Automating maintenance of delegation information

draft-ietf-dnsop-delegation-trust-maintainance-00
and
draft-hardaker-dnsop-csync-02

Warren Kumari

What's the problem?!

- Rolling DNSSEC keys is hard.

  ... no it's not...

- **Publishing** new DNSSEC keys is hard...

  ... and dangerous....

Solution.

- Simply publish your new DNSSEC delegation trust info in your current zone, with a ‘c’ in front of it...

So, if your new DS is:

```
example.com. IN DS 23206 5 1 A0D8F46F62F9CF052A488869FFEB7B1D21E3F1C2
```

it becomes:

```
example.com. IN CDS 23206 5 1 A0D8F46F62F9CF052A488869FFEB7B1D21E3F1C2
```

... and if your parent prefers DNSKEY instead of DS

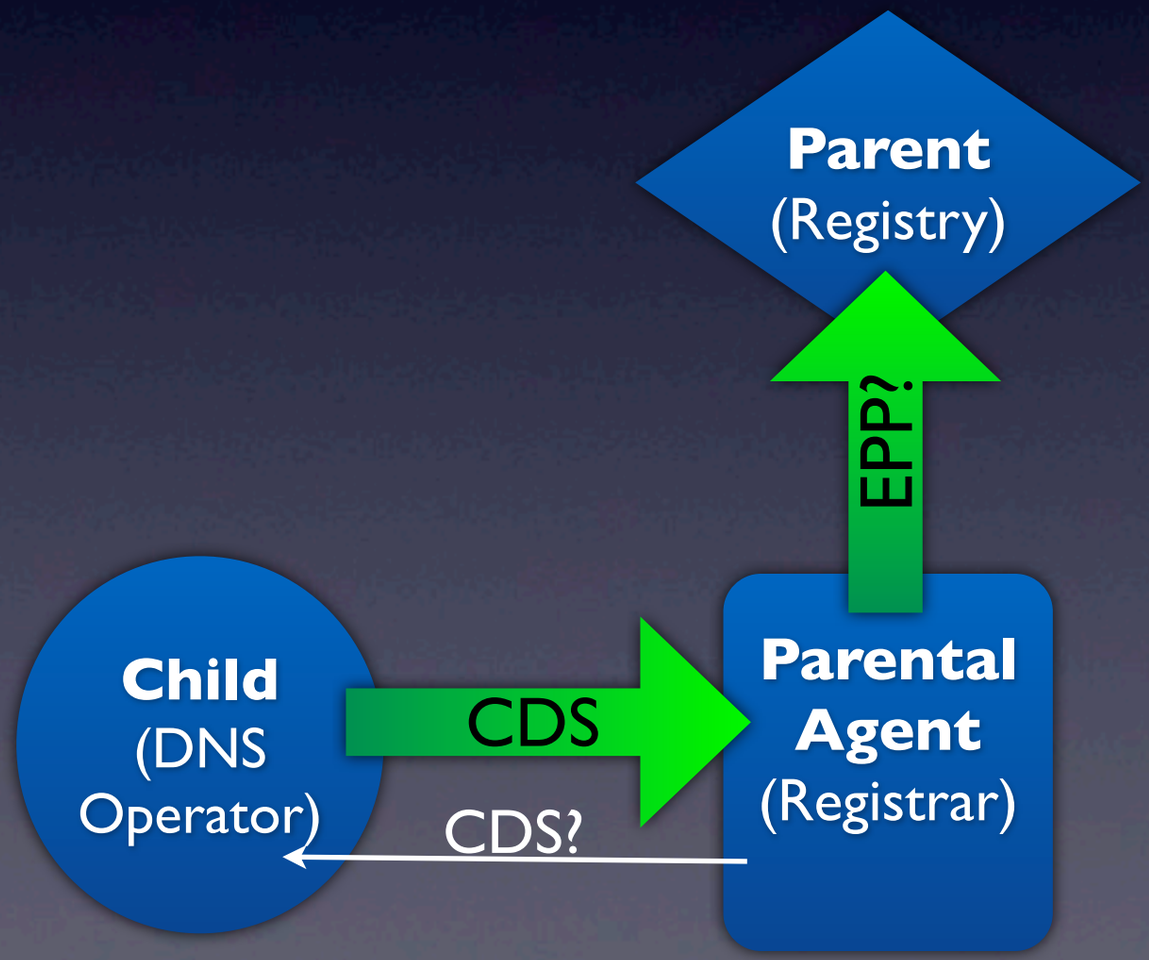
```
$TTL 600  ; 10 minutes
     DNSKEY 257 3 5 (AwEAAZDfLmweYGpszqbmC21NKTdNd28U4s+y/s6/6PlK
                     X8JIfXS4kkvTGWb+Xs2QX9ia636EJY+/Vo88XbokGA8y
                     VUJuKiC+1M4f7JaHarg1E1cM1IOeaPXhJQsdkwIb5AYZ
                     qTX7pY5DdY9X6hcAHfeQkizGrcpfmGvHM9nPYjikjtr5)
```

becomes:

```
$TTL 600  ; 10 minutes
     CDNSKEY 257 3 5 (AwEAAZDfLmweYGpszqbmC21NKTdNd28U4s+y/s6/6PlK
                      X8JIfXS4kkvTGWb+Xs2QX9ia636EJY+/Vo88XbokGA8y
                      VUJuKiC+1M4f7JaHarg1E1cM1IOeaPXhJQsdkwIb5AYZ
                      qTX7pY5DdY9X6hcAHfeQkizGrcpfmGvHM9nPYjikjtr5)
```

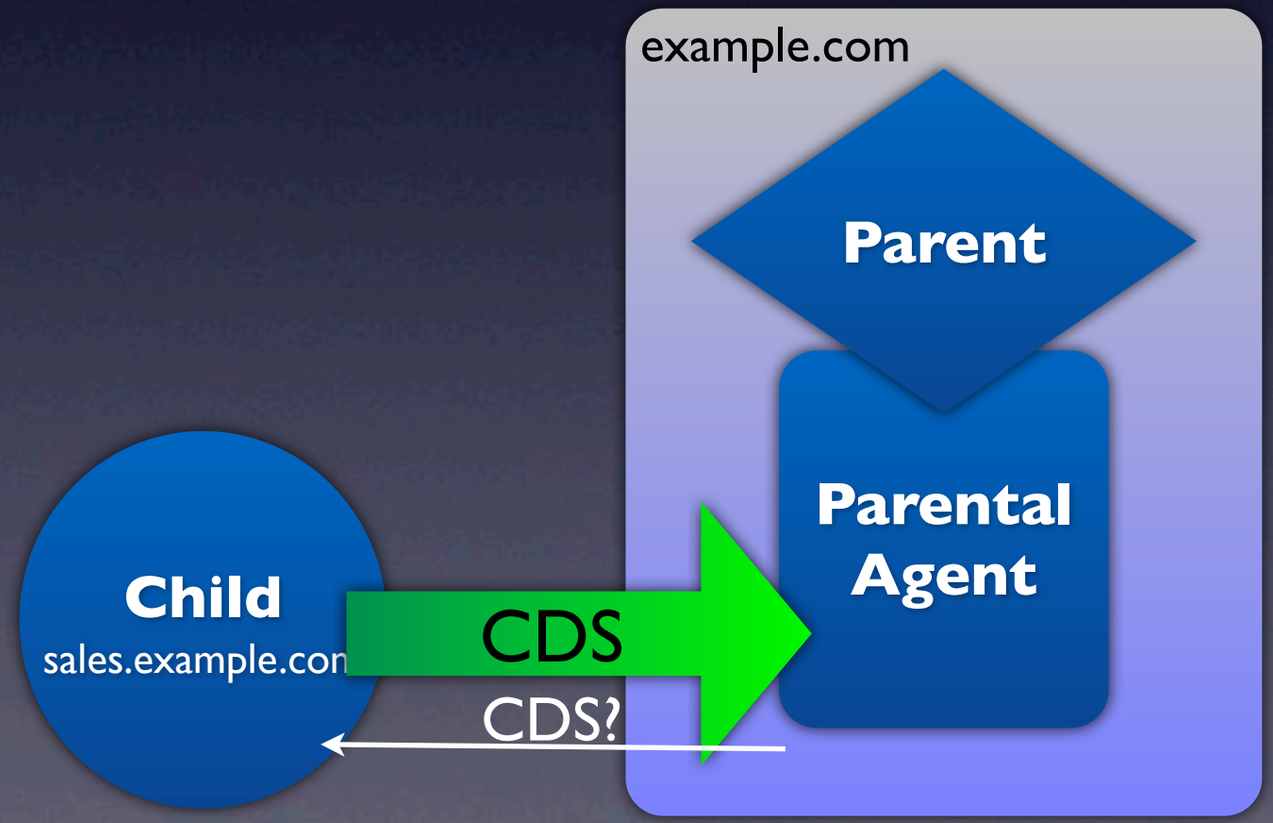
Publishing...

- Your "parental agent" polls and publishes the CDS / CDNSKEY .... err, who!?



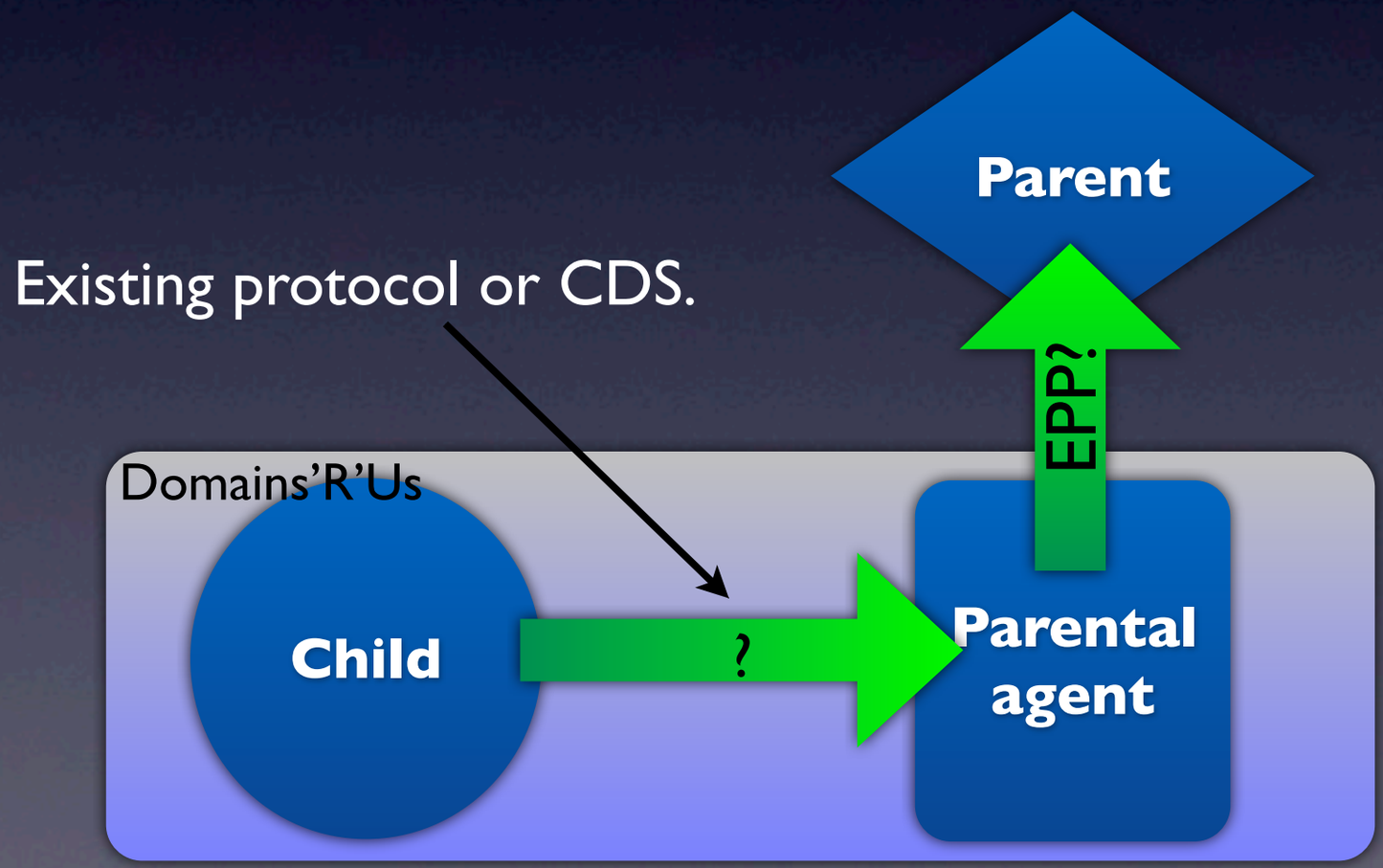
Publishing...

- If Parent = Parental Agent (e.g Enterprises, Educational, some ccTLDs)



Publishing...

- If Operator = Parental Agent (e.g: Registrar runs DNS) can use this if they want.



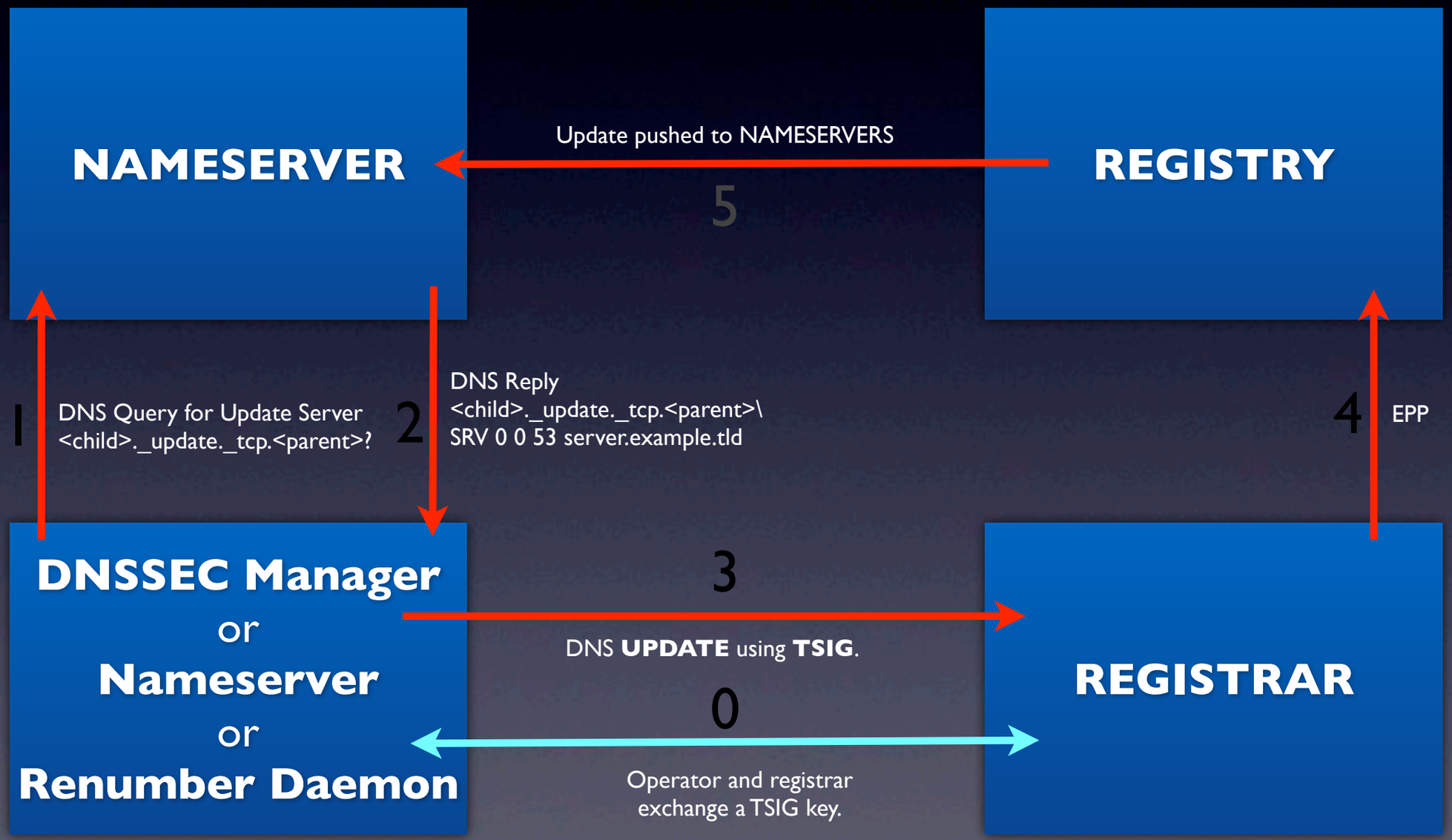
Additional details

- Polling?!
  - Fully expect additional triggers.
- CSYNC
  - Like CDS / CDNSKEY but for NS / glue.
  - Type Bit Map of what to copy.
- What's the difference?
  - CDS / CDNSKEY for DNSSEC key stuff
  - CSYNC for NS / glue / <other>

Questions?

Another proposal...

draft-andrews-dnsop-update-parent-zones-04



New rules.

- Child MAY publish both.
- Parent SHOULD choose one or the other.
- Parent SHOULD NOT perform consistency check between CDS and CDNSKEY.
- Limits error conditions / complexity.

More info

- Automating DNSSEC delegation trust maintenance (draft-kumari-ogud-dnsop-cds-05) https://datatracker.ietf.org/doc/draft-kumari-ogud-dnsop-cds/

- Child To Parent Synchronization in DNS (draft-hardaker-dnsop-csync-02) https://datatracker.ietf.org/doc/draft-hardaker-dnsop-csync/

- Updating Parent Zones (draft-andrews-dnsop-update-parent-zones-04) https://datatracker.ietf.org/doc/draft-andrews-dnsop-update-parent-zones/

POC Implementation

```
def CDS(name):
// d_lookup() enforces DNSSEC validation of lookup
// common() finds a key that is in both sets and signs second set
// verify() performs DNSSEC verification of set using specified key
C= d_lookup(name, CDS)
if (C == NULL)
  C = d_lookup(name, CDNSKEY)

if (C != NULL)
 // CDS or CDNSKEY exist so DS and DNSKEY exist
 D = d_lookup(name, DS)
 K = d_lookup(name, DNSKEY)
 same = common(C, K)
 if (verify( C, same) && verify(K, same))
   print C
```