How we made DNSSEC simple(r)

24.10.18
Brett Carr

NOMINET

DNSSEC at Nominet

- NO STATS

DNSSEC at Nominet
A potted history

- 2009 we signed .uk
- 2011 we had a small issue ☺
- 2014 we started signing gtlds

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

DNSSEC Tech used

- 2009 SCA6000 opendnssec
- 2013 Thales netHSM opendnssec
  Both Complex and difficult to support
- 2016 New simpler solution (next slide)

2016- New DNSSEC

- No HSM
- All signing is done on a geographically replicated VM with BIND.
- Supported by one company (ISC)
- Keys on encrypted partition protected by a split password.
- 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