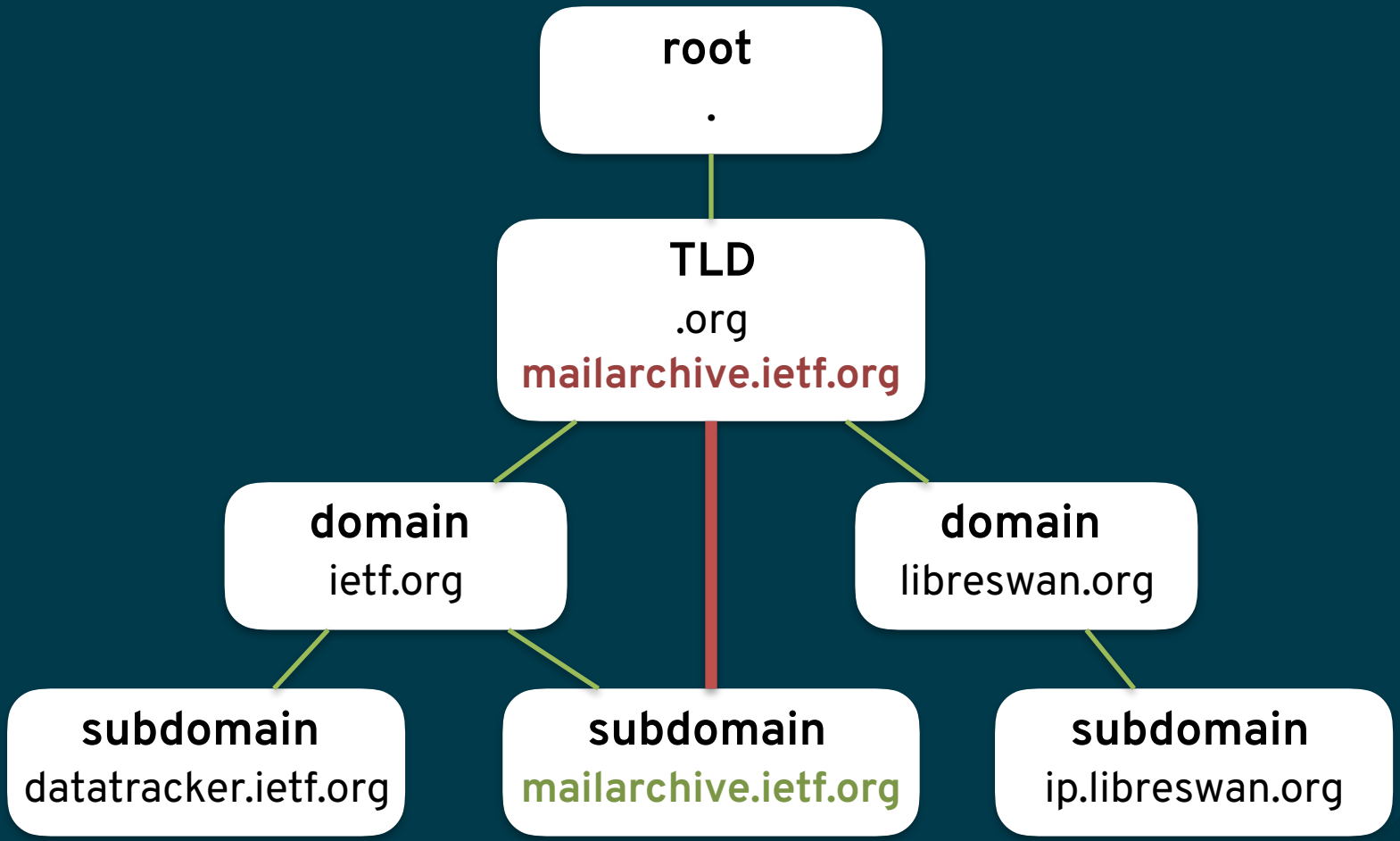
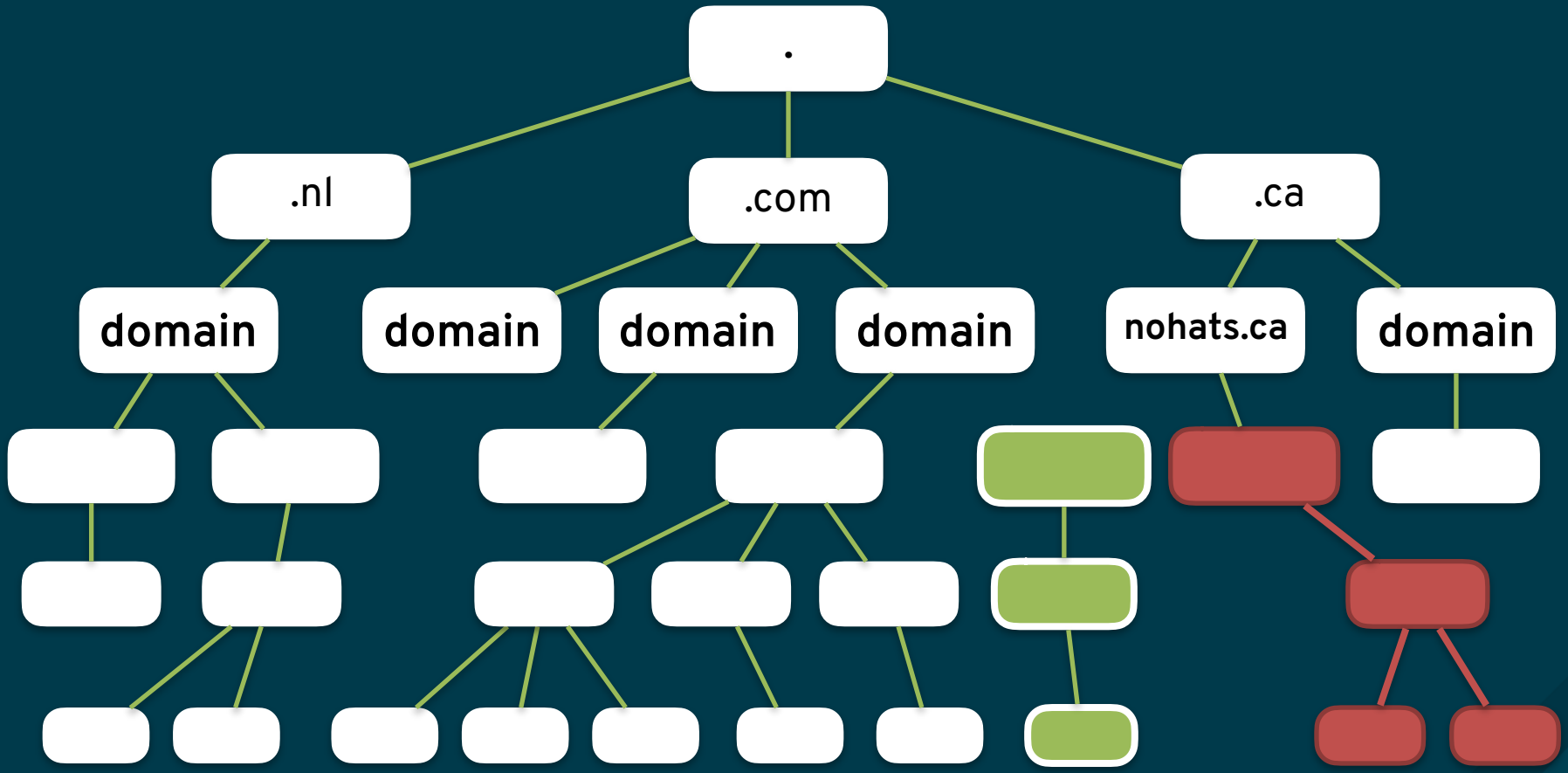
Increasing trust in the DNSSEC hierarchy

draft-pwouters-powerbind

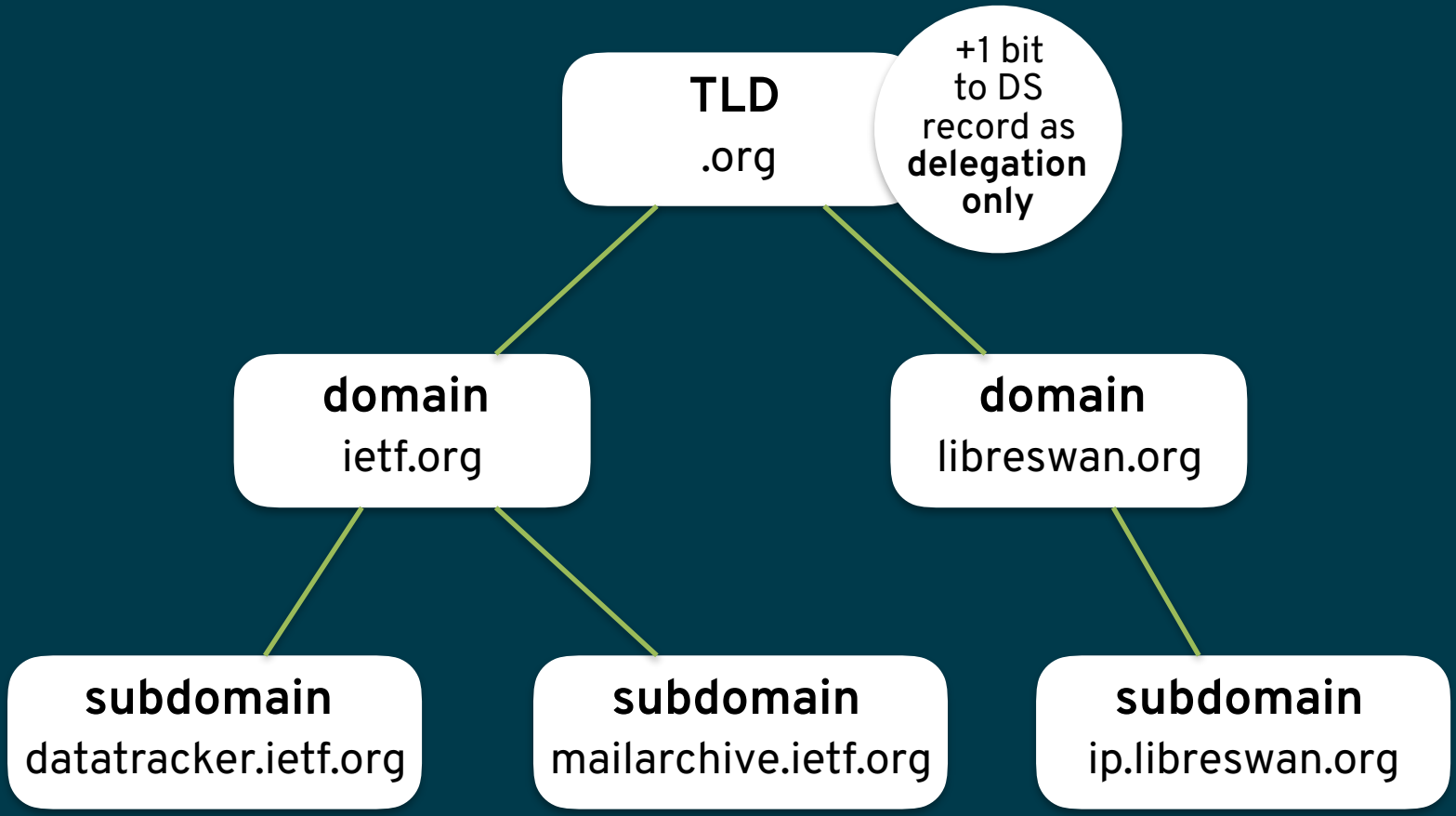
Attack 1: Parental override of delegation



Attack 2) Replacing child delegation



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 (
        AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
        ) ; 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 (
        AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
        ) ; 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 this break existing deployments?

- Tested with squatted dnskey flag 0x40 in powerbind.nohat.ca.
- All tested DNSSEC resolvers validate properly
  - bind, unbound, powerdns, Quad[148]

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")
  (but see next slide)
- 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
    (but see next slide)
- Requires delegations for _prefix labels

  (but see next slide)

IETF #102 Hallway conversations…

- Change the flag to mean two things:
  - Commit to delegation only for child data
  - All parents above me cannot skip my delegation
    - helps in all cases except startup/empty cache
    - makes flag much less important for root zone
- Exempt _prefix labels from “no skip” directive
  - Allows signing 443._tlsa.example.com.
- Use 2 bits instead of 1, indicating “path len”