DNSSEC Key Rollover

An update from APNIC

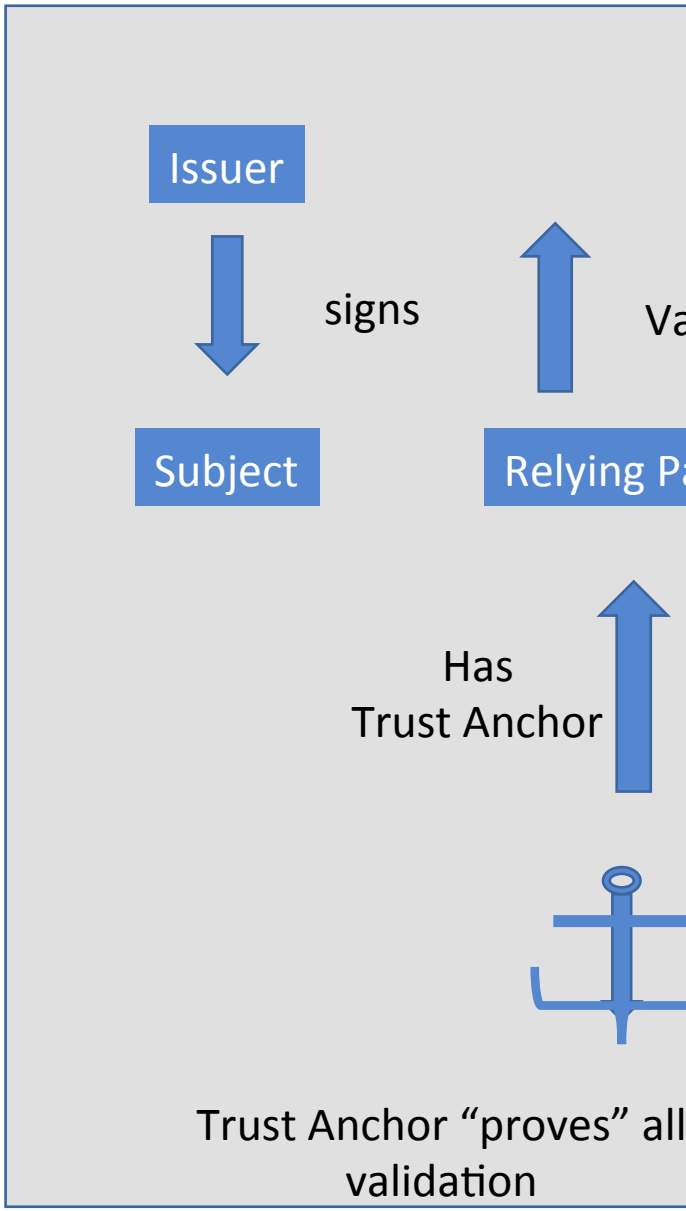
George Michaelson APNIC Labs (ggm@apnic.net)

Why DNSSEC? Because of public trust in names

- Integrity of the name-to-address function now vital
- Significant damage potential, in lying in the DNS
  - Pretend to be banking, finance industry websites, steal keys with phishing attacks and cloned sites
- Loss of service to government and other significant agencies
  - Increasing expectation of delivery of critical public service online
- DNSSEC Protects against “lies in the DNS”
  - Is the zone up to date or is something being hidden from you?
  - Is the label in the zone, or has it been inserted (authenticated denial)
  - Is the response correct or has it been corrupted?
- Wide community benefit from DNSSEC
  - Defence against phishing, exposes MiTM, censorship

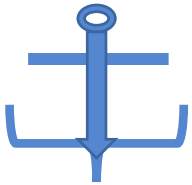
Overview of DNSSEC

- Cryptographically protected DNS responses
- Like X509 Public Key Certificate hierarchy
  - No certificates: just keys and signatures
  - Two kinds of key: Key Signing Key and Zone Signing Key
- Protects against “lies in the DNS”
  - Signatures prove zone is authoritative & correct
  - No additional data can be inserted
  - MiTM attacks can be detected.
- Wide community benefit from DNSSEC
  - Defence against phishing, exposes MiTM, censorship



Roles in DNSSEC

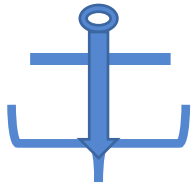
- Zone holders sign
- Resolvers with DNSSEC enabled “validate”



  - Validator called “relying party” in PKI terms have **TRUST ANCHOR**
  - If the DNSSEC fails validation return SERVFAIL
  - If no other DNS resolvers available (or all DNSSEC enabled) then no DNS response
- SIGNER
  - Must keep signatures valid
- Relying party
  - Must have up-to-date trust anchor:

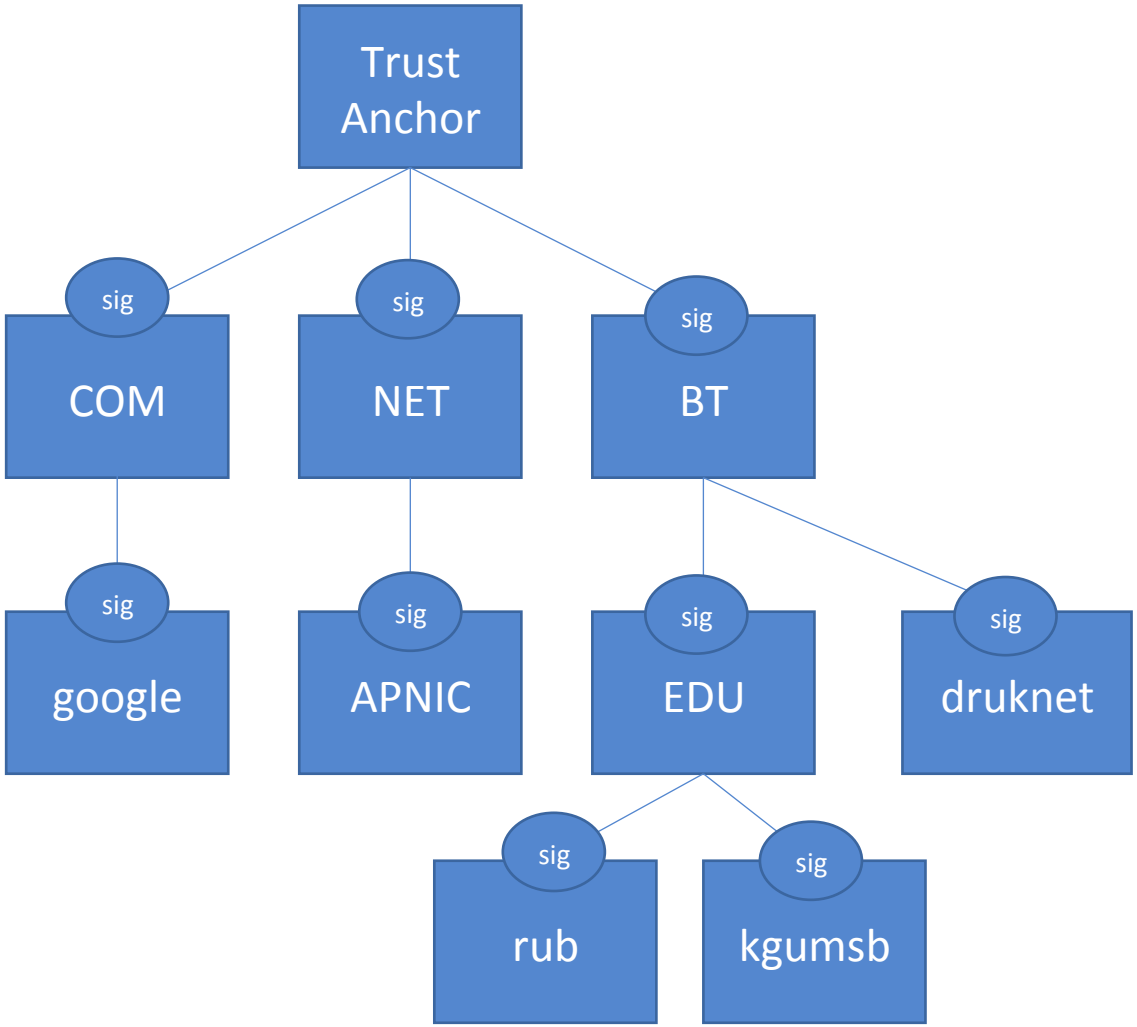
Roles in DNSSEC

- Zone holders sign
- Resolvers with DNSSEC enabled “validate”
  - Validator called “relying party” in PKI terms have **TRUST ANCHOR**
  - If the DNSSEC fails validation return SERVFAIL
  - If no other DNS resolvers available (or all DNSSEC enabled) then no DNS response
- SIGNER
  - Must keep signatures valid
- Relying party
  - Must have up-to-date trust anchor:

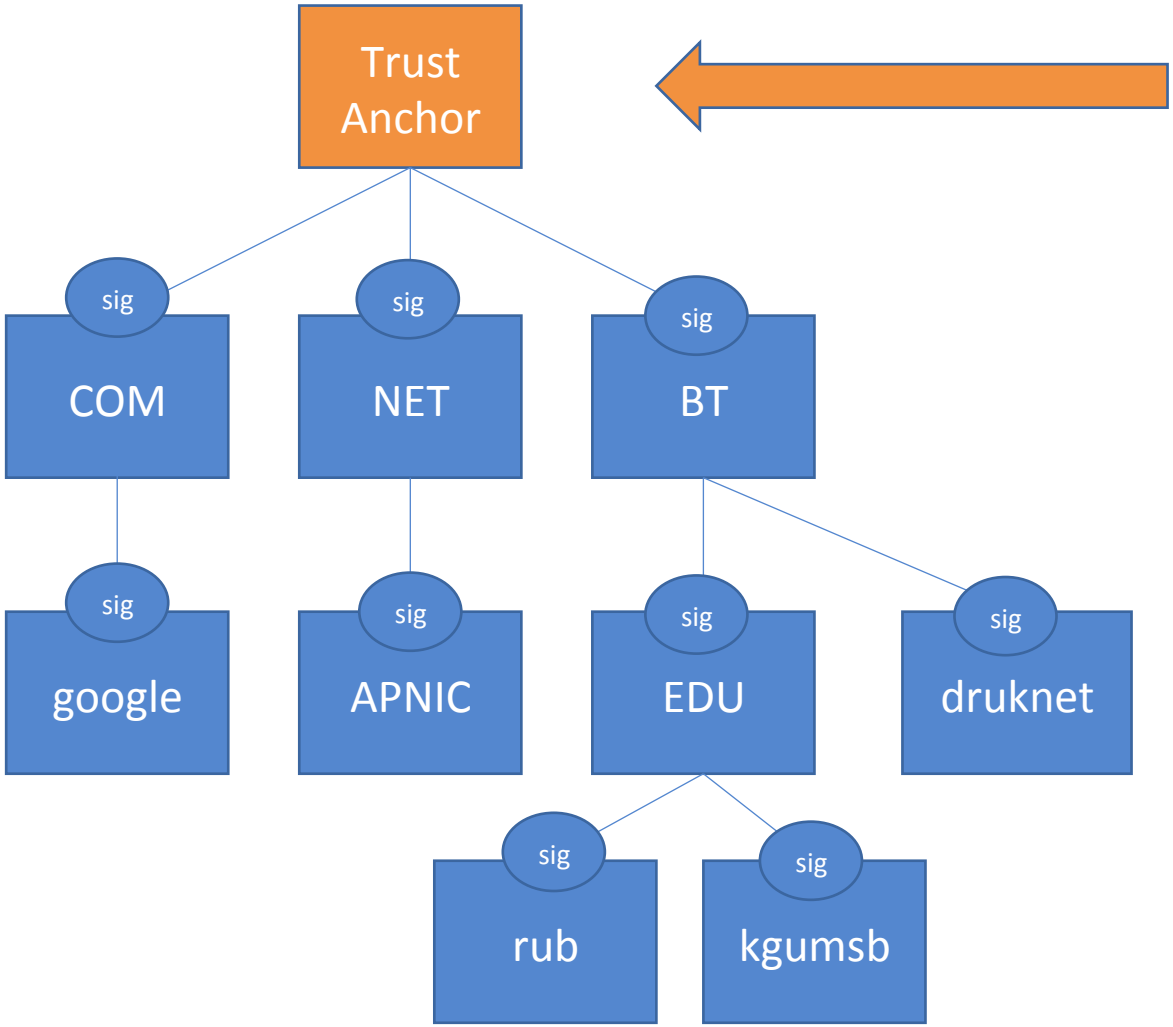


What happens when it changes?

Tree failure at the root is fatal

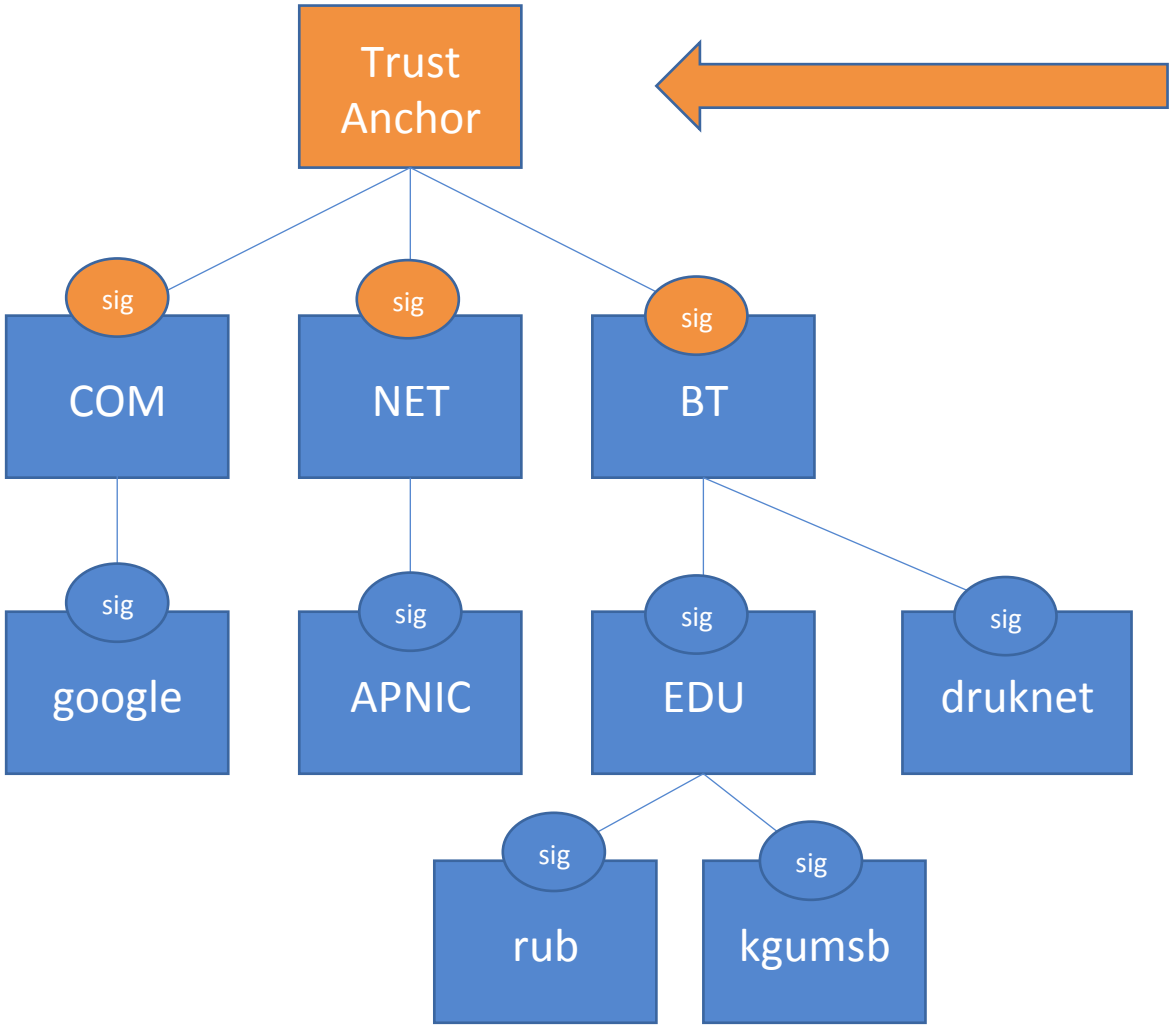


Tree failure at the root is fatal



If this goes stale or out of date…..

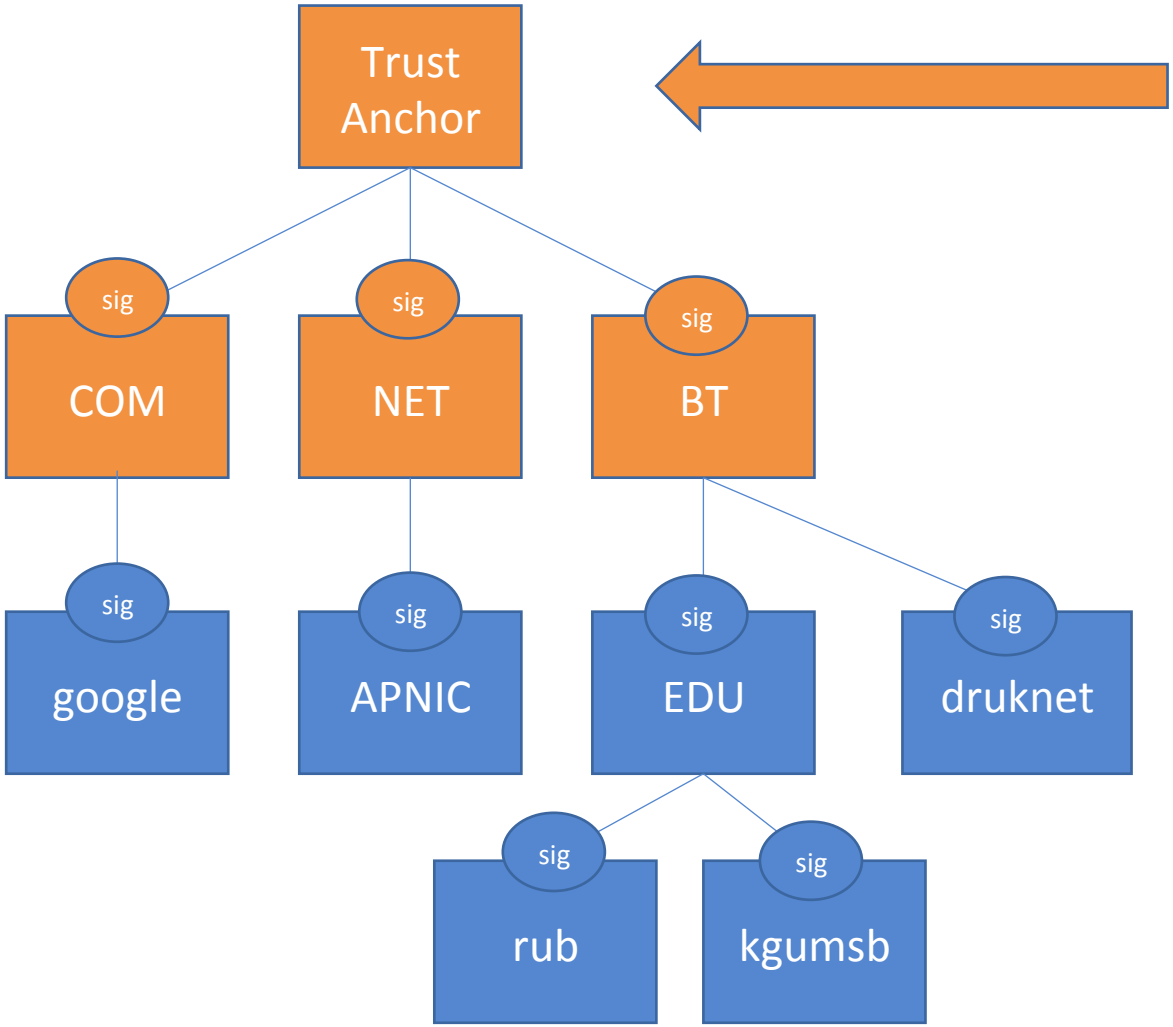
Tree failure at the root is fatal



If this goes stale or out of date…..

Then its signatures are invalid

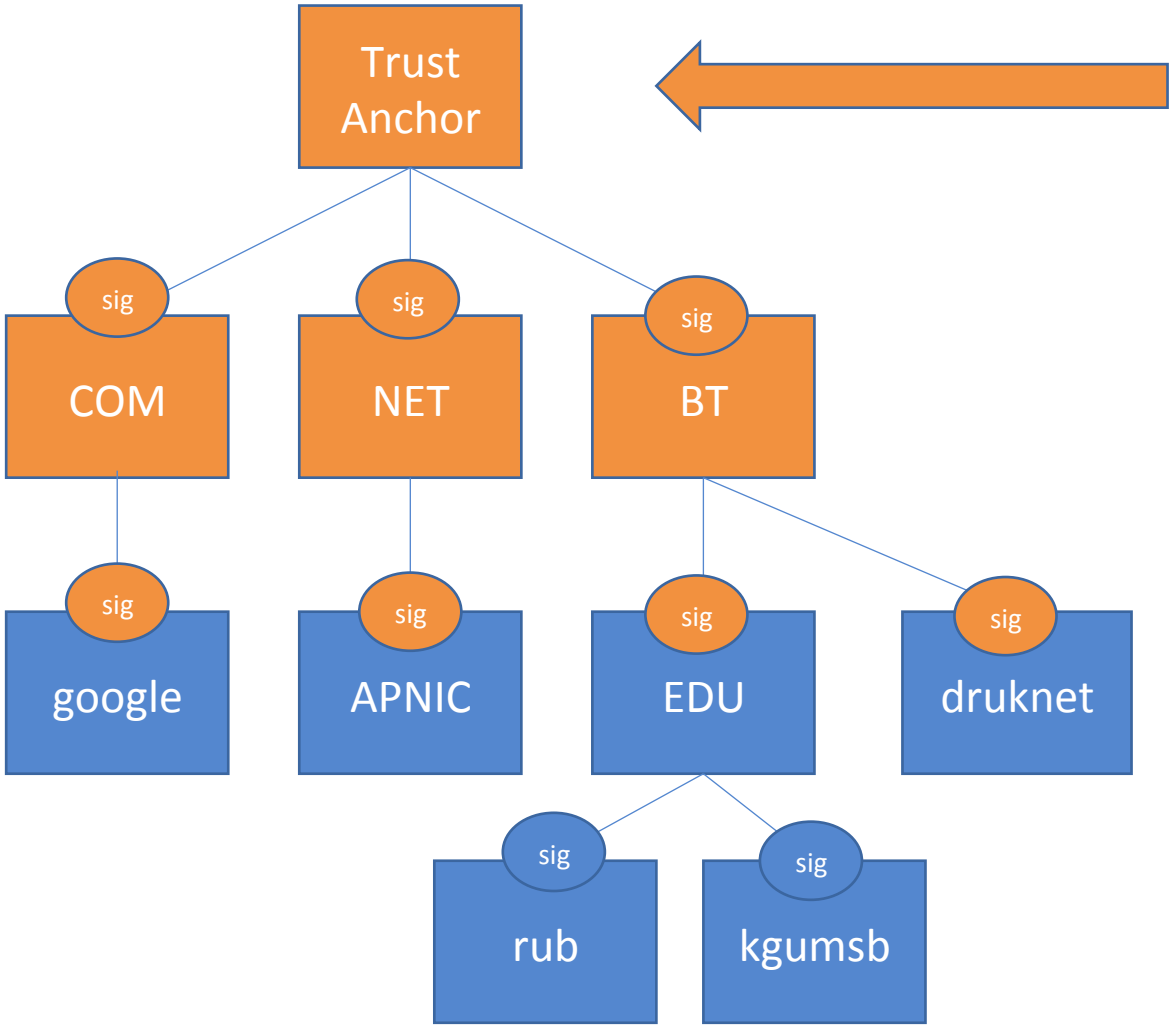
Tree failure at the root is fatal



If this goes stale or out of date…..

And the child zones are invalid

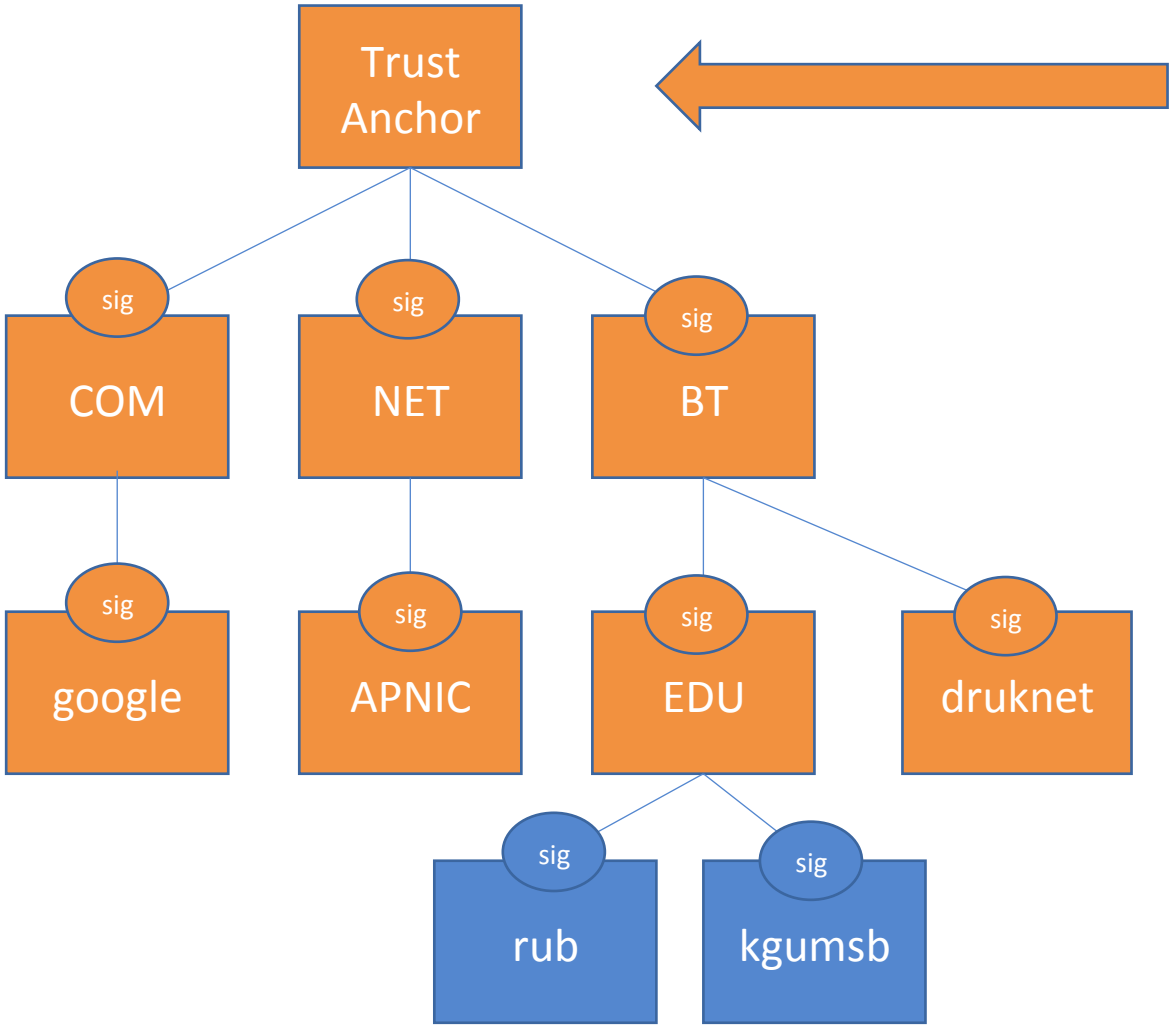
Tree failure at the root is fatal



If this goes stale or out of date…..

And so their signatures are invalid

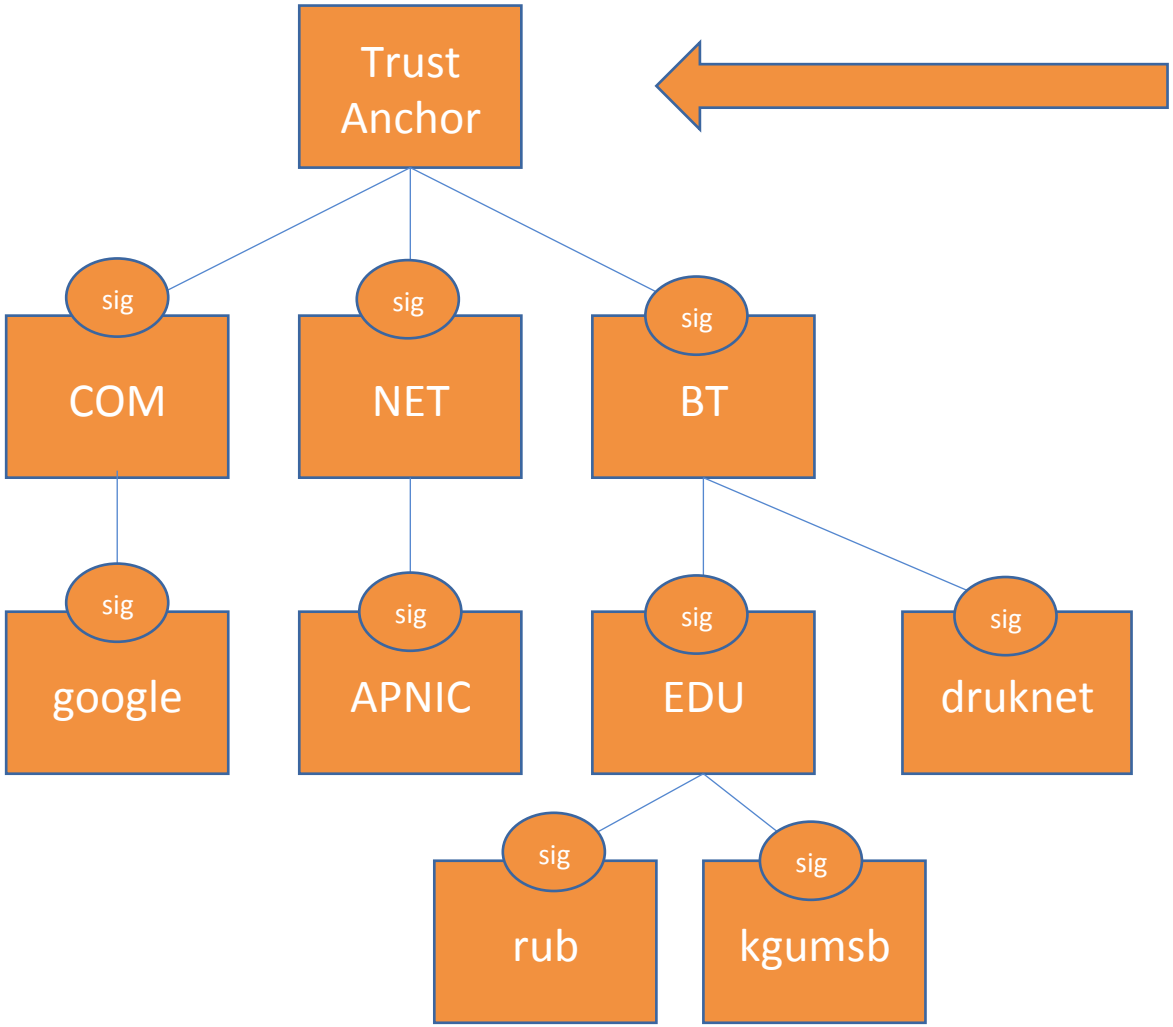
Tree failure at the root is fatal



If this goes stale or out of date…..

And so the grandchild zones are invalid

Tree failure at the root is fatal

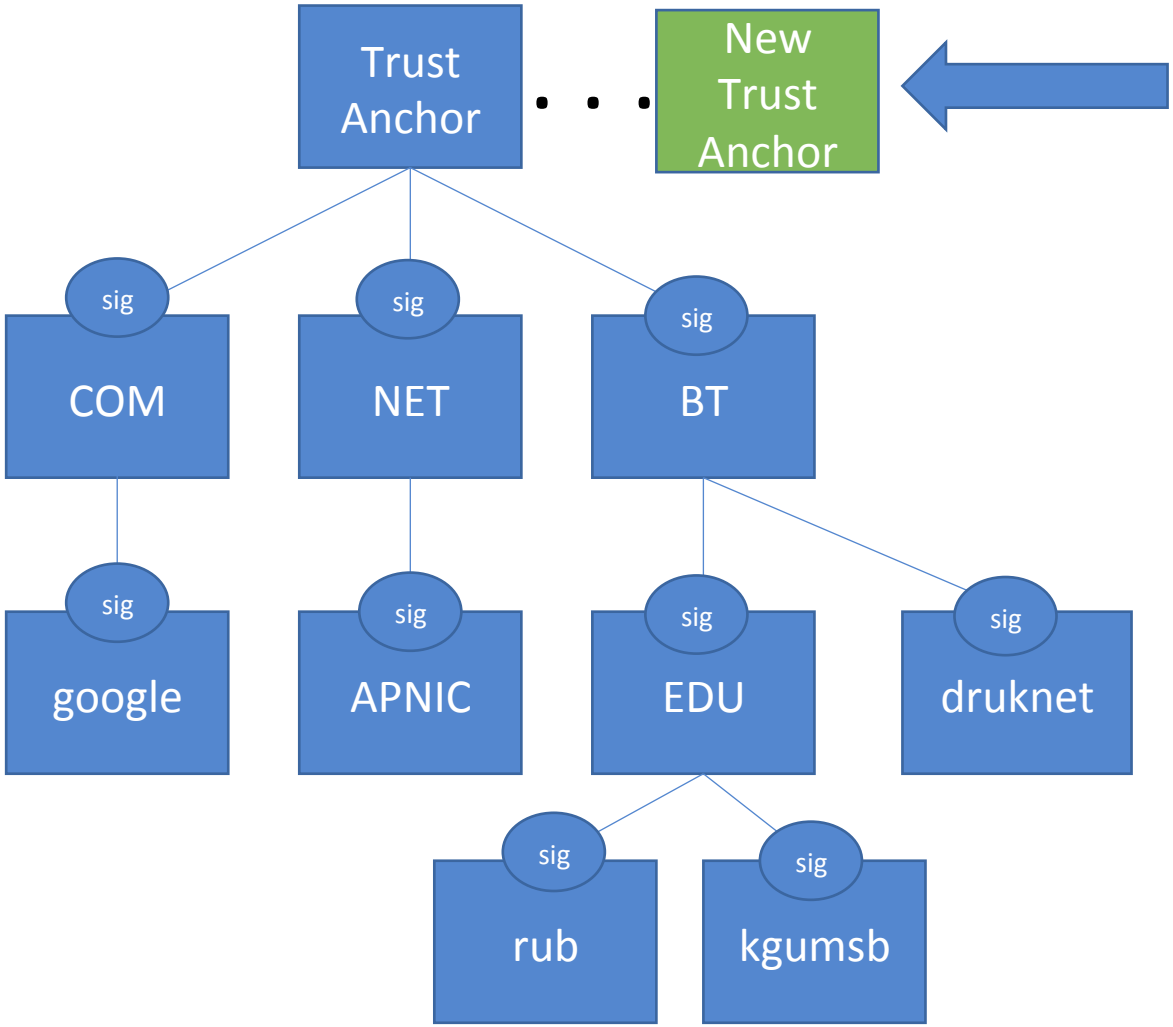


If this goes stale or out of date…..

And so the grandchild zones are invalid all the way down.

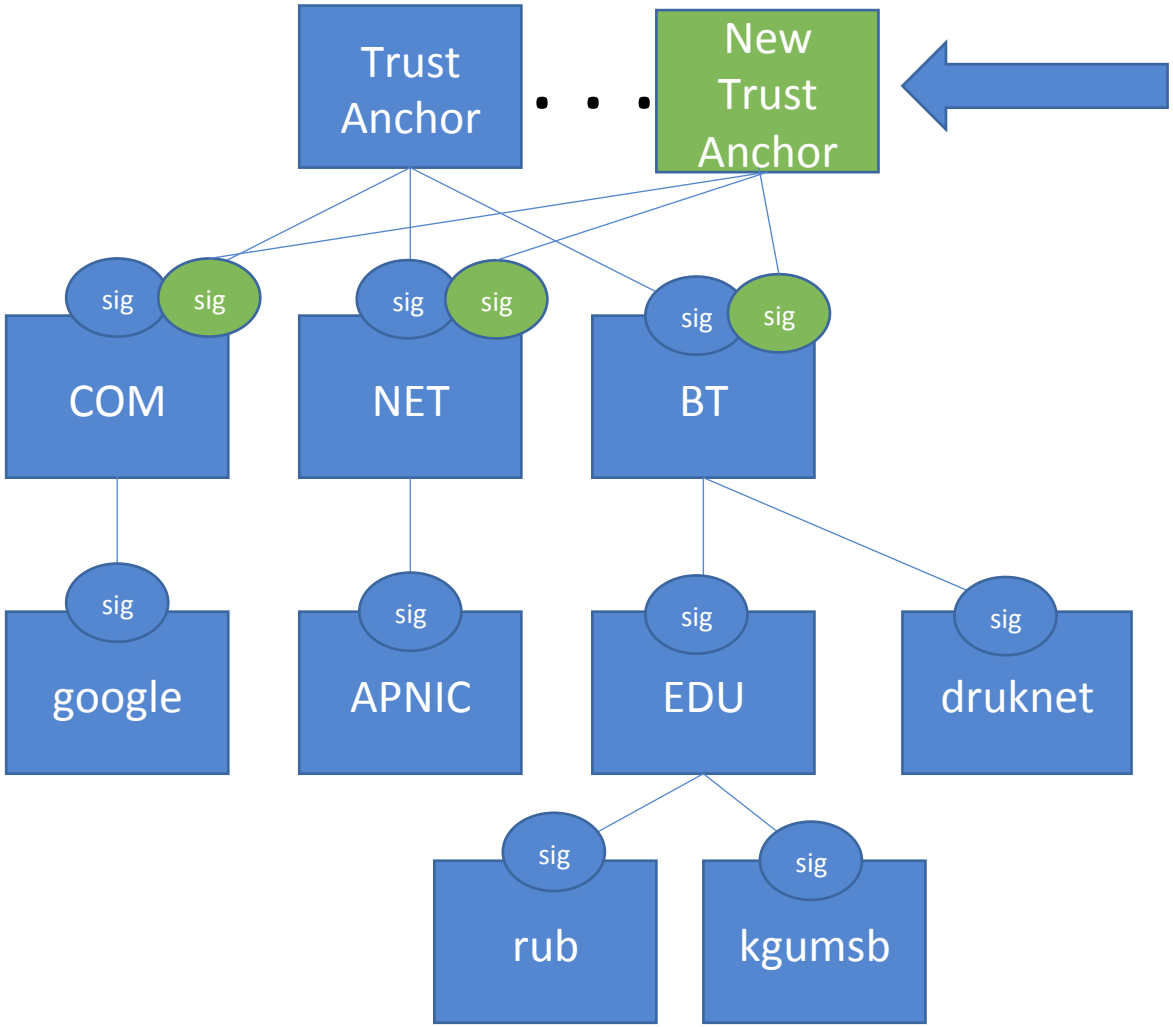
ANYTHING DNSSEC SIGNED BELOW IT IS INVALID

During Key Rollover



This is the KSK. This is what is changing.

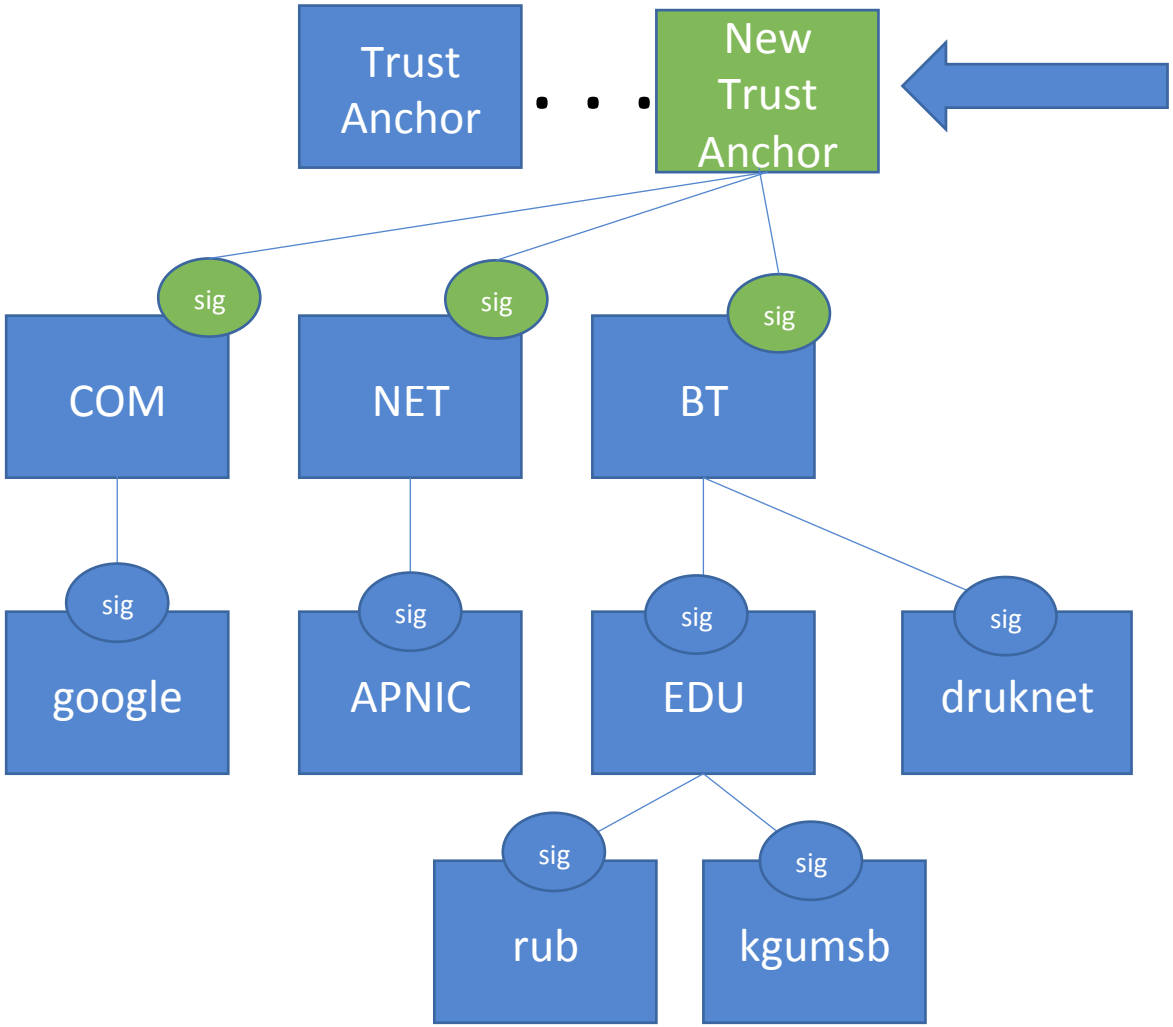
During Key Rollover



This is the KSK. This is what is changing.

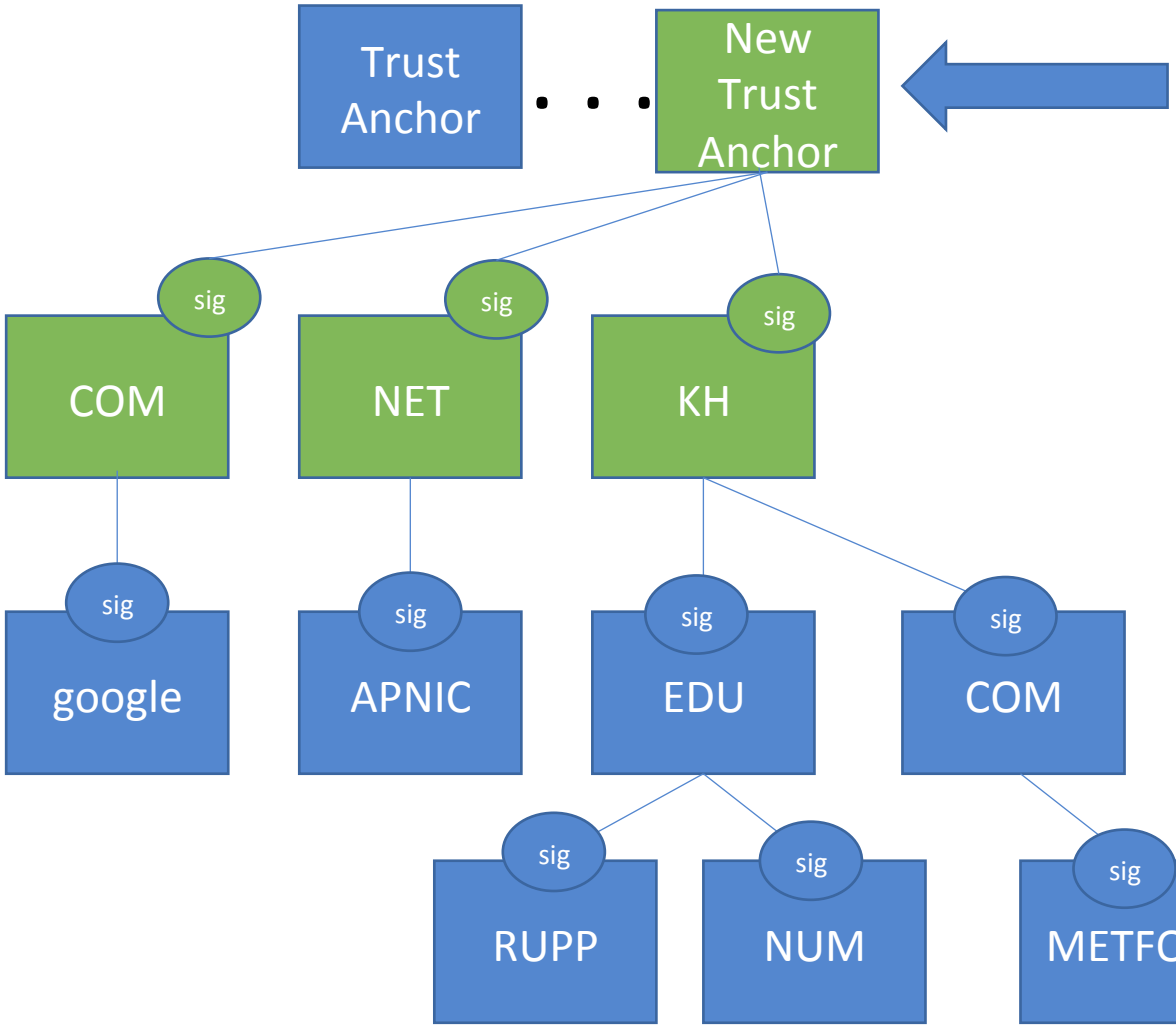
The root is co-signed by two sets of keys…

During Key Rollover



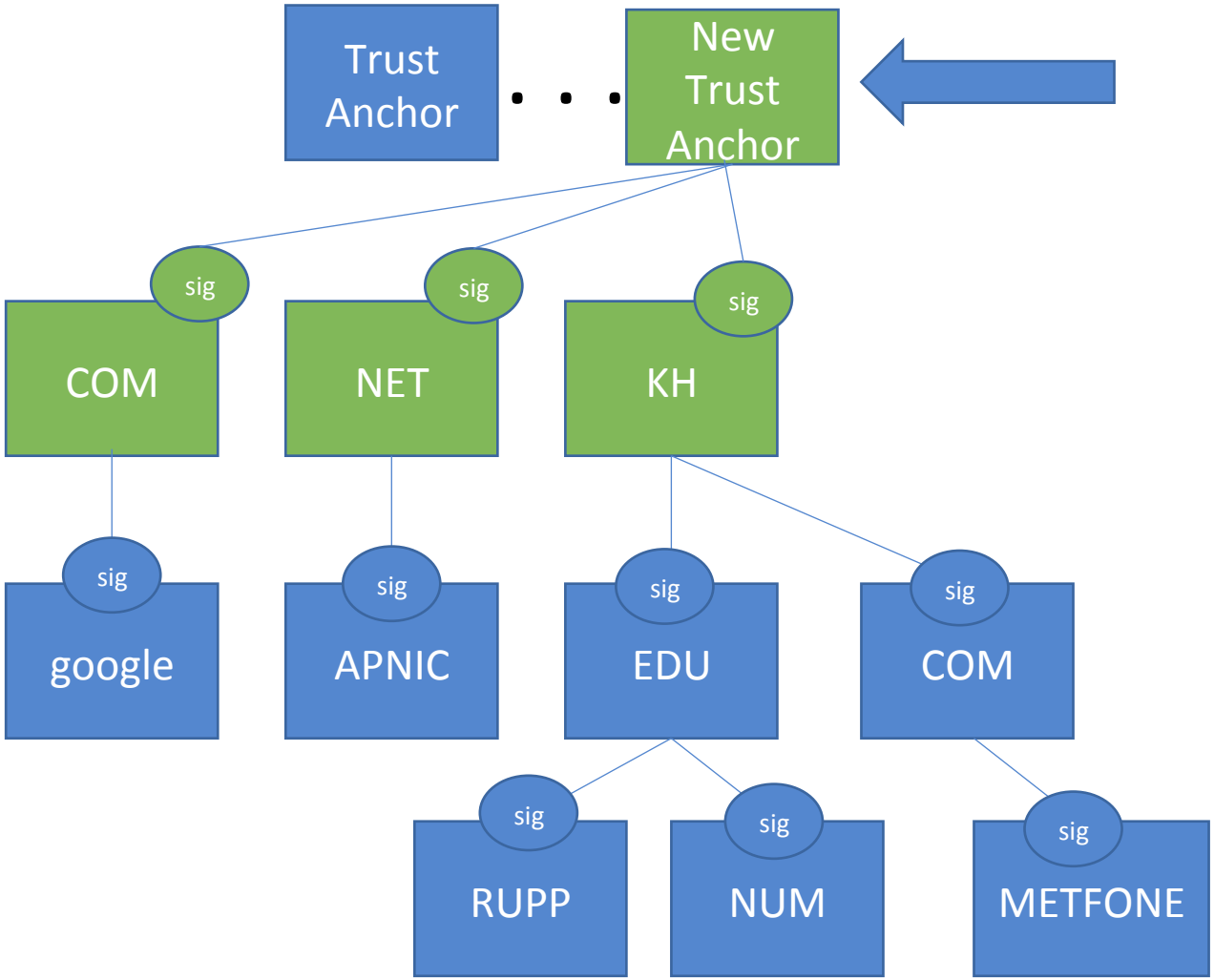
Then the old key is “deprecated”

During Key Rollover…



Then the old key is “deprecated”

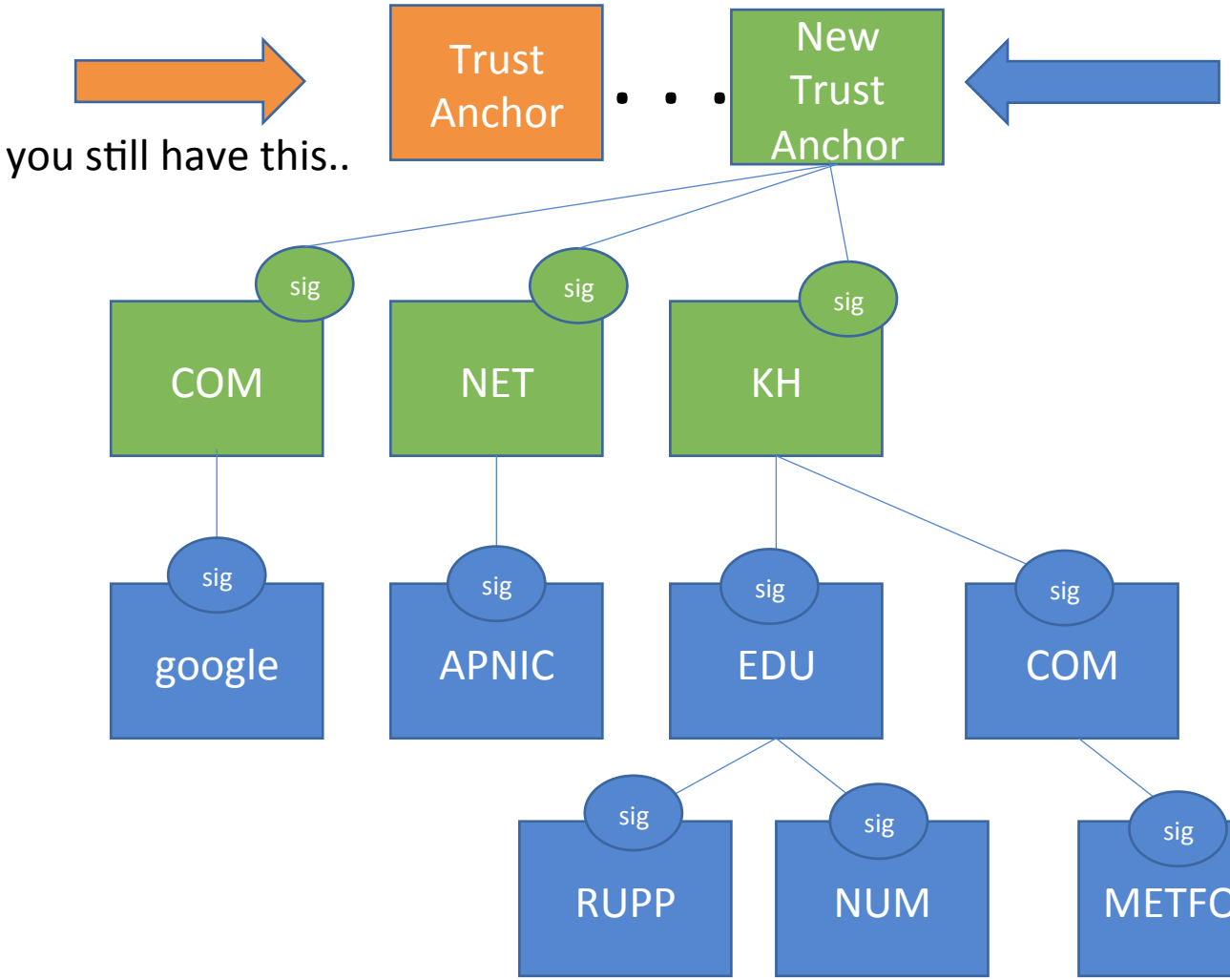
During Key Rollover…



And everyone now trusts the new key.

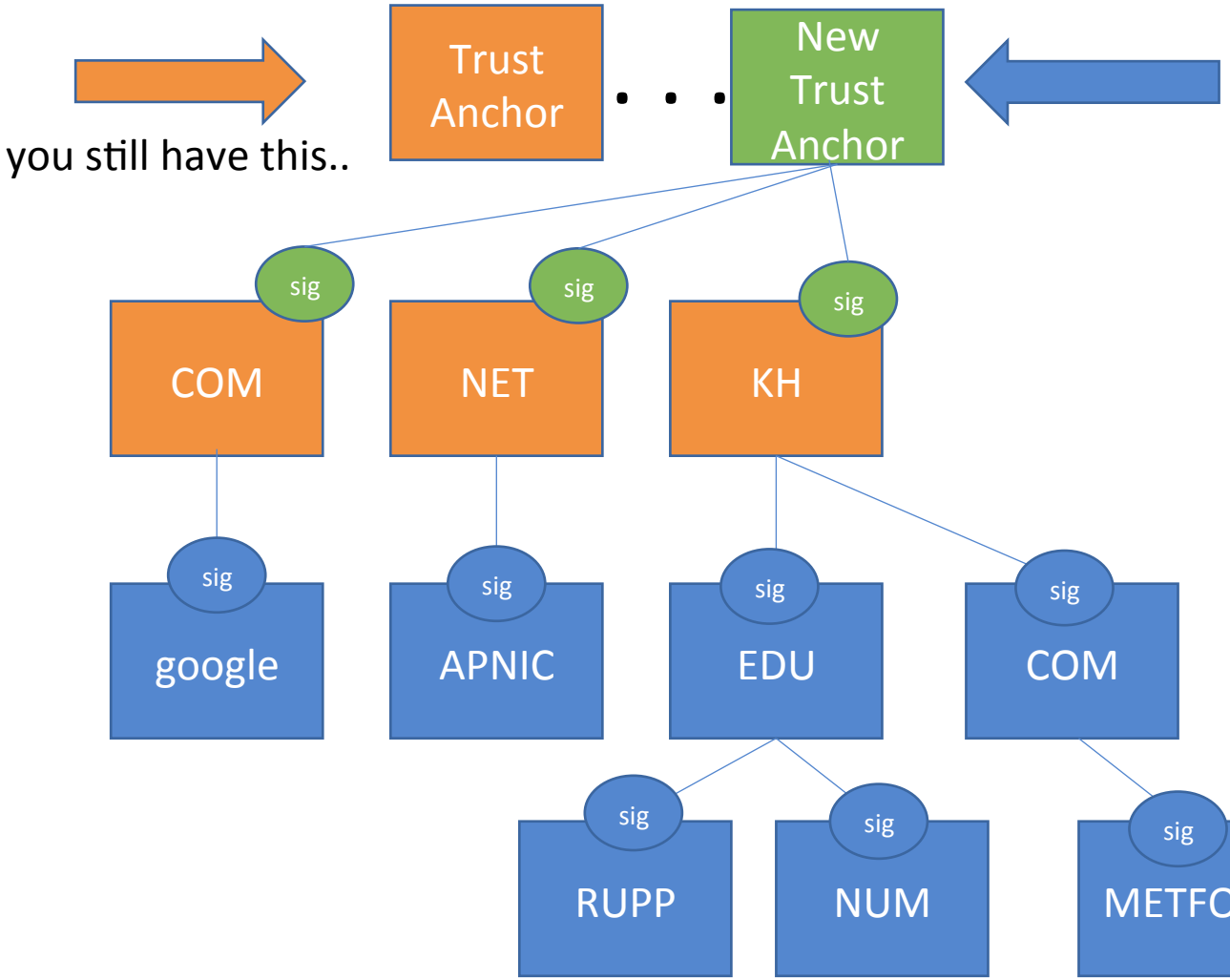
No child or grandchild signatures need to change.

Not upgrading your trust anchor is fatal when its signatures are dropped.



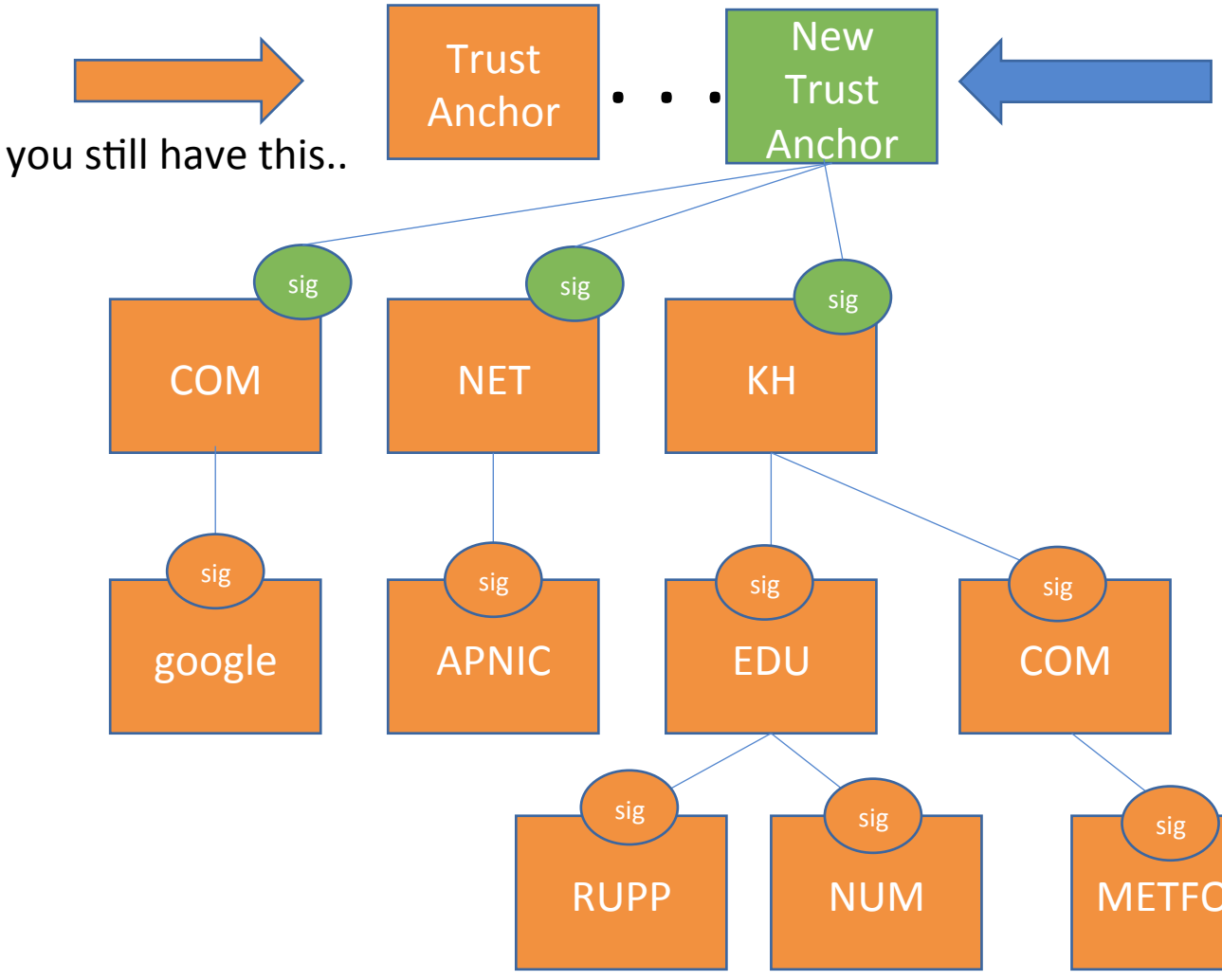
Uh oh… the old key is “deprecated” and there are no signatures you can validate

Not upgrading your trust anchor is fatal when its signatures are dropped.



Uh oh… the old key is “deprecated” and there are no signatures you can validate

Not upgrading your trust anchor is fatal when its signatures are dropped.



Uh oh… the old key is “deprecated” and there are no signatures you can validate

So everything fails.

ANYTHING DNSSEC SIGNED BELOW IT IS INVALID because you don’t “see” valid signatures.

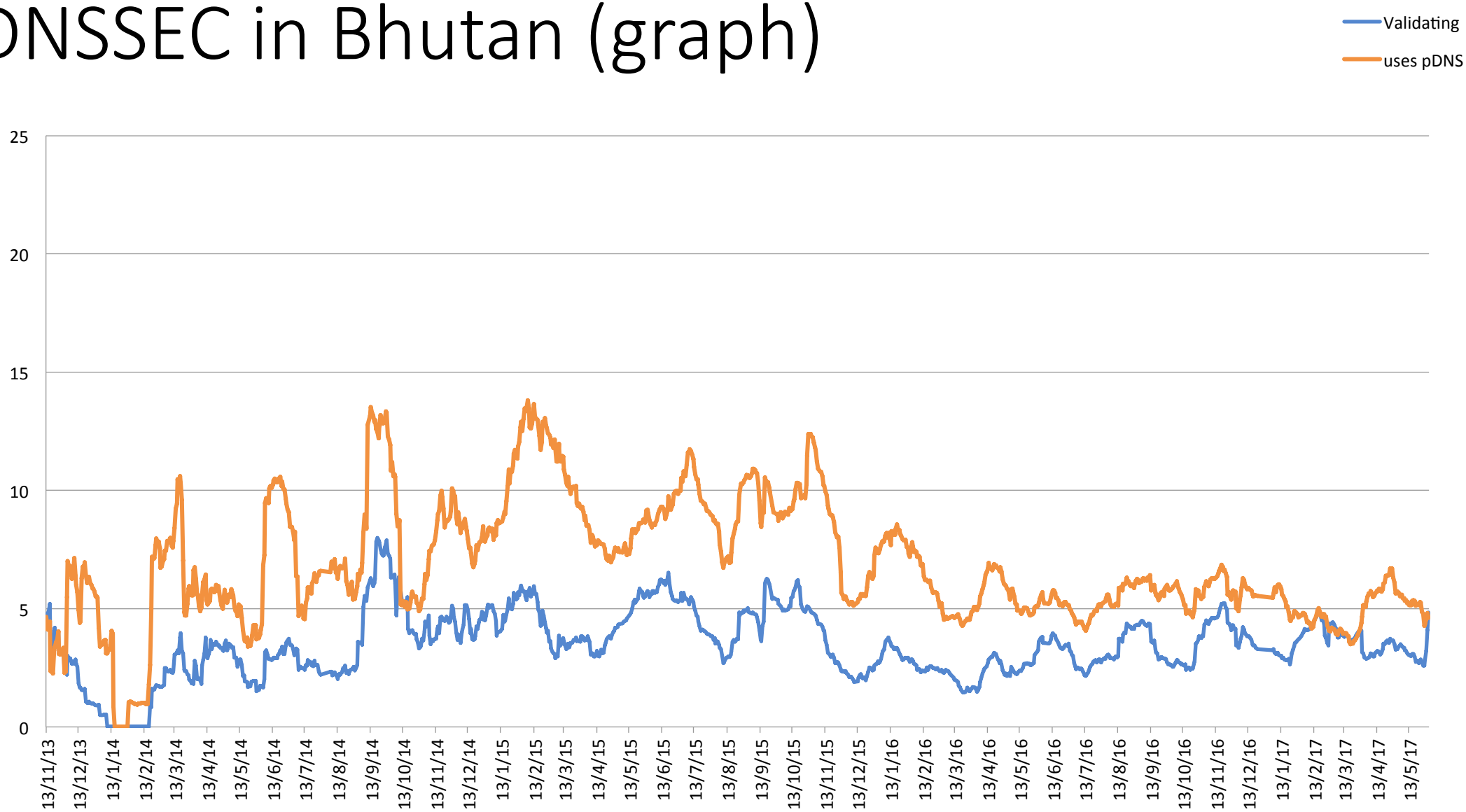
Google public dns (pDNS) is good!

- Globally visible, anycast, highly reliable DNS service
  - 8.8.8.8 and 2001:4860:4860::8888
- Implements DNSSEC Validation
  - With RFC5011 (key roll intent signalling)
  - Will be updated in line with the ICANN KSK roll
- Using pDNS is a good idea but...
  - Google acquire knowledge of what your users are doing

Can we see inside Bhutan? APNIC Labs can!

- Worldwide, long baseline (2010 onward) measurement of end users
- Leverages HTML5 JavaScript code in advertisements placed through google
- Random placements worldwide, 24/7
  - 5m to 15m daily samples
  - 30,000 from Bhutan in a 90 day window
- Analyzed for Origin-AS (BGP) and GeoLoc (delegation stats, maxmind)
- Ask clients to fetch 1x1 pixels from DNS labels with different qualities
  - DNSSEC signed zone, DNSSEC mis-signed zone
  - IPv6 enabled, dual-stack, large packets (pMTU)
- Can fetch DNSSEC signed, won't fetch DNSSEC badly signed? Validating!
- Analyze DNS resolver query to find use of google public DNS

DNSSEC in Bhutan (graph)



https://stats.labs.apnic.net/dnssec/BT

Bhutan and DNSSEC

- Around 5% of the Bhutanese end users appear to be using google pDNS
  - low to no exposure of risk to DNSSEC issues
  - Google knows a *lot* about what your community is doing!
- Less than 5% if the Cambodian end users are DNSSEC secured
  - Only using DNSSEC enabled resolvers, will not be led to false DNS outcomes
  - Therefore, the worst-case number of potential users who could see side effects of the DNSSEC key roll
    - This is unlikely: its very much the worst-case risk side. We do not expect anything like this number of users to be affected.
- How does this distribute over the top ISP by samples seen
  - Not ‘market share’ but a good model for what end users experience
  - Based on APNIC Labs advertising based random samples

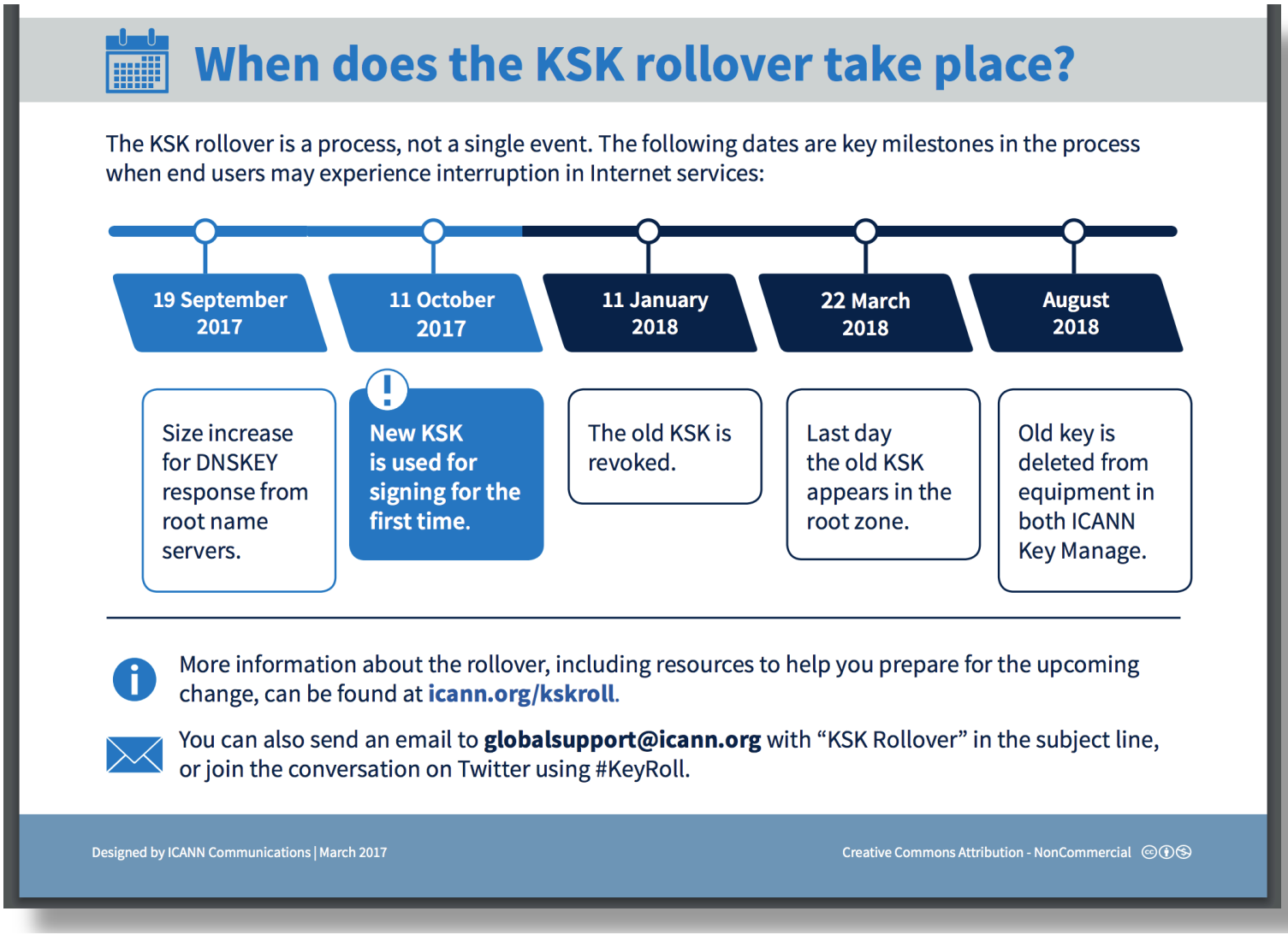
NSSEC in Bhutan (top 3)

ASN	Name	% validating	% pDNS	sample count
38004	FASTLINK-ISP FastLink Wireless ISP	28.93	47.11	121
38740	TASHICELL-AS TashiCell Network AS	3.55	3.34	15023
17660	DRUKNET-AS DrukNet ISP	3.22	6.01	39505

https://stats.labs.apnic.net/dnssec/BT

Basically, only Fastlink have any exposure to risk, and since half the visible DNSSEC is pDNS, it's a very small risk.
Also, its from reasonably small market share

Stages of the DNSSEC Key rollover (ICANN slide



For more information see the ICAN

https://www.icann.org/
resources/pages/ksk-rollover/#ov

Where are we in the timeline? ✔ completed

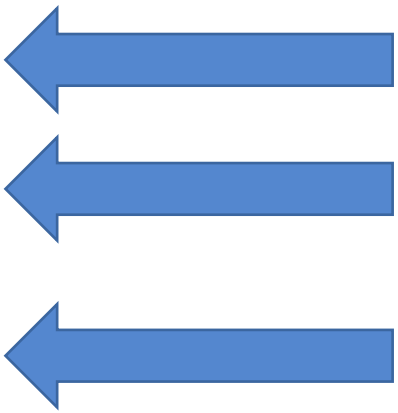
- ✔ Phase A: Key generation (Oct 2016)
  - ✔ KSK-2017 generated at the first key management facility
- ✔ Phase B: Key replication (Feb 2017)
  - ✔ KSK-2017 copied to the second key management facility. KSK now qualified for entering the production state.
- ✔ Phase C: First data is signed with KSK-2017 for use in Phase D (May 2017)
  - ✔ First set of key signing requests are signed.

- Phase D: Publication (Aug 2017)
  - KSK-2017 is published to the root zone.
  - Both KSK-2010 and KSK-2017 are used to sign the root zone.
- Phase E: Rollover (Nov 2017)
  - Only KSK-2017 is used to sign the root zone.
- Phase F: Revocation (Feb 2018)
  - KSK-2010 is removed from the root zone.
- Phase G: Delete 1 (May 2018)
  - KSK-2010 is deleted from the first key management facility.
- Phase H: Delete 2 (Aug 2018)
  - KSK-2010 is deleted from the second key management facility

Where are we in the timeline? ✔ completed

- ✔ Phase A: Key generation (Oct 2016)
  - ✔ KSK-2017 generated at the first key management facility
- ✔ Phase B: Key replication (Feb 2017)
  - ✔ KSK-2017 copied to the second key management facility. KSK now qualified for entering the production state.
- ✔ Phase C: First data is signed with KSK-2017 for use in Phase D (May 2017)
  - ✔ First set of key signing requests are signed.

- Phase D: Publication (Aug 2017)
  - KSK-2017 is published to the root zone.
  - Both KSK-2010 and KSK-2017 are used to sign the root zone.
- Phase E: Rollover (Nov 2017)
  - Only KSK-2017 is used to sign the root zone.
- Phase F: Revocation (Feb 2018)
  - KSK-2010 is removed from the root zone.
- Phase G: Delete 1 (May 2018)
  - KSK-2010 is deleted from the first key management facility.
- Phase H: Delete 2 (Aug 2018)
  - KSK-2010 is deleted from the second key management facility



Packets get bigger

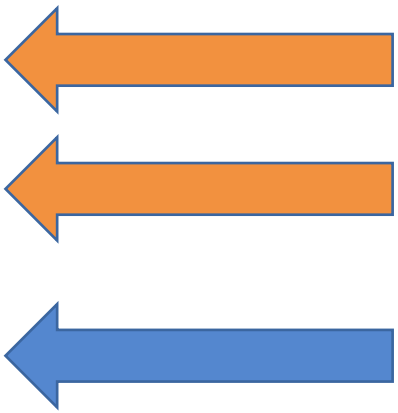
DNSSEC needs to know new TA

“tidying up afterward”

Where are we in the timeline? ✔ completed

- ✔ Phase A: Key generation (Oct 2016)
  - ✔ KSK-2017 generated at the first key management facility
- ✔ Phase B: Key replication (Feb 2017)
  - ✔ KSK-2017 copied to the second key management facility. KSK now qualified for entering the production state.
- ✔ Phase C: First data is signed with KSK-2017 for use in Phase D (May 2017)
  - ✔ First set of key signing requests are signed.

- Phase D: Publication (Aug 2017)
  - KSK-2017 is published to the root zone.
  - Both KSK-2010 and KSK-2017 are used to sign the root zone.
- Phase E: Rollover (Nov 2017)
  - Only KSK-2017 is used to sign the root zone.
- Phase F: Revocation (Feb 2018)
  - KSK-2010 is removed from the root zone.
- Phase G: Delete 1 (May 2018)
  - KSK-2010 is deleted from the first key management facility.
- Phase H: Delete 2 (Aug 2018)
  - KSK-2010 is deleted from the second key management facility

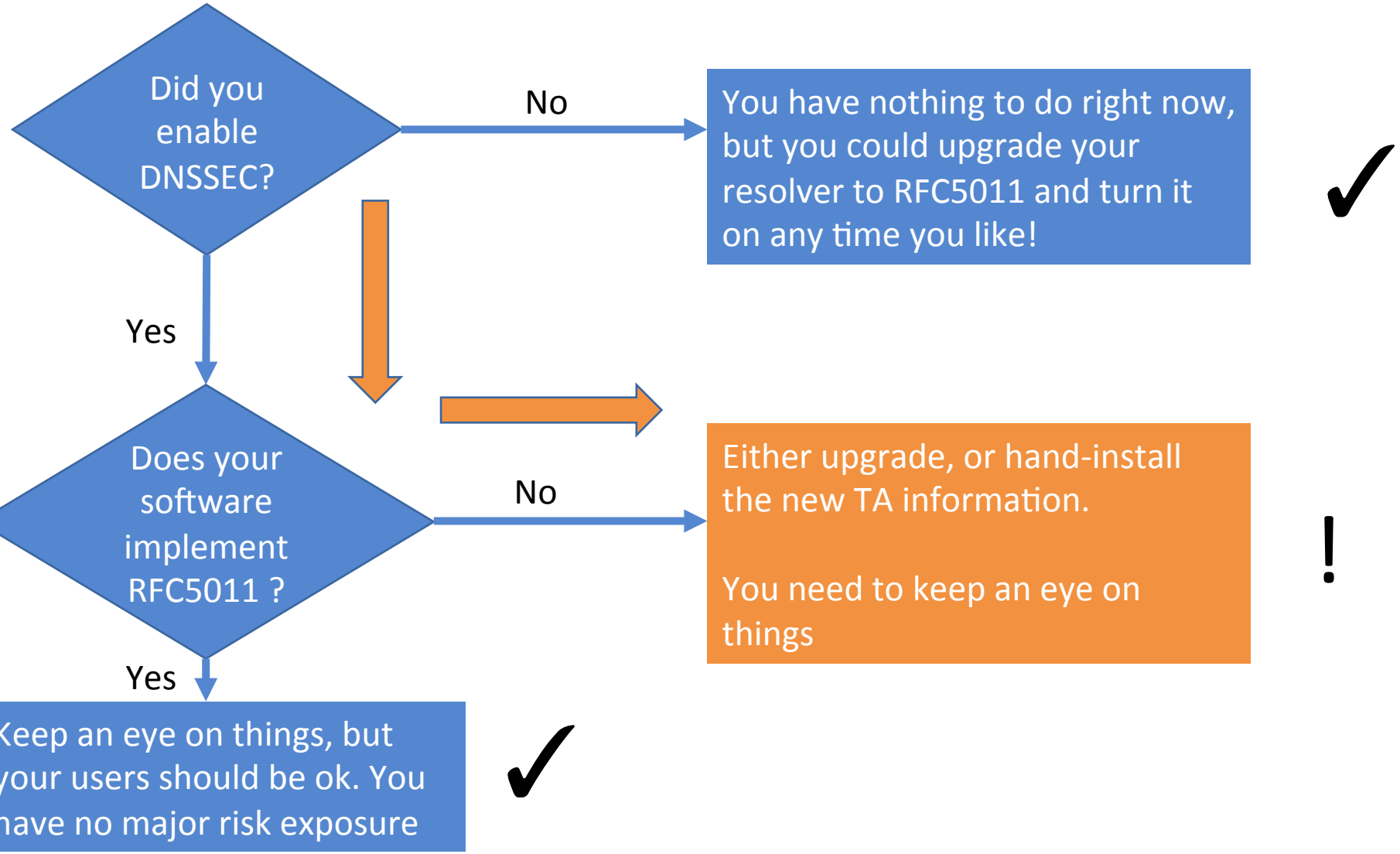


This is when you may start to see problems

You really need to fix systems

“tidying up afterward”

What can you do? Check your resolver!



Summary: Check your DNS.

- Check if your visible DNS resolvers are DNSSEC enabled
  - Check if they are RFC5011 enabled, if not upgrade
- Be aware of downstream (SME, Corporate, customer) DNS resolvers
  - Maybe your helpdesk is going to get “DNS is broken” queries!
- IF things don’t work.. You can do some things
  - Disable DNSSEC (if you know how) or upgrade (better)
  - Enable pDNS
- Keep informed: **https://www.icann.org/resources/pages/ksk-rollover/**

August 2017

Upgrade after September

- DNSSEC offers significant long term value to DNS
  - Attacks on the network only get better.
  - DNSSEC is going to become more important to protect against phishing
- There is no point updating now, before key rollover
  - although if you use new software (RFC5011) it should be ok
- The .BT zone is not signed
  - so your zone itself will not be affected by any external exposure to risk in this keyroll, except for general loss at the root if a validating resolver externally does not have the new TA.
- **BT denoted names will be fine. Inside BT based on the visible deployment levels**

Signing BT

- Key roll is all about relying parties and trust in public DNS services
- To protect .BT denoted names long term, the zone has to be signed
- This isn't an ISP role, but community input to the BT zone authority is important.
  - Your name space is a public good. Protecting it feels like the right thing to do.
- **Time to have a conversation?**