Root KSK Rollover Wrap-up

João Damas for the DNS WG chairs

Why?

Why, oh why, was a key roll necessary?

ICANN DPS (https://www.iana.org/dnssec/icann-dps.txt)

6.5. Key signing key roll-over

Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

Timeline

- First attempt at rolling 11 Oct 2017.

- Postponed until there was a better understanding of signalled issues (was 1 year)

  - New KSK remains published in the root zone

- KSK rolled on 11 October 2018

- revoked on 11 January 2019

Observations

- There is still a shortage of reliable data regarding what is available in resolvers and what impact resolver failure may have on end users (who, how many, etc)

- Not everything was smooth even if there are claims that it was.

  - exempli gratia: ISP in Ireland. https://www.rte.ie/news/2018/1013/1002966-eir-outage/

    - ~20% of Ireland's Internet users/ .022% of Internet

What now?

- Have a look at Paul Hoffman's presentation

  https://www.icann.org/sites/default/files/packages/ids-2019/11-hoffman-ksk-10may19-en.pdf

- Mailing list "ksk-rollover": https://mm.icann.org/mailman/listinfo/ksk-rollover

Contribute

Some aspects that have been brought up:

Do we need another roll?

Frequency of future rolls

When to have the next roll

Should the next roll include a change in the key parameters?

algorithm, size, ….?

The floor is yours