

From NSEC to NSEC3

CZ.NIC - <http://www.nic.cz>

Ondrej Filip / ondrej.filip@nic.cz

Dec 6 2010, Cartagena, Colombia

ccNSO Tech Day



Short history of DNSSEC.CZ

- April 4, 2008 - ENUM (0.2.4.e164.arpa) zone signed – first signed ENUM
- September 2, 2008 – .CZ signed
- September 30, 2008 - .CZ open for end-user public key registration (DS records)
- Started with NSEC – NSEC3 not deployed that time
- Consultation with Personal Data Protection Office
- July 15, 2010 – root zone signed

Reasons for the rollover



- Current key published 2 years ago
- Administrative
 - Zone walking
 - Data mining (whois)
- Technical
 - SHA-1 not recommended any more
 - Known cryptographic attacks
 - SHA-2
 - Recommended by NIST for next years
- Side effect – awareness increase

NSEC3



- About 15% of Czech domains signed
- (109k of 741k)
- We expect more to come
- NSEC3 with OPT-OUT would not reduce zone file size in the future
- “pure” NSEC3 chosen

Key algorithm rollover



- Different from simple key rollover
- Complex process
 - Exact timing (Aug 3 – Aug 24) + preparation phase
 - Exact order of the steps
 - Check RFC4035 2.2 – algorithm downgrade protection
- Thorough testing environment
 - Replicated setup in the lab
- And also first tested on ENUM

Steps for the change



- RFC4641bis
 - <http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis>
 - Section 4.1.5 – Key algorithm rollover
- Signature for every algorithm in zone apex!
- You cannot use key prepublishing
- Key with the algorithm for every algorithm in DS
- Double signed zones

Rollover in detail



- 1) Generation of new keys + preparation of DNS infrastructure, communication with resolver operators (root, algorithm)
- 2) Add new RRSIGs (and wait for TTL time)
- 3) Add new DNSKEY(s) (and wait...)
- 4) Exchange DS records (and wait...) - 2 days in root zone, removal from ITAR – 14 days, DLV tied with ITAR
- 5) Remove old DNSKEY(s) (and wait...)
- 6) Remove old RRSIGs (and you're done)

DNS servers differ



- Bind 9 is more tolerant
 - Can cope if there are keys, but no signatures
 - No AD bit between steps 5 and 6
- Unbound is stricter
 - Adhere to the standards
 - Adding a DNSKEY with new algorithm and without signatures - causes validation failures

Lessons learnt



- Test, test, test... and test...
- Implementation details differ...
 - So test with different implementations and versions
- Timing is crucial
 - Do rehearsals
- Plan you DNS infrastructure properly - sufficient memory
 - More than twice of current consumption

Thank you

Questions?

Ondrej Filip

ondrej.filip@nic.cz

<http://www.dnssec.cz>