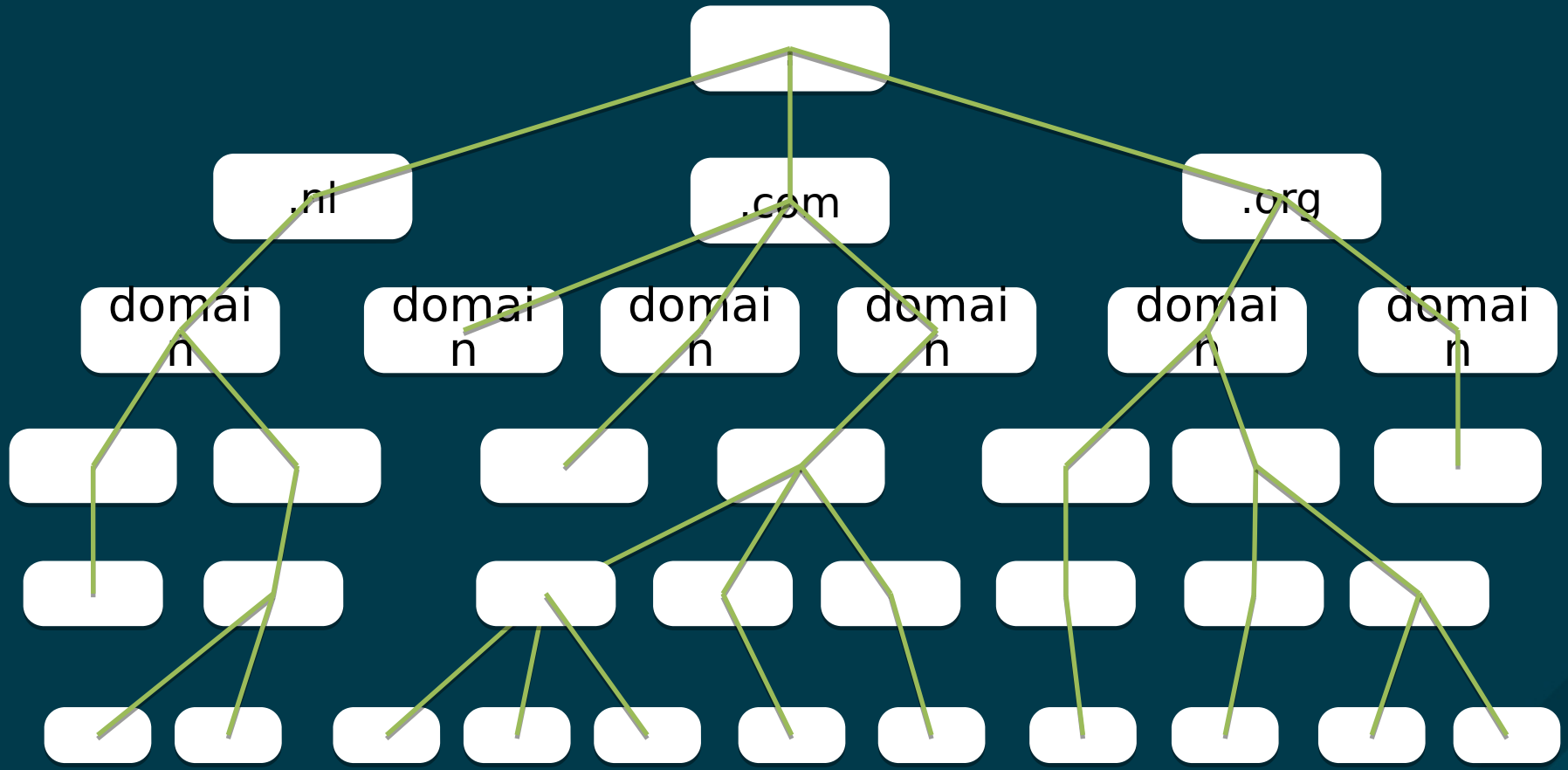
draft-pwouters-powerbind-03

Increasing the Trust of the DNS Hierarchy

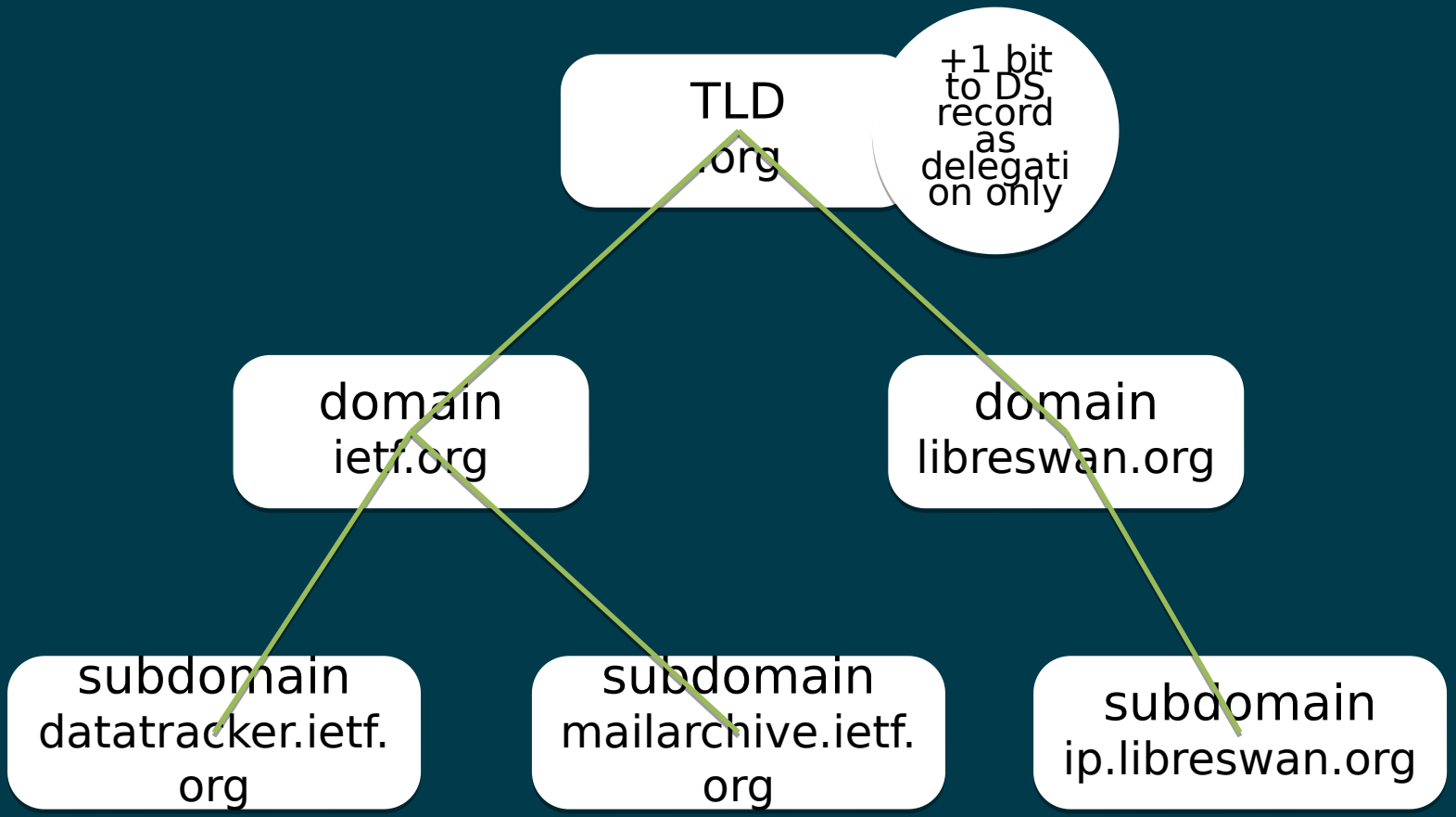
interim-2020-dnsops-01
april 14, 2020

A few very powerful DNSKEYs

if you can’t not trust your friends, who can you not trust?



The solution:
The DNSKEY DELEGATION_ONLY flag



DELEGATION_ONLY DNSKEY flag

Traditional Key Signing KEY DNSKEY record:

powerbind.nohats.ca. IN DNSKEY **257** 3 8 (BLOB)
; KSK; alg = RSASHA256 ; key id = **17869**

powerbind.nohats.ca. IN DS **17869** 8 2
f22bbb3315c48b719fb67da0fc019ae4af534143569f7a63022eba4d87c1f56d

DNSKEY with DELEGATION_ONLY flag set:

powerbind.nohats.ca. IN DNSKEY **321** 3 8 (BLOB)
; KSK; alg = RSASHA256 ; key id = **17933**

powerbind.nohats.ca. IN DS **17933** 8 2
096749AAB0CFE225A3779AC7BD21EBDC1D8573511DD5AFA0889EB5E8A00B9AF9

DELEGATION_ONLY flag benefits:

1) Public commitment by parent to be a delegation-only zone to prevent rogue parents from deep-signing child data.
   - Publish commitment via DNSKEY flag

2) DNSSEC transparency that does not require logging ALL DNS records with public keys
   - With above flag, we only need to log DNSKEY / DS records or their NSECs

Does introducing a new DNSKEY flag break any existing validating resolvers?

1) It shouldn’t ….
2) It didn’t when tested in 2018
3) bind, unbound, Google DNS, powerbind were tested and worked fine

4) run a test on example.com so Geoff Huston can test it at scale? :)

Changes since draft-pwouters-powerbind-00

1) Wes Hardaker added as co-author. He cleaned up a lot of language in the draft
2) Clarified that a zone with DELEGATION_ONLY flag set, expects its own parent not to skip the zone itself
3) Clarified setting the flag in a zone where the parent has not set the flag is still very useful for DNSSEC Transparency
4) Suggest the root key is treated by resolver software as if it has the flag set.
5) _underscore label exception (these are never a real zone cut)
6) Added operational considerations, migration from/to process, signed glue death

Pros

- Protects child zone data from parent
  - Including TLSA, SMIMEA, OPENPGPKEY
- Allows DNSSEC Transparency
- Very simple
  - No new RRTYPE
  - no changes required for authoritative servers
  - Only minimal changes in validator
- Only requires DNS resolver/stub code changes

Cons

- Does not allow exceptions for ENT (“co.uk")
  (no more dots without NS delegations)
- Zone might need sub-zone for NS records
  - root and most (all?) TLDs already do this
  - SLD usually do not need to set this flag
- Orphaned glue signed by parent becomes BOGUS
- Does not protect child APEX data
  - A/AAAA, MX, IPSECKEY[*]
  - Not a big issue, as we care most about prefixed records, eg TLSA, SMIMEA, DKIM

Next steps?

- More (technical) discussion
- Followed by adoption call
- Implement DNSSEC TRANS
- ???
- Profit!