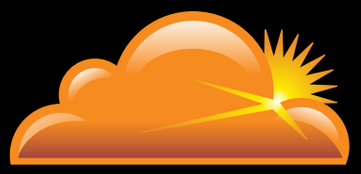


CLOUDFLARE®

Adding new DNSSEC algorithms: reality check

Ólafur Guðmundsson olafur at CloudFlare dot com

Disclaimer: we have done this

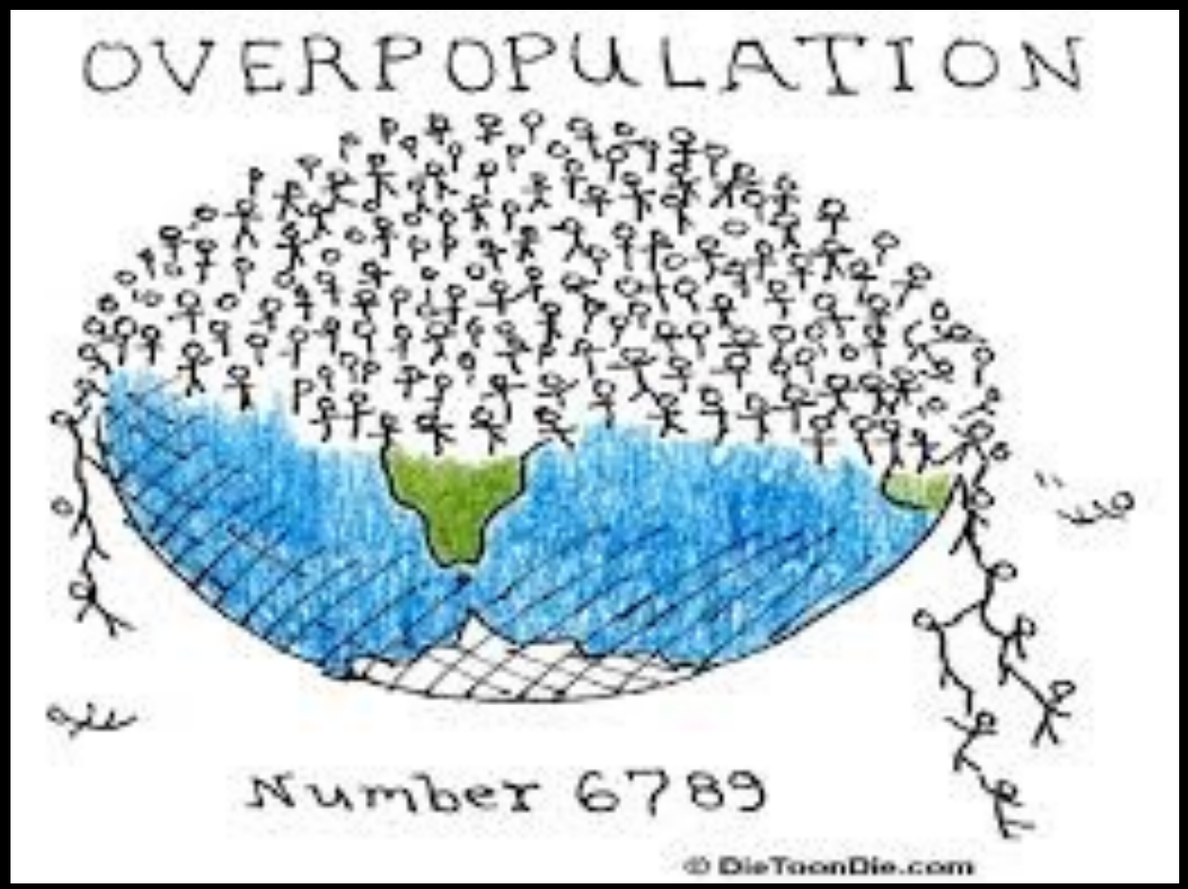
- First major DNSSEC user of ECDSA P256
- Working on getting others to support it
- ICANN Registration model is defective

Simple DNS world view

- DNS consists of
  - Authoritative servers: like KNOT, NSD, BIND…..
  - Resolvers: like BIND, Unbound, …..
  - Clients: Applications and stub resolvers

Zone files are last century

- Provision systems include more than emacs/vi/SubLime/ …
- Alternatives
  - scripts
  - UI/API to DB
  - Dynamic update
  - EPP
  - Calculated answers



Non DNS factors

- DSP says what is allowed in DS
- Software is not maintained
- HSM does not support
- Management does not provide resources
- No benefit to support new stuff
- Not our problem

Crypto timeline

- Algorithm proposed: year 0
- Algorithm gains traction: year 7+
- Algorithm gets standardized by IETF: year 10+
- Algorithm included in libraries: year 2-12
- DNSSEC specification: after IETF standard
- Release cycles for DNS software: 2+ years
- Release cycle for: DNS stuff ==> what release cycle?

Think hard before adding

- Getting everyone's attention is hard
- Motivating for limited benefit change is HARDER
- Stop assuming that people know what they are doing
- Ignore naysayers

Change is possible

- Only once in a while
- Assume it will take time
- Show benefits upfront
- Educate people that there will be “regular” changes

TODO's

- No vanity algorithms
- Educate people about deployment costs of algorithms
- Retire old ones
- Better tools to measure what is validated