



RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Deployment of CDS

Automating DNSSEC maintenance

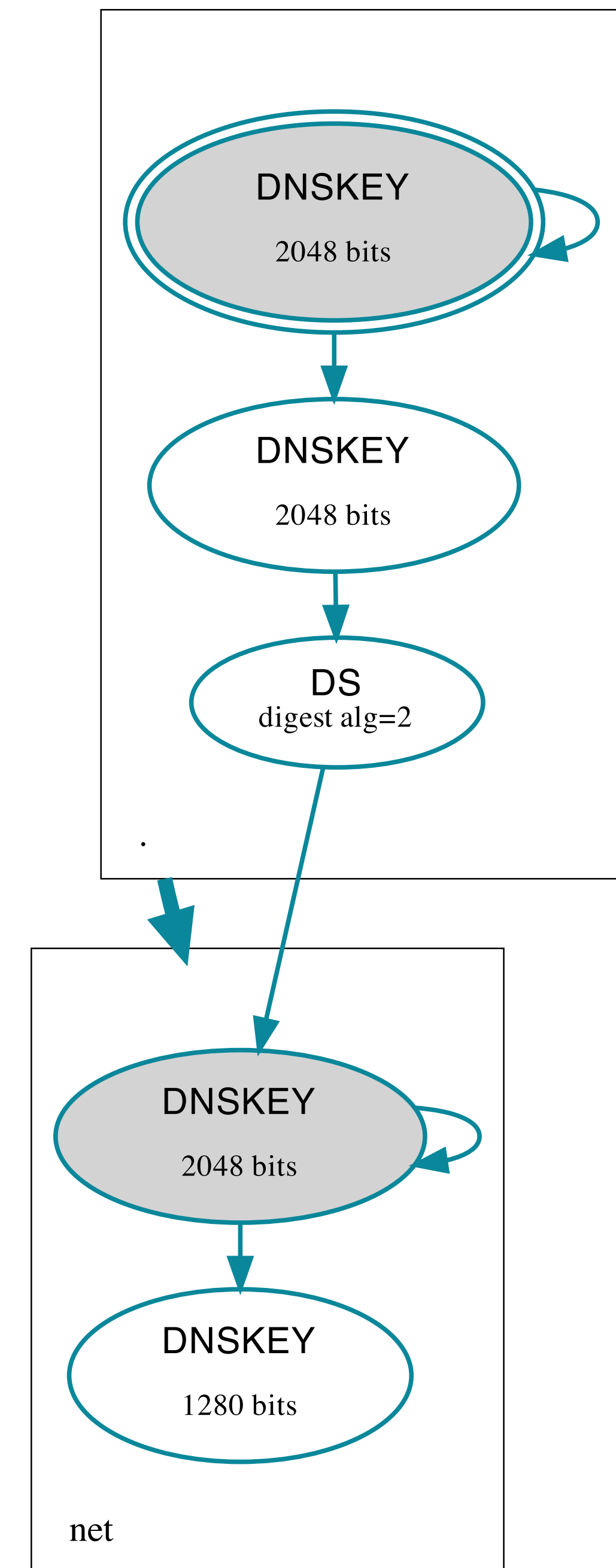
Ondřej Caletka | 19 May 2021 | RIPE 82

Trust model of DNSSEC



- Every zone is an *island* with its own signatures and public keys
- Trust is delegated from the parent zone by DS records
- DS records are unique for particular **key**, **hash function** and **zone name**

$$DS = \text{hash}(\text{DNSKEY} + \text{zonename})$$



Updating the DS records



- Submit DS records directly
 - via *Extensive Provisioning Protocol* if you are a *registrar* and parent is a *registry*
 - via e-mail, web interface, or custom API to your *registrar*
 - as a *zonelet* containing the DS records if your parent uses plain zone files
- Submit DNSKEY and let the parent calculate DS
 - the **only supported option** for some TLD *registries* like .eu or .cz
 - allows **easy key sharing** between different domain names
 - allows parent to be in control of the used **hashing algorithm**

Use of CDS/CDNSKEY records



- In-band signalling for change in parent delegation
- Child publishes desired state of DS records in the zone
 - SHOULD publish both CDS and CDNSKEY and they MUST match
- Parent consumes either CDS or CDNSKEY
 - the CDS content replaces current DS set
 - no CDS means no update
 - a special DNSSEC Delete algorithm for removing DS records
- Bootstrapping from insecure to secure
 - usually by TCP queries to all authoritative servers over a longer time period

Registries supporting CDS



Registry	CDS	CDNSKEY	Delete	Bootstrap from insecure	Notes
.cz				7 days TCP-only	FRED is used
.cr				7 days TCP-only	No info found; FRED is used
.ch				72 hours TCP-only	
.li				72 hours TCP-only	
.sk				72 hours	No clear information about using TCP for bootstrap
RIPE NCC				No support	

DNS providers supporting CDS



Provider	CDS	CDNSKEY	Delete
Cloudflare			
DNSimple			
GoDaddy			
Google Domains			

Self-hosted DNSSEC solutions



- CDS publishing supported in **Knot DNS, BIND9, PowerDNS**
- **Fully automated** KSK rollovers in Knot DNS
- Manual intervention needed to finish the key rollover in others
- All of them publish both CDS and CDNSKEY records

```
DS check, outgoing, remote ::1@53, KSK submission check: positive
DS check, outgoing, remote 2001:4860:4860::8888@53, KSK submission check: positive
DS check, outgoing, remote 2606:4700:4700::1111@53, KSK submission check: positive
DNSSEC, KSK submission, confirmed
DNSSEC, signing zone
DNSSEC, key, tag 12829, algorithm ECDSAP256SHA256, KSK, public, active
DNSSEC, key, tag 55288, algorithm ECDSAP256SHA256, KSK, public, active+
DNSSEC, key, tag 39374, algorithm ECDSAP256SHA256, public, active
DNSSEC, signing started
DNSSEC, zone is up-to-date
```

Parent-side software



- dnssec-cds
 - part of BIND9 meant to keep DS *zonelets* up to date
 - can read both CDS and CDNSKEY records
 - can produce a script for nsupdate utility
- parts of FRED registry
 - fred-akm: scanning management
 - cdnskey-scanner: the actual scanner worker
 - akm-multi-scanner: next generation scanner
 - probably hard to reuse outside FRED *registry*

Adoption slowly grows



- CDS updates are well supported in DNSSEC software
 - confirmed with RIPE NCC CDS scanner: there are **already users out there**
- Single, standard way to perform updates seems beneficial even for *registrars* with EPP access to *registries*
 - there are many incompatible dialects of EPP
- List of *registries* is *slowly* growing
- Join the **CDS Updates** channel on DNS-OARC Mattermost



Questions



ondrej.caletka@ripe.net
[@ripencc](#)