RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Implementing RFC 7344

Automating DNSSEC Trust Maintenance

Ondřej Caletka | 24 February 2021 | DNS WG

Reverse DNS Domain Registry

- Provisioned using `DOMAIN` objects in the RIPE Database
- Delegation to other DNS servers using “`nserver:`” attribute
- Secure delegation using “`ds-rdata:`” attribute

```
domain:         8.b.d.0.1.0.0.2.ip6.arpa
descr:          rDNS for my IPv6 network
admin-c:        NOC12-RIPE
tech-c:         NOC12-RIPE
zone-c:         NOC12-RIPE
nserver:        pri.example.net
nserver:        sns.company.org
ds-rdata:       45062 8 2 275d9acbf3d3fec11b6d6…
mnt-by:         EXAMPLE-LIR-MNT
created:        2015-01-21T13:52:29Z
last-modified:  2016-02-07T15:09:46Z
source:         RIPE
```

Automating Trust Maintenance

- RFC 7344 and RFC 8078
- Child zone **publishes** CDS and/or CDNSKEY records
- Parent zone **adjusts DS record** accordingly
- The change is **secured by DNSSEC** and other safeguards
- Child can request **deletion of DS records** (switch to insecure)
- Insecure to secure bootstrapping possible (with caution)
- Implemented in *a few* TLD registries: .cz, .ch, .li, .cr, .sk

CDS Scanning at the RIPE NCC

- About to **go live** soon
- Scanning **only for CDS** records on **already secure** delegations
- No support for insecure-to-secure bootstrap
- Support for **switching to insecure** with `CDS 0 0 0 00`
- Safeguards against malicious changes:
  - CDS has to have valid DNSSEC signature
  - CDS must be signed by KSK
  - CDS must not break secure delegation
  - Harden against replay of previous CDS records

Replay Attack Protection

> The Parental Agent **MUST** ensure that previous versions of the CDS/CDNSKEY RRset **do not overwrite more recent versions.** This MAY be accomplished by checking that the signature inception in the Resource Record Signature (RRSIG) for CDS/CDNSKEY RRset is later and/or that the serial number on the Child's Start of Authority (SOA) is greater. This may require the Parental Agent to **maintain some state** information.
>
> **RFC 7344, section 6.2**

- We compare "`last-modified:`" attribute of the `DOMAIN` object with the signature inception date of `CDS` record
- All CDS records signed before the last modification of `DOMAIN` object are **ignored**

Signer and Continuity Check

Signer: **MUST** be signed with a key that is represented in both the current DNSKEY **and DS** RRsets,…

Continuity: **MUST NOT** break the current delegation if applied to DS RRset.

RFC 7344, section 4.1

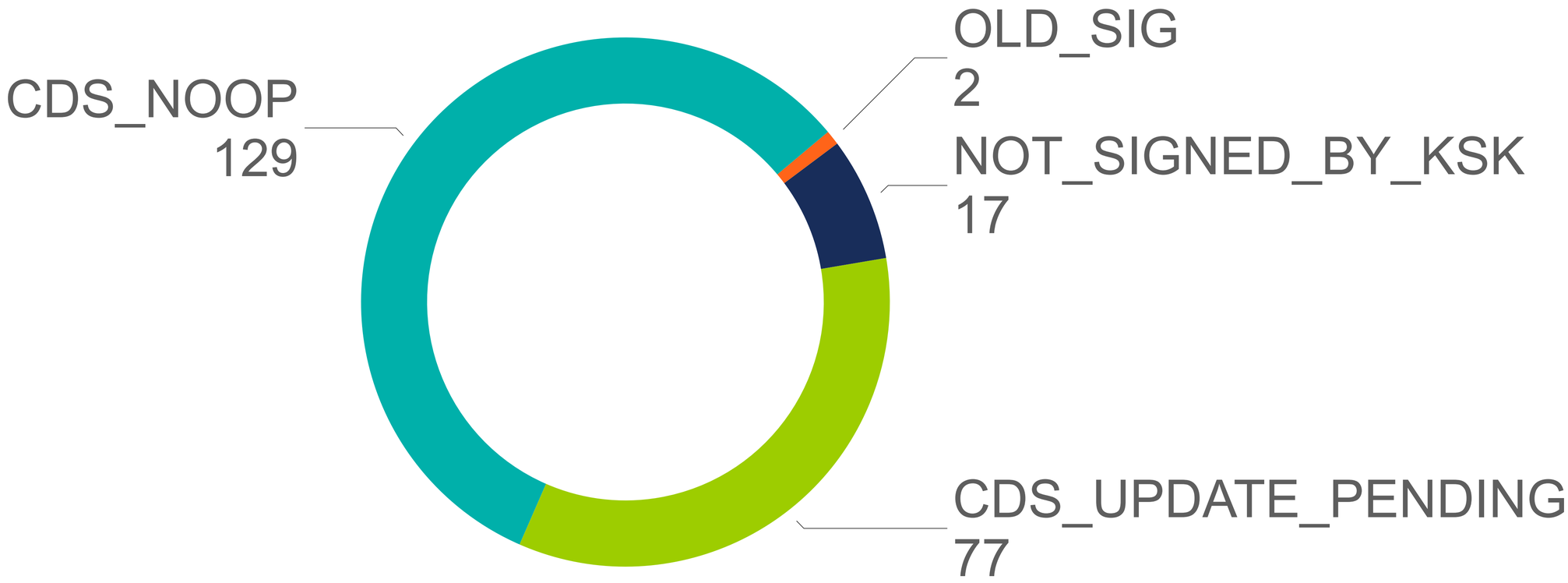
- We check whether the CDS is signed by a key whose digest is in the current "ds-rdata:" attribute of the DOMAIN object
- For **each algorithm** present in CDS RRSet, we check whether there is **at least one** matching key and signature of the DNSKEY RRSet

Updating the RIPE Database

- We have to use the RIPE NCC's *superpowers* to override the authorisation of `DOMAIN` object edits
- No locking mechanism, possibility of race conditions
- The risk is minimised by doing a **fast GET-modify-PUT** cycle
- Update is **cancelled** if "`last-modified:`" attribute has changed since the CDS scan
- The RIPE Database will send a standard e-mail '*Notification of RIPE Database changes*', if configured to do so

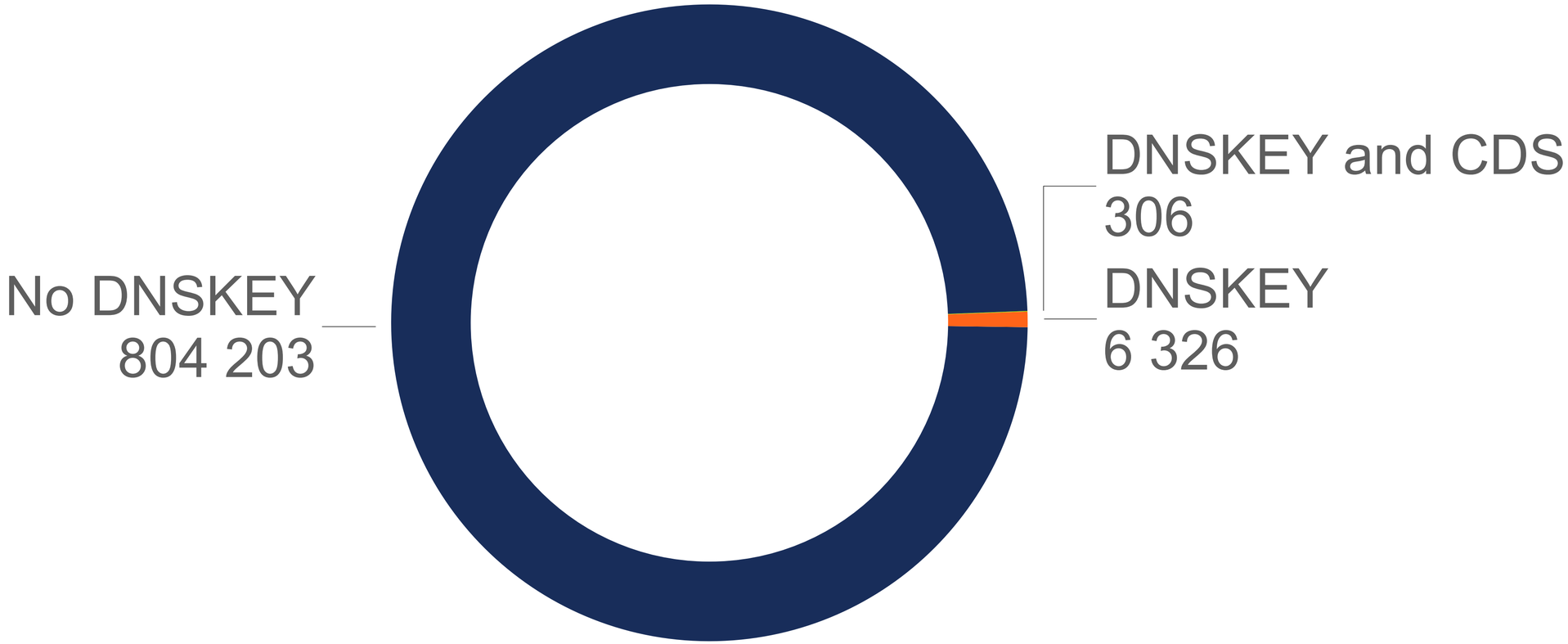
CDS Presence

CDS Scan Results



Secure vs. insecure delegations

Insecure delegations



Questions

ondrej.caletka@ripe.net
@ripencc