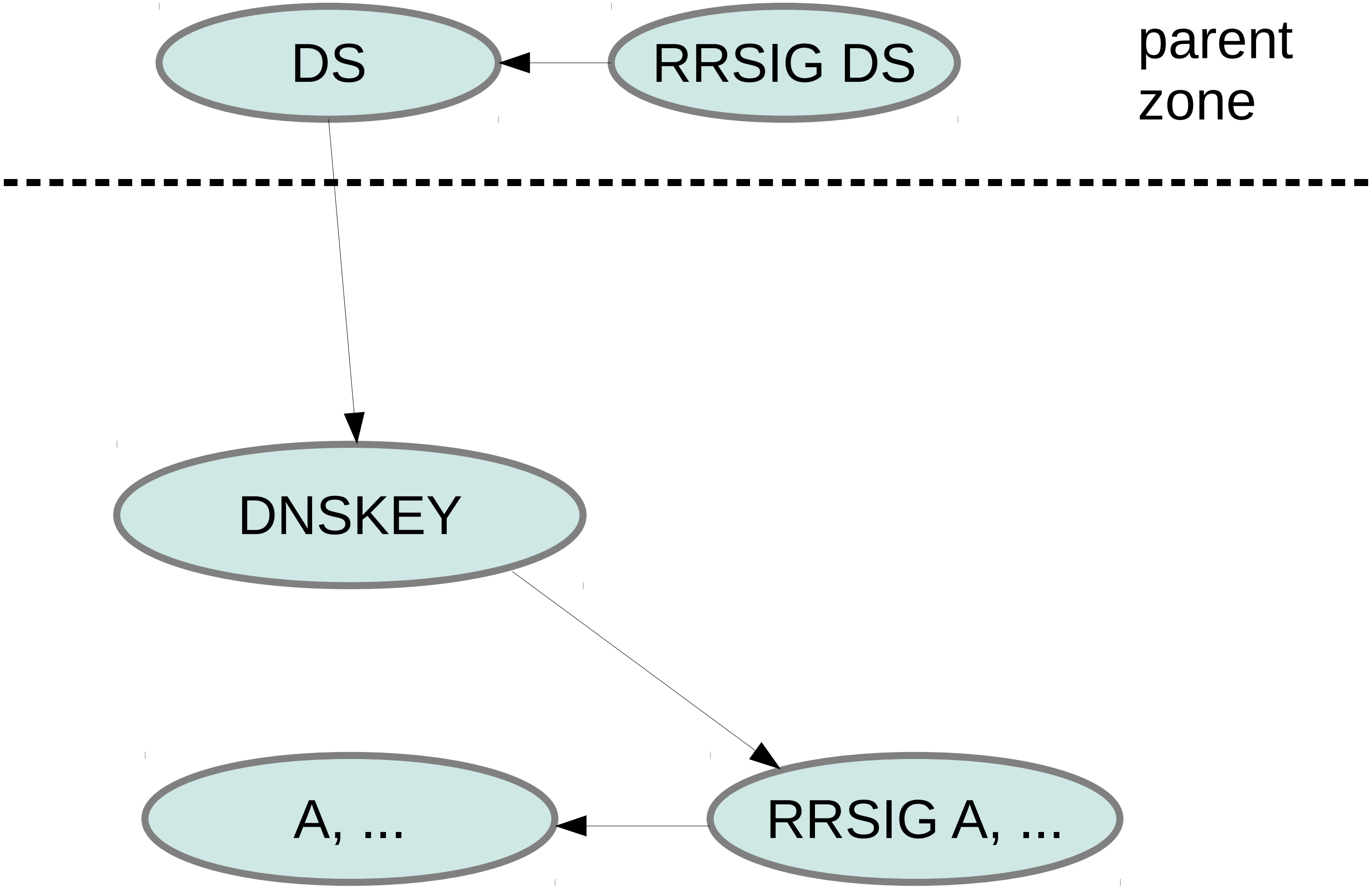
Automating DNSSEC

Libor Peltan • libor.peltan@nic.cz • 2019-06-03

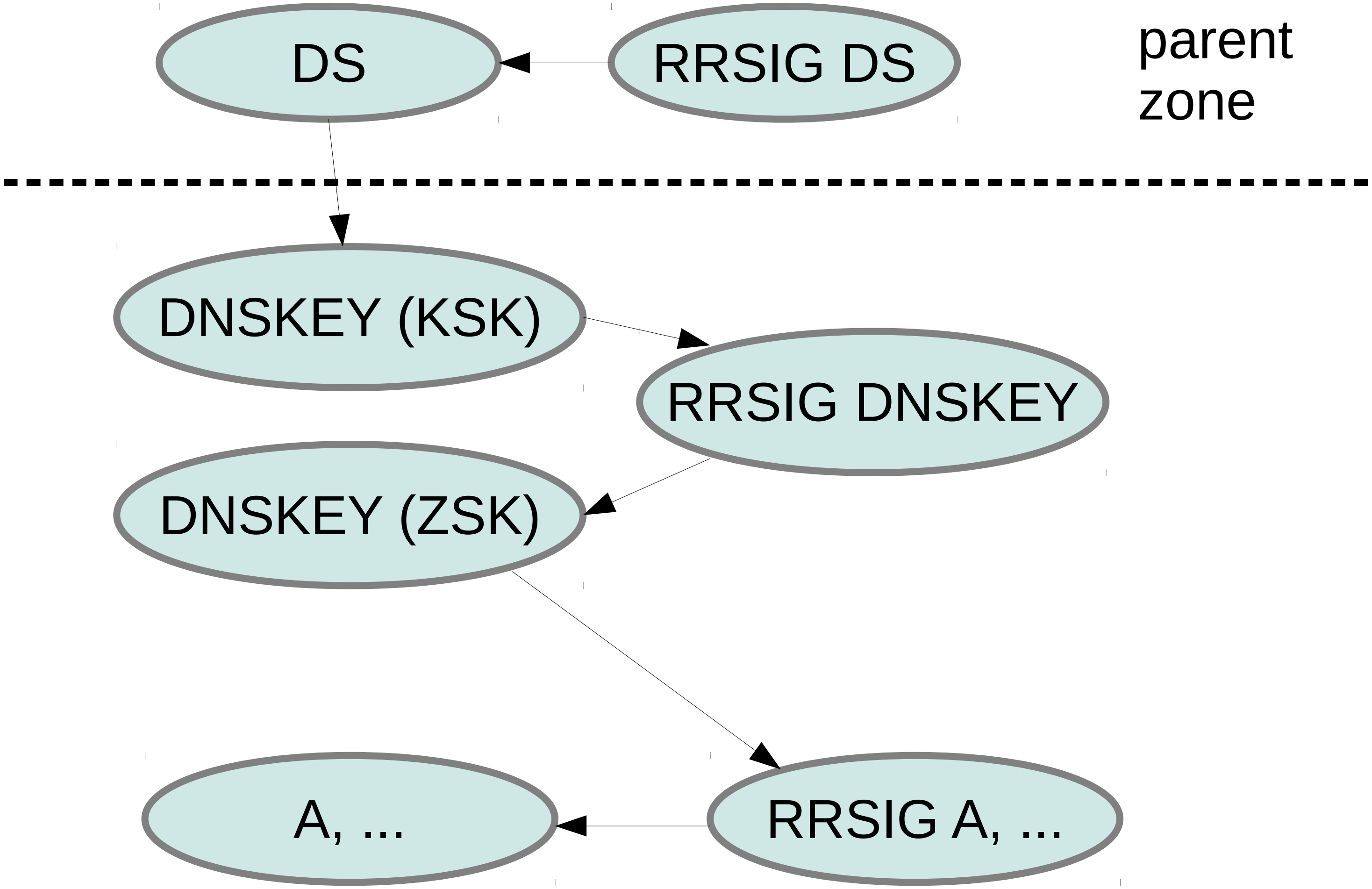
What is DNSSEC (good for)

- Between Authoritative server and Recursive resolver
- Protection against spoofing and modification of DNS responses
- Ensure data integrity even for negative answers
- Each DNS response is signed by asymmetric key
- Signatures can be pre-computed
- No encryption, everything sent in open form

DNSSEC for one zone



DNSSEC for one zone



DS

RRSIG DS

parent
zone

DNSKEY (KSK)

RRSIG DNSKEY

DNSKEY (ZSK)

A, ...

RRSIG A, ...

Reasons for KSK+ZSK

- ZSK can be exchanged w/o updating delegation
- ZSK can be weaker => smaller signatures => traffic
- Managed by separate teams
- Possible Offline KSK

DNSSEC needs maintenance

- Refresh RRSIGs soon enough
- ZSK and KSK shall be changed sometimes
- Key roll-overs need propagation delays
- Algorithm change is a complicated roll-over

...how to take care of it all? Configure the server to take care for you.

Implementation in software

- OpenDNSSEC – ZSK, KSK, Alg rollover
- PowerDNS – only manual rollovers
- BIND9 – only manual, can be pre-planned
- Knot DNS – ZSK, KSK, Alg rollover

  – fully automatic!

Configuration example (Knot DNS)

```
policy:
  - id: my_policy
    algorithm: RSASHA256
    ksk-size: 2048
    zsk-size: 1024
    rrsig-lifetime: 7d
    rrsig-refresh: 1d

zone:
  - domain: example.com.
    dnssec-signing: on
    dnssec-policy: my_policy
```

RRSIGs‘ validity is limited

Knot takes care of re-signing
when RRSIGs are gonna expire

Configuration example (Knot DNS)

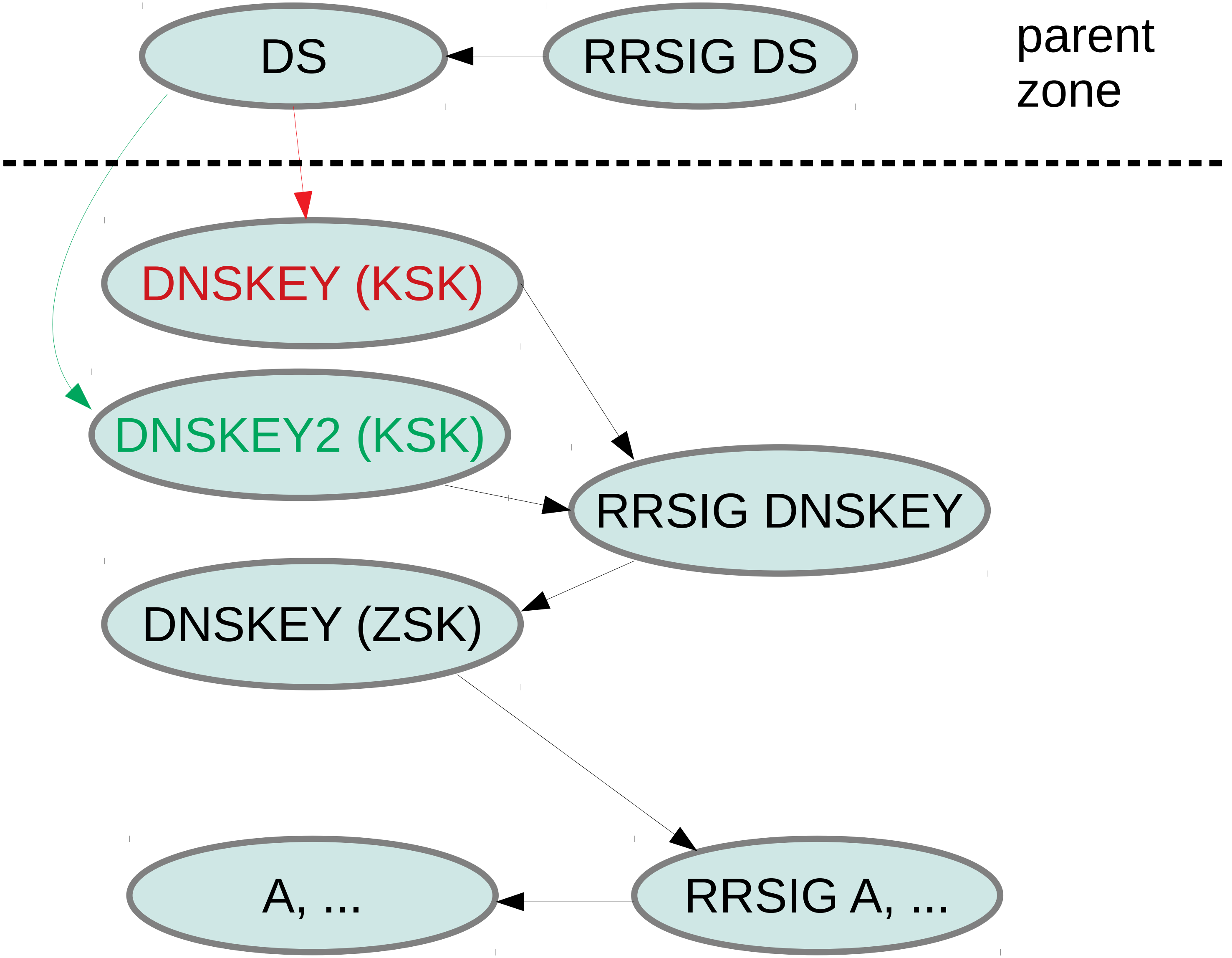
```
policy:
  - id: my_policy
    algorithm: RSASHA256
    ksk-size: 2048
    zsk-size: 1024
    rrsig-lifetime: 7d
    rrsig-refresh: 1d
    zsk-lifetime: 30d
    ksk-lifetime: 365d
    propagation-delay: 1d

zone:
  - domain: example.com.
    dnssec-signing: on
    dnssec-policy: my_policy
```

Keys‘ validity is limited

Knot performs key rollover,
re-signing the zone as needed

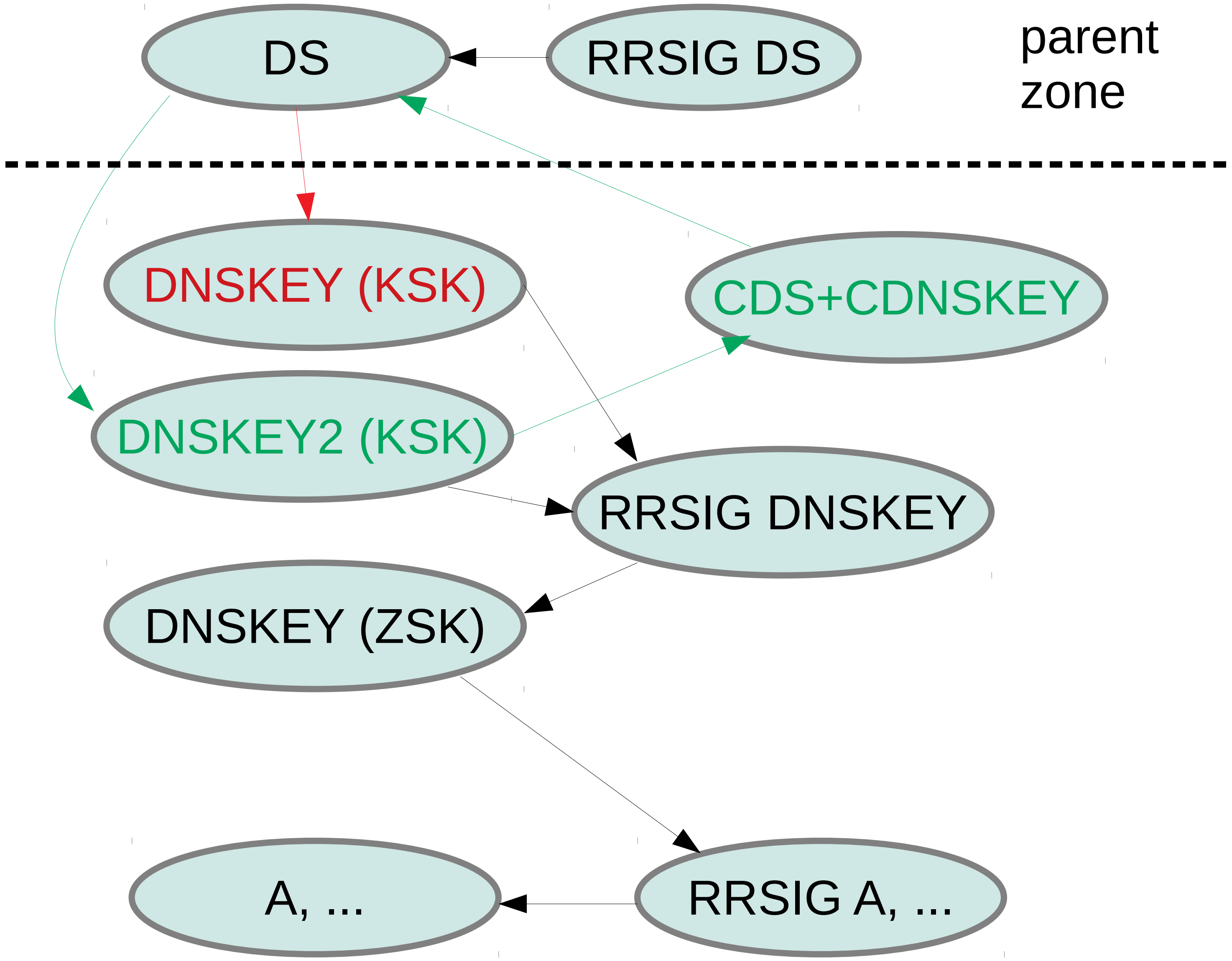
Challenge: update secure delegation



Challenge: update secure delegation

- No standard for direct update of DS
- Signaling with CDNSKEY and CDS records
  - Support:
    - PowerDNS (partial), BIND9 (partial)
    - Knot DNS
  - Not clear whether and when DS updated
  - Parent should periodically scan for CDS
    - Implemented e.g. in .CZ, .AT, .CH, .LI TLD
- Need to check parent DS periodically

Challenge: update secure delegation



Configuration example (Knot DNS)

```
policy:
  - id: my_policy
    ...
    propagation-delay: 1d
    ksk-lifetime: 365d
    ksk-submission: my_subm
```

CDNSKEY & CDS
published by default

```
zone:
  - domain: example.com.
    ...
```

```
remote:
  - id: pub_resolver
    address: 8.8.8.8
```

(or authoritative servers instead)

```
submission:
  - id: my_subm
    parent: pub_resolver
    check-interval: 1h
```

Knot asks configured server for updated parent DS periodically

Logging example (Knot DNS)

```
notice: [example.com.] DNSSEC, KSK submission,
waiting for confirmation

info: [example.com.] DS check, outgoing, remote
127.0.0.1@22619, KSK submission attempt: negative

…

info: [example.com.] DS check, outgoing, remote
127.0.0.1@22619, KSK submission attempt: positive

notice: [example.com.] DNSSEC, KSK submission,
confirmed
```

Algorithm rollover

- More steps than KSK rollover
- Same prerequisites (configured KSK submission)
- Simply change algorithm in policy config

Summary

- DNSSEC is dynamic and complex
- It’s easy to automate
- No further maintenance needed
- Please use DNSSEC!