Jak vyměnit klíč k Internetu?

Ondřej Surý • ondrej.sury@nic.cz • 13. 10. 2015

CZ.NIC | SPRÁVCE DOMÉNY CZ

The Internet

Root Zone Key Signing Key

- Vstupní bod důvěry do DNSSECu (Trust Anchor)
- V provozu od července 2010
- RSASHA256 (2048b) (id = 19036)
  - Síla odpovídá přibližně ~100b symetrické šifry
  - Zvýšení složitosti == zvýšení velikosti DNS odpovědí
- Uložený v Hardware Security Module
  - Pravidelné ceremonie podepisování ZSK
  - Nedávno proběhla výměna hardware

Root KSKR Design Team

- Root Zone Partners
  - ICANN (KSK)
  - Verisign (ZSK)
  - USG DoC NTIA
- Dobrovolníci
  - Joe Abley, Dyn, CA
  - Jaap Akkerhuis, NLNetLabs, NL
  - John Dickinson, Sinodun, UK
  - Geoff Huston, APNIC, AU
  - Ondřej Surý, CZ.NIC, CZ
  - Paul Wouters, No Hats/Red Hat, NL
  - Yoshiro Yoneya, JPRS, JP

Root Zone KSK Rollover Plan

- Cíle dokumentu
  - Návrh postupu při výměně KSK
  - Technická, provozní, kryptografická, a komunikační doporučení
  - Zhodnocení dopadů změny KSK
- Co není obsahem?
  - Zda-li klíč měnit nebo ne
  - Zone Signing Key
- Draft verze dokumentu – 6. srpna 2015
  - Možnost se vyjádřit k draftu do 5. října 2015
  - https://www.icann.org/public-comments/root-ksk-2015-08-06-en
- Finální verze dokumentu – do konce roku 2015

Vybraná doporučení

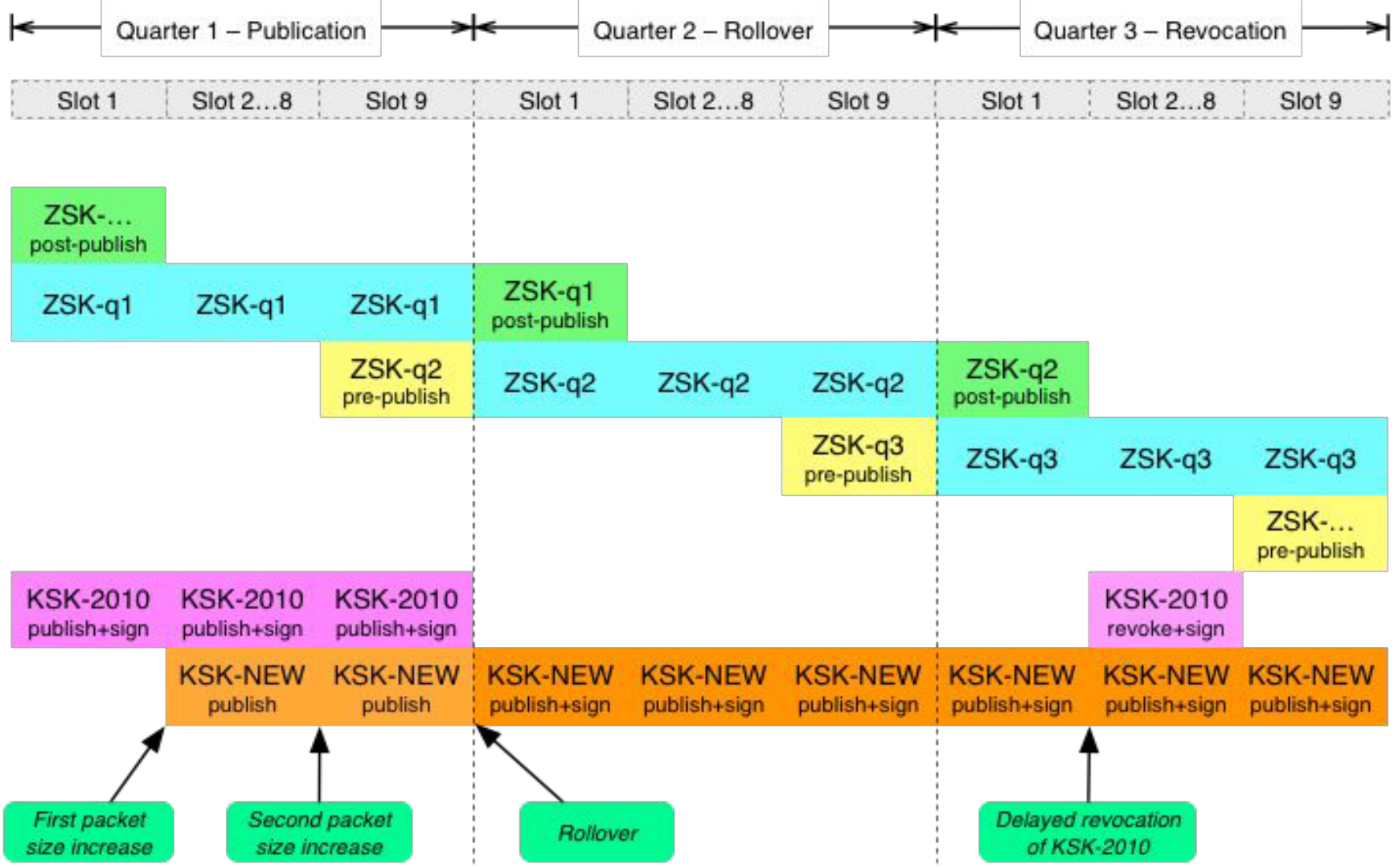
Výměna KSK by neměla mít významné dopady na existující mechanizmy správy KSK, aby nebyla snížena důvěryhodnost procesu správy KSK

ICANN by měl identifikovat výrobce DNS serverů, operačních systémů a integrátory DNS řešení a úzce s nimi spolupracovat při výměně TA

ICANN by měl vydat doporučení, jak řádně ověřit správnost TA a jak s ním řádně pracovat

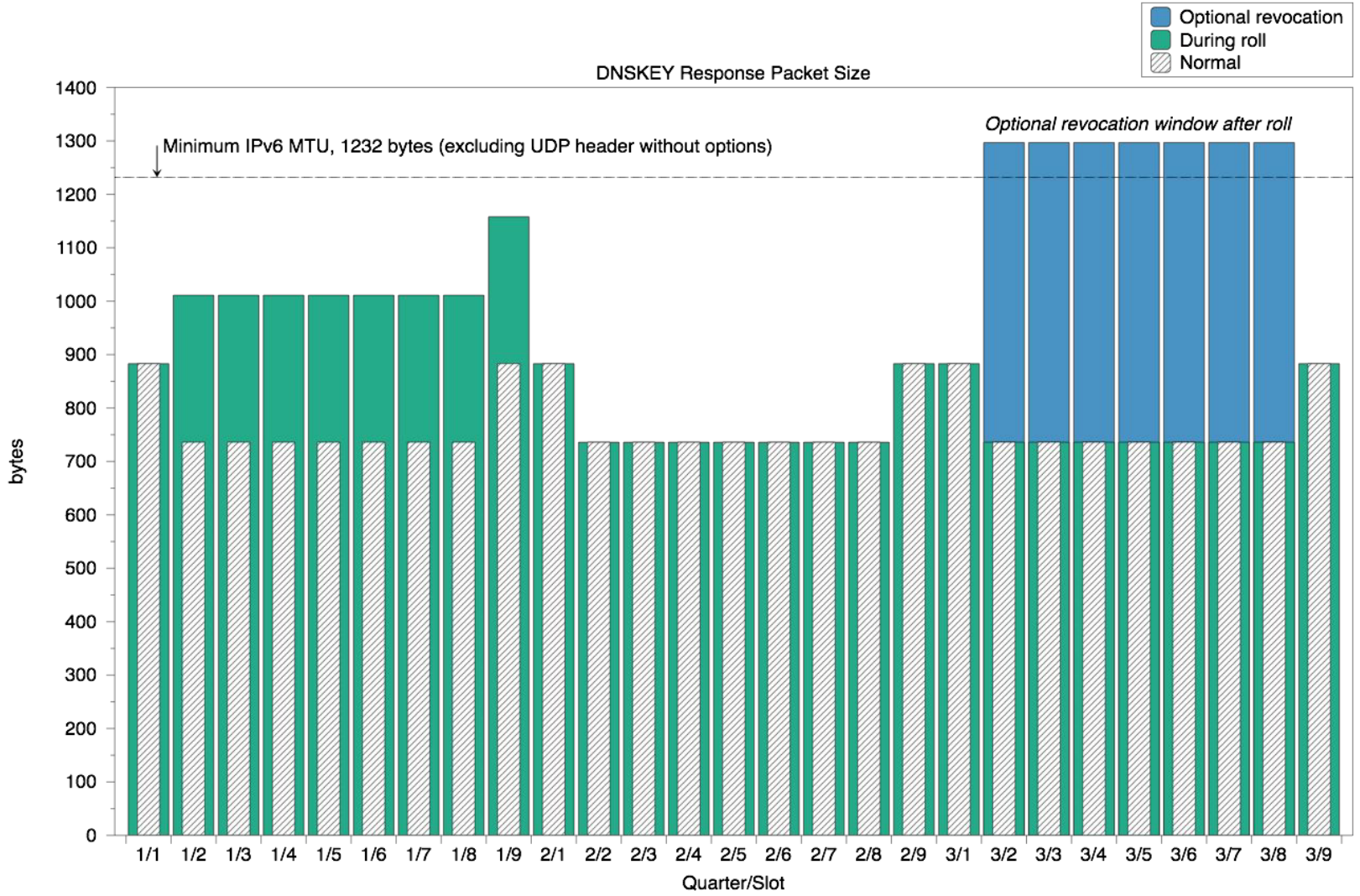
Výměna Root KSK by se měla řídit postupem popsaným v RFC 5011

Všechny změny v DNSKEY RRSetech musí být zarovnány na 10. denní sloty popsané v *DNSSEC Practice Statement for the Root Zone KSK Operator*


Quarter 1 – Publication
Quarter 2 – Rollover
Quarter 3 – Revocation
Slot 1
Slot 2…8
Slot 9
Slot 1
Slot 2…8
Slot 9
Slot 1
Slot 2…8
Slot 9
ZSK-…
post-publish
ZSK-q1
ZSK-q1
ZSK-q1
ZSK-q1
post-publish
ZSK-q2
pre-publish
ZSK-q2
ZSK-q2
ZSK-q2
ZSK-q2
post-publish
ZSK-q3
pre-publish
ZSK-q3
ZSK-q3
ZSK-q3
ZSK-…
pre-publish
KSK-2010
publish+sign
KSK-2010
publish+sign
KSK-2010
publish+sign
KSK-2010
revoke+sign
KSK-NEW
publish
KSK-NEW
publish
KSK-NEW
publish+sign
KSK-NEW
publish+sign
KSK-NEW
publish+sign
KSK-NEW
publish+sign
KSK-NEW
publish+sign
KSK-NEW
publish+sign
First packet size increase
Second packet size increase
Rollover
Delayed revocation of KSK-2010

UDP/IP Fragmentace

- IP fragmenty jsou identifikovány pouze 16-bitovým ID (IP-ID)
- Integritu UDP paketu zajišťuje jednoduchý 16-bitový checksum
- DNS hlavička je pouze v prvním fragmentu
- S MTU můžeme manipulovat i jako off-path útočník (src-ip spoofing)
- Popsán útok na DNS pomocí UDP fragmentace (Herzberg & Shulmanová)
  - Stačí uhádnout IP-ID (a např. CGN nám práci dost zjednodušuje)
  - Dopočítat UDP checksum (což není složité, protože známe obsah)
  - http://arxiv.org/pdf/1205.4011v1.pdf
- Fragmentaci je potřeba se vyhnout!!!
  - Minimální IPv4 MTU: ?? (RFC 791) → na Linuxu je minimální MTU == 552
  - **Minimální IPv6 MTU: 1280** ← útok přestává být realizovatelný


Optional revocation
During roll
Normal
DNSKEY Response Packet Size
Optional revocation window after roll
Minimum IPv6 MTU, 1232 bytes (excluding UDP header without options)
bytes
1400
1300
1200
1100
1000
900
800
700
600
500
400
300
200
100
0
1/1
1/2
1/3
1/4
1/5
1/6
1/7
1/8
1/9
2/1
2/2
2/3
2/4
2/5
2/6
2/7
2/8
2/9
3/1
3/2
3/3
3/4
3/5
3/6
3/7
3/8
3/9
Quarter/Slot

Nový KSK má zachovat existující algoritmus a velikost soukromého klíče RSASHA256 (2048b)

Nicméně volba algoritmu má být pro další výměnu KSK zrevidována

Eliptické křivky – proč ne?

- RSA2048 by mělo být stále bezpečné pro následujících pět let
  - Pokud nedojde k významnému pokroku ve faktorizaci velkých čísel
- (Minimálně) Unbound vyžaduje podpis oběma algoritmy (dual signing)
- ECDSA
  - Poměrně nový standard – pro DNSSEC standardizováno v roce 2012
  - NIST P-224, 256 a P-384 mají některé špatné vlastnosti – viz http://safecurves.cr.yp.to/
  - Podpora ECDSA v DNSSECu je menší než podpora RSASHA256
- cfrg WG pracuje na nových doporučených křivkách
  - ed25519 a ed448 (goldilocks)
  - https://tools.ietf.org/html/draft-irtf-cfrg-curves
- Následně je zapotřebí implementace těchto křivek pro DNSSEC
  - https://tools.ietf.org/html/draft-sury-dnskey-ed25519
  - https://tools.ietf.org/html/draft-sury-dnskey-ed448 (?)

...a další...

(draft) KSK Rollover má začít v průběhu roku 2016, změny v DNSKEY RRSetu mají začít v lednu 2017, což znamená, že se nový KSK začne používat v dubnu 2017

Děkuji za pozornost

Ondřej Surý • ondrej.sury@nic.cz • 13. 10. 2015

CZ.NIC | SPRÁVCE DOMÉNY CZ