DNSSEC Key Algorithm Rollover

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
14. 10. 2010

cz nic
cz domain registry

DNSSEC Key Algorithm Rollover

- Exchange the keys and their algorithm
- RFC4641bis 4.1.5
  - Draft (-04)
- 5 step process
  - Timing needed
  - Parent-child interaction

Key rollover in the detail

1) Add new RRSIGs (and wait for TTL time)
2) Add new DNSKEY(s) (and wait...)
3) Exchange DS records (and wait...)
4) Remove old DNSKEY(s) (and wait...)
5) Remove old RRSIGs (and wait...)
6) Switch from NSEC to NSEC3 (done)

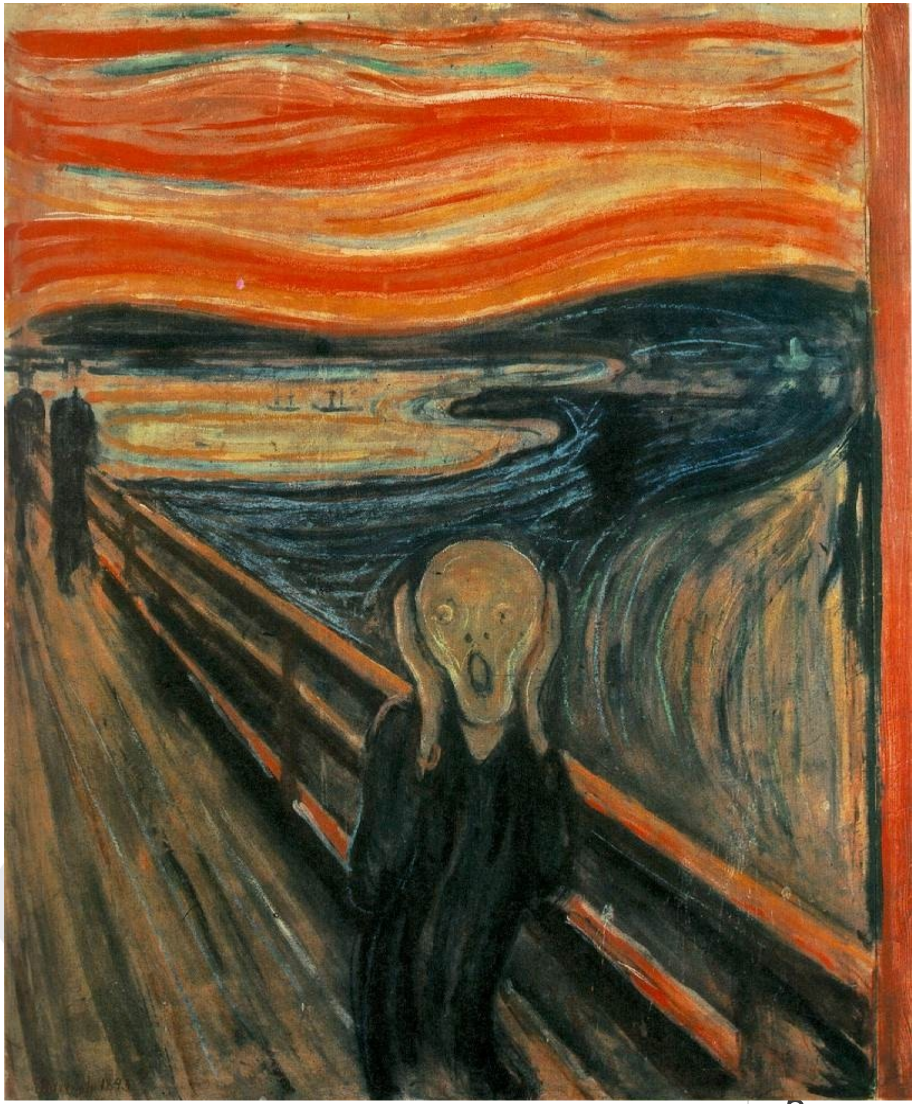
Reasons for rollover

- “Political”
  - Prevent zone walking
    - Zone + whois data
    - “Privacy” breach
- Administrative
  - Root zone signed
    - Align with root zone algorithm
    - Push resolvers to use root zone key

- Technical
  - SHA1 (almost) deprecated
    - Known crypto attacks
    - Although DNSSEC should be fine
  - SHA2 recommended
  - Test the process of the rollover

Our experience

- Testing environment
  - Replicated .CZ setup
    - Fake authoritative servers
    - Resolvers to test
  - Theory != Praxis :)
  - Not perfect
    - But improved during the testing



Problems, pitfalls and bugs

The pitfalls and traps (1)

1) Add new RRSIGs (and wait for TTL time)

- Problem
  - RRSIGs size double
  - Zone size grows (again)
- Resolution
  - Just throw in more memory

The pitfalls and traps (1)

1) Add new RRSIGs (and wait for TTL time)

2) Add new DNSKEY(s) (and wait...)

- Problem
  - RFC 4035 Section 2.2

    There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY Rrset.
- Results
  - Bind 9 – works (more tolerant, but not compliant)
  - Unbound – returns BOGUS (compliant)

The pitfalls and traps (2)

3) Exchange DS records (and wait...)

- Problem
  - RFC 4035 Section 2.2

    The apex DNSKEY RRset itself MUST be signed by each algorithm appearing in the DS RRset located at the delegating parent (if any).
- Results
  - Not tested yet, but I would be careful :)

The pitfalls and traps (3)

4) Remove old DNSKEY(s) (and wait...)

- Problem
  - Bind Bug #22309
    - RSASHA1 → SHA256
    - SHA256 → SHA512
  - Remove the “old” key
    - Bind returns INSECURE (no AD bit)
- Result
  - Insecure secured domains for a short period of time
  - Replicated in the lab, awaiting solution from ISC

The pitfalls and traps (4)

5) Remove old RRSIGs (and wait...)

6) Switch from NSEC to NSEC3 (done)

- Problem
  - No (known) problems here

Lessons learnt

- Test before you do anything
- Then test again :)
- Implementations differ
  - Test with different implementations and version
- Don't underestimate planning
  - Precise timing is needed
    - If you want to make it painless

Questions?