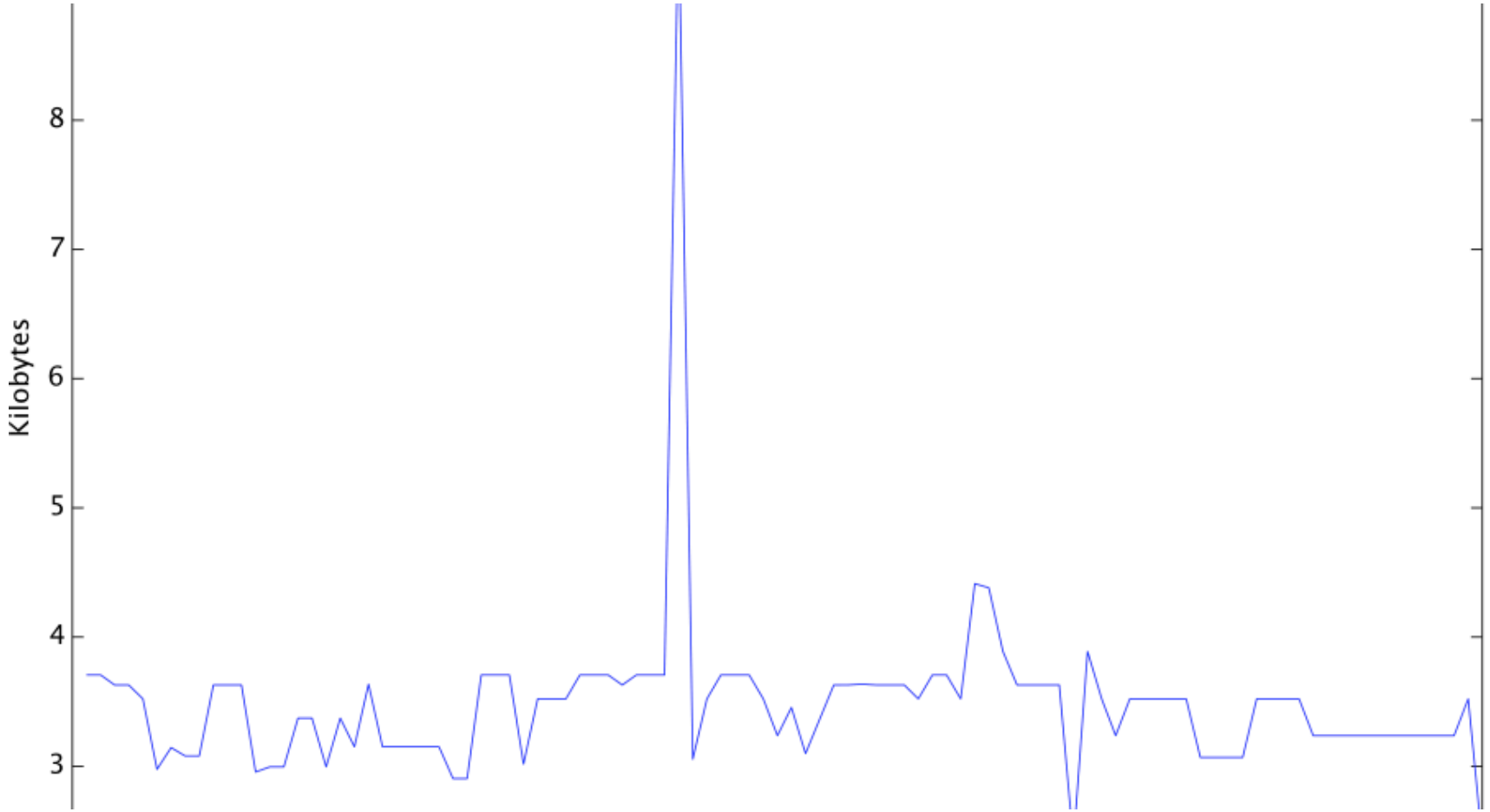
State of DANE?

- Resolver side and clients:
  - For HTTPS there is not much application support available
  - For SMTP already an option
  - Others: IPsec, S/MIME, SSHFP
- Authoritative servers:
  - Requires DNSSEC trust chain

Issues?

- Mother should I trust the resolver?
  - Verify that bit!
- New ways to hick up
  - For instance, signzone default expiry 30d
- The security properties of DNS change drastically
- Amplification?
- One root to rule them all?

Certificate Sizes



Do you see a pattern here?