DNSSEC in ORG with a dash of COVID

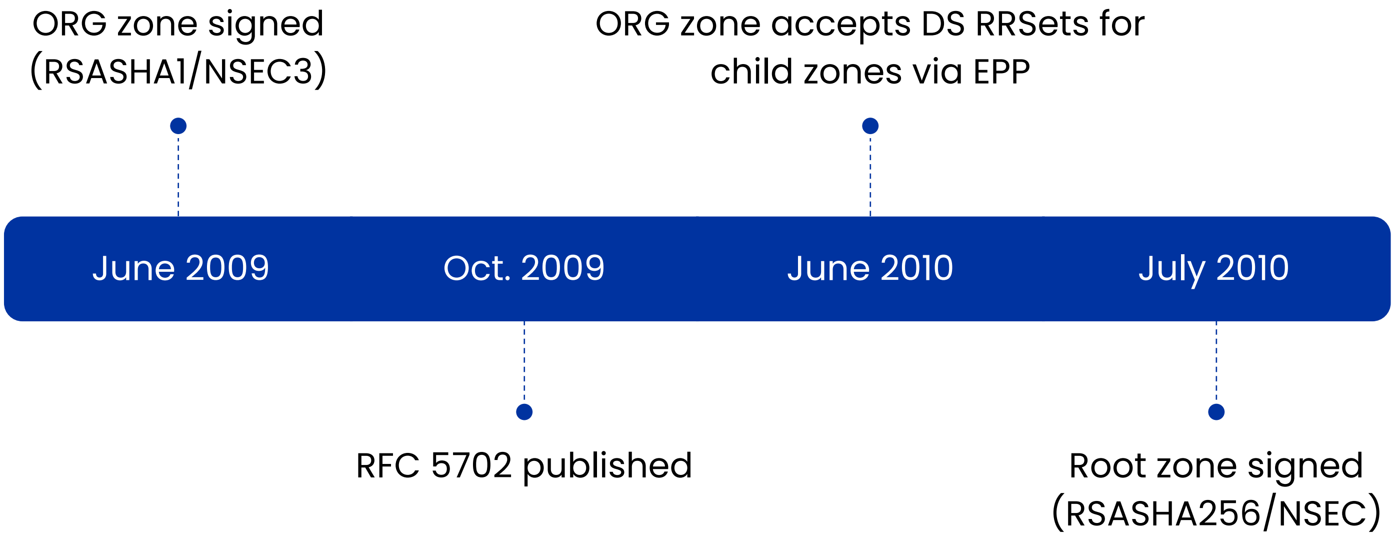
Joe Abley

ccNSO Tech Day

Virtual ICANN 68

22 June 2020

IN OUR LAST EPISODE...



June 2009

ORG zone signed (RSASHA1/NSEC3)

Oct. 2009

RFC 5702 published

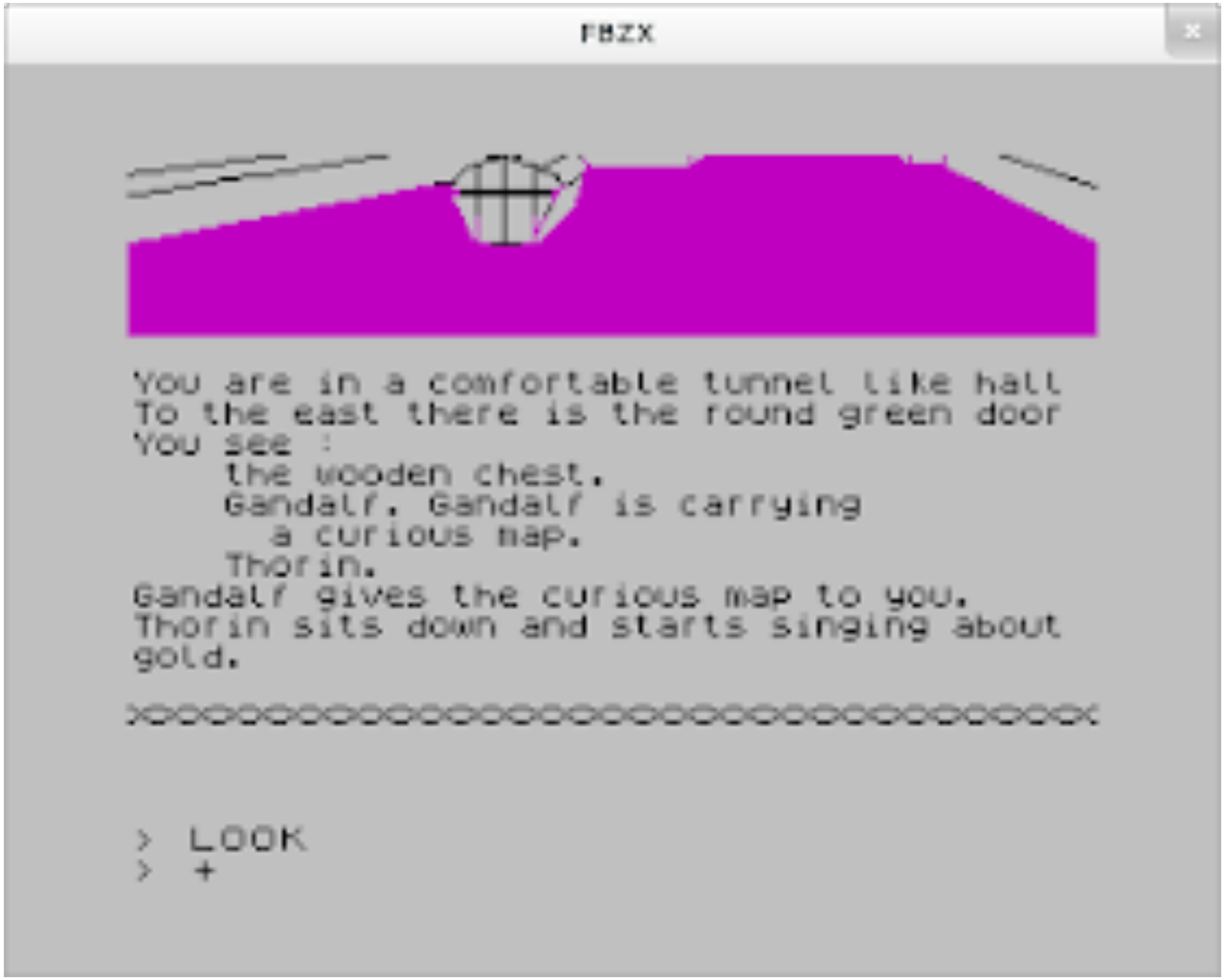
June 2010

ORG zone accepts DS RRSets for child zones via EPP

July 2010

Root zone signed (RSASHA256/NSEC)

TIME PASSES



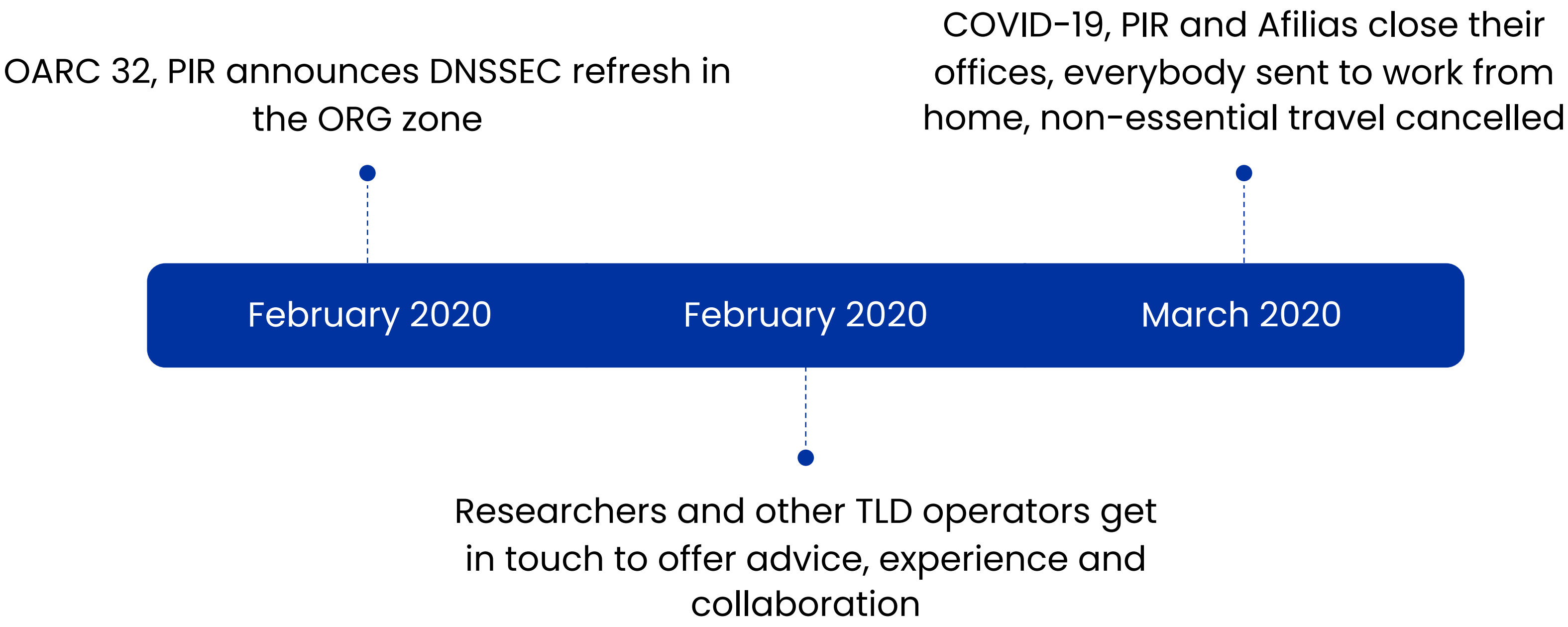
```
You are in a comfortable tunnel like hall
To the east there is the round green door
You see :
     the wooden chest.
     Gandalf. Gandalf is carrying
        a curious map.
     Thorin.
Gandalf gives the curious map to you.
Thorin sits down and starts singing about
gold.

XOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOX



> LOOK
> +
```

IN OUR LAST EPISODE...



OARC 32, PIR announces DNSSEC refresh in the ORG zone

February 2020

February 2020

Researchers and other TLD operators get in touch to offer advice, experience and collaboration

March 2020

COVID-19, PIR and Afilias close their offices, everybody sent to work from home, non-essential travel cancelled

WHAT DID WE WANT TO ACHIEVE?

- **ORG had an enormous DNSKEY RRSet**
  - Enormous enough that some guy called Geoff Huston once wondered aloud on stage in various conferences how .ORG even worked at all *for an entire year* to see if we would react
  - We should really make that smaller…
  - … but we'll wait because we wouldn't want to deprive Geoff of comedic material

- **ORG is signed using algorithm 7 (RSASHA1)**
  - Rijmen, Oswald, "Update on SHA-1" January 2005
  - Wang, Yin, Yu, "Finding Collisions in the Full SHA-1" August 2005
  - Wang, Yao, Yao, "Notes on the Wang et al. 2^{63} SHA-1 Differential Path", August 2005
  - … and many other old-time favourites, including…
  - Leurent, Peyrin, "From Collisions to Chosen-Prefix Collisions – Application to Full SHA-1" April 2019
  - Leurent, Peyrin, "SHA-1 is a Shambles First Chosen-Prefix Collision on SHA-1 and Applications to the PGP Web of Trust" January 2020

- **ORG is signed using NSEC3**
  - Negligible and increasingly unimportant protections against zone-walking
  - Opt-out sections make aggressive negative caching difficult
  - Complicates provisioning since zone size depends on DNSSEC uptake in children

WHERE WERE WE HEADING?

- **ORG had an enormous DNSKEY RRSet**
  - Identify operationally incomplete KSK rolls and complete them
  - Review pre-publication parameters for as-yet unused keys
  - Start lab testing different signer parameters to find out what else we could improve on

- **ORG is signed using algorithm 7 (RSASHA1)**
  - Plausible targets are algorithm 8 and 13
  - All the cool kids are doing algorithm 13 though, and that will help with the DNSKEY response size. Let's do that, we're cool. Algorithm 8 is lame, etc.
  - Start lab testing to find the performance implications of algorithm 7 vs. 8 vs. 13

- **ORG is signed using NSEC3**
  - NSEC is operationally less complicated
  - We're fairly sure we are no longer concerned with the zone-walking problem
  - With 10,000,000 delegations, most of which are insecure, adding NSEC + RRSIG to each one means something like 20,000,000 additional resource records and 10,000,000 additional signatures
  - Start lab testing to find the performance implications of signing the NSECs
  - Start reviewing the edge capacity forecasts for memory footprint

WHO SHOULD WE WORK WITH?

- **Community Engagement**
  - We want to make sure resolver operators are well aware of our plans
  - Let's review the relative differences in the validator population when it comes to 8 vs. 13
  - We should do a bunch of lab testing, and if we're going to do lab testing, we may as well make it a public lab

- **Research Opportunities**
  - ORG might have a more widespread base of dependent validators than the ccTLDs that have rolled to 13; perhaps there are interesting differences, there
  - We don't know for sure, but we think that possibly there hasn't been a production TLD roll from NSEC3 to NSEC, so perhaps that is new and exciting

- **Communications and Data Collection Partners**
  - Started talking to the good people at DNS-OARC about our plans
  - Keith and Matt offered to host a mailing list
  - We started talking about how we might contribute funds to help with data collection exercises, if researchers suggested they were interested in data

BUT THEN OF COURSE

- **Huge performance impact of Algorithm 13 on Existing Signers**
  - The current signing platform in use for .ORG has unoptimized support for ECDSA, and it shows
  - The new signing platform under development for other TLDs that would very likely not have this problem is still, well, under development

- **No Travel**
  - Setting up a lab with new hardware is suddenly much more difficult
  - Crossing borders to increase edge capacity, memory footprints, etc suddenly seems difficult
  - Changes to key management that involve people handling credentials seem unwise, even if they are practical

- **No Universities**
  - Universities all over the planet start closing down and sending their students home
  - Campuses close, courses are suspended
  - Some regional universities have already cancelled lectures through the end of 2021

- **Everybody Suddenly Depends on the DNS Even More than they Used To**
  - Let’s face it, this would be a particularly terrible time for anything to go wrong
  - Critical Critical Infrastructure

THAT WAS MARCH. SURELY APRIL WOULD BE FINE.

keep-calm.net

WHAT *CAN* WE DO THIS YEAR?

- **We can review relevant parameters in the existing signers, like**
  - Key pre-publication strategy
  - Signature lifetimes and zone-wide re-sign intervals
  - ZSK rollover policies
  - TTLs

- **We can test the performance implications of a roll to algorithm 8**
  - We've already done most of this, in fact, and the differences are negligible

- **We can test the robustness of the algorithm rollover in the current signer**
  - We could do this in private and publish the results
  - We could run a public testbed

- **We could do a dry run in some smaller TLDs**
  - While we would take full precautions with *any* TLD, no matter how small, the impact of a problem in a much smaller TLD would be easier to mitigate and would affect far fewer end-users

- **We can do communications, outreach and coordination with researchers**

WHAT *SHOULD* WE DO THIS YEAR?

- **You tell us what you would like to see**
  - If you have experience to share, or
    - Interesting research questions to answer, or
    - Ideas about other things we could do, or
    - Observations about weirdness that you can't explain
  - Please talk to us!

https://lists.dns-oarc.net/mailman/listinfo/org-algorithm-roll

- **Complete a feasibility study for a roll to algorithm 8**
  - This is a much more incremental change than we were anticipating, but perhaps it's a reasonable piece of work that other people considering a move away from SHA-1 might benefit from
  - It's not often that this kind of planning work has such a direct and practical reason to include the kind of disaster scenarios that exist outside the window right now

- **If feasible, complete the roll**
  - We would still love to get this done in 2020
  - We're going to prioritise stability, however, and it's always possible that the risk analysis will indicate that we are better off waiting

STATUS, DRAFT NEXT STEPS

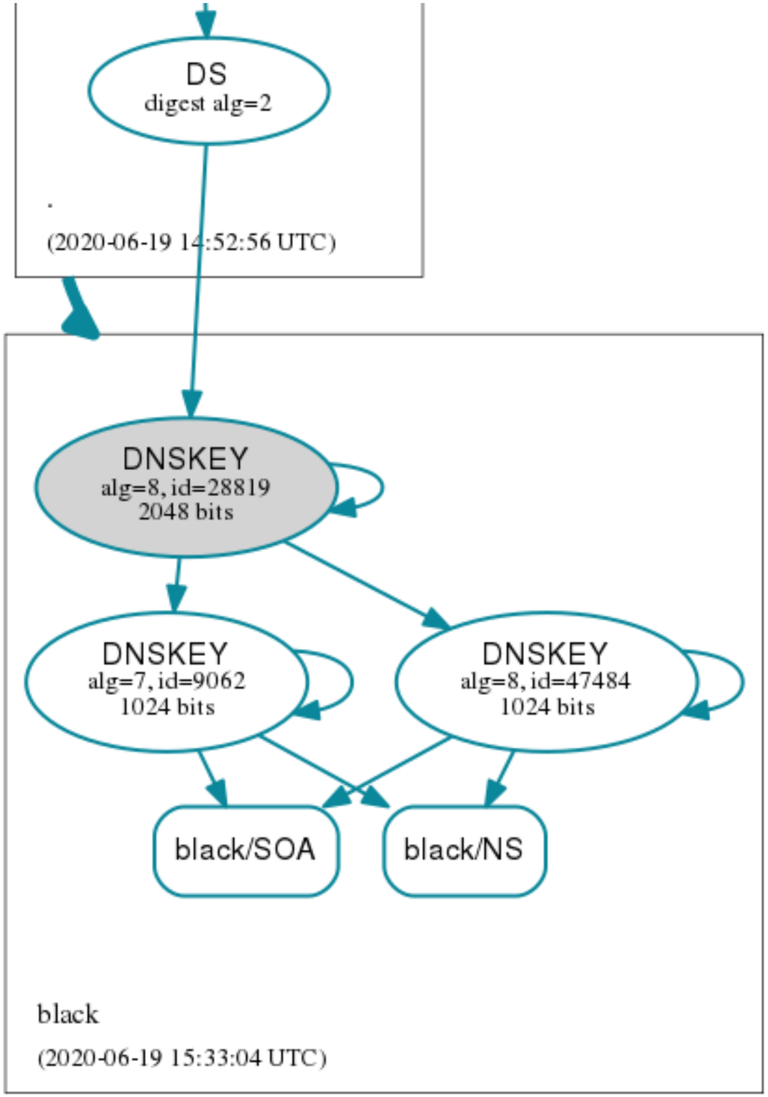
- **We have delivered presentations of this presentation to various audiences**
  - RIPE dns-wg, May 2020
  - DNS-OARC, June 2020
  - ccNSO Tech Day, ICANN 68, June 2020

- **Preparatory Work carried out by our Back-End Registry Services Provider**
  - Indicative results suggesting that a roll from 7 to 8 is feasible
  - Successful Lab testing of a roll from 7-8 using the same signer platform
  - Production roll from 7 to 8 using the same signer platform but for a different, small new gTLD is ongoing but results to date are very encouraging

- **We have around 40 people subscribed to our org-algorithm-roll list**
  - Mainly subscribed following each of the two presentations preceding this one
  - Substantially technical audiences
  - Once the preparatory work described above is complete we expect to start a public conversation about choice of technical parameters, timeline and future outreach efforts

- **We continue to have reasonable confidence that we can complete a roll in 2020**
  - Surely no other global problems can emerge this year, right?

OBLIGATORY DNSVIZ OUTPUT



Questions?

Joe Abley <jabley@pir.org>
Suzanne Woolf <swoolf@pir.org>