How we made DNSSEC simple(r)

RIPE DNS WG

Brett Carr

NOMINET

DNSSEC primer

- Public keys published in zone.
- Private keys need to be protected.
- Rapidly updated zones need constant signing.
- If signing breaks updates stop.
- Classed as a critical top tier service.

DNSSEC at Nominet
A potted history

- 2008 initial infrastructure deployment
- 2009 we first signed .uk
- 2011 we had a small issue ☺
- 2013 changed infrastructure
- 2014 we started signing gtlds
- 2016 Changed infrastructure

Helping Daddy to fix the Internet (or some such thing).

DNSSEC Tech used 2009

- Sun SCA6000 HSM and Centos 5
- opendnssec signing automation
- Sites in Oxford and Kent
- Unreliable
- Failure caused 2011 Issue
- Taken over by Oracle – Price Hike
- Support split between two companies

DNSSEC Tech used 2013

- Thales HSM Network based
- Opendnssec signing automation
- Sites in Slough and West London
- Reliable but Complex and difficult to support.
- Support split between two companies

2016- New DNSSEC

- No HSM
- All signing is done on a geographically replicated VM with BIND.
- Supported by one company (ISC)
- Private Keys on encrypted partition protected by a split password.
- Split password intervention needed at boot.
- Access to machine is XFR and console only. (no ssh)
- Console login protected by split password.
- All changes done by engineer and monitored by a security officer.

2018 Brett is less stressed

Questions ?