



nominet[®]

The DNSSEC debate in .uk

Cath Goulding

Head of Information Security

Background

- .uk zone signed in March 2010
- Second level .uk domains in May 2011
- Registry systems accepted DS records in May 2011

- Outreach
 - Marketing campaigns
 - Individual briefings
 - A free signing service
 - UK Gov support (but not implemented in .gov.uk!)

- Very poor uptake so far

Update 2013 (Direct .uk)

- Consultation regarding opening up second level domain registrations
- Contained a number of security 'features'
 - Malware scanning/monitoring of domains (mostly websites)
 - A trustmark for websites
 - Increased validation/verification
 - Mandatory DNSSEC
- Not transitory (continue to support existing 10 million domains primarily in .co.uk)
- Consultation ran from August 2012 to Jan 2013
- Feedback extensive and varied
 - See <http://www.nominet.org.uk/news/latest/update-directuk>
 - Or chat to me later

Security feedback

- Security could be summed up as “it’s generally a good thing but don’t bundle it with Direct .uk”
 - Malware scanning – *should be optional*
 - Trustmark – *fairly universally disliked*
 - Increased validation – *seen as a good thing*
 - DNSSEC - *seen as a good thing*
- Conclusion
 - Open up .uk with increased validation and mandatory DNSSEC???

Spotlight on DNSSEC

- How risky is the proposal?
- DNSSEC is technical – does everyone understand/appreciate/care?
- It doesn't solve all security issues
- It isn't visible to consumers – no perceived benefit
- Nominet will be blamed regardless for all future DNSSEC incidents in .uk
 - *Regeneration of crypto sigs*
 - *Caching of old DNSKEYs in the DNS*
 - *Stale trust anchors in legacy DNSSEC validators*
 - *Synchronisation of DS records and DNSKEYs*
 - *Transferring process of domains between registrants/registrars*
- The debate continues...