

EPP keyrelay:

A solution for DNS operator changes with DNSSEC

10-04-2013

ICANN DNSSEC workshop

Beijing

Antoin Verschuren

DNSSEC in .nl

Recent figures:

- 5.211.124 domains
- 1.425.018 DNSSEC domains (27,35%)
- 57.479 Bogus (4,05% of DNSSEC domains)
- Many bogus due to transfer/dns operator change

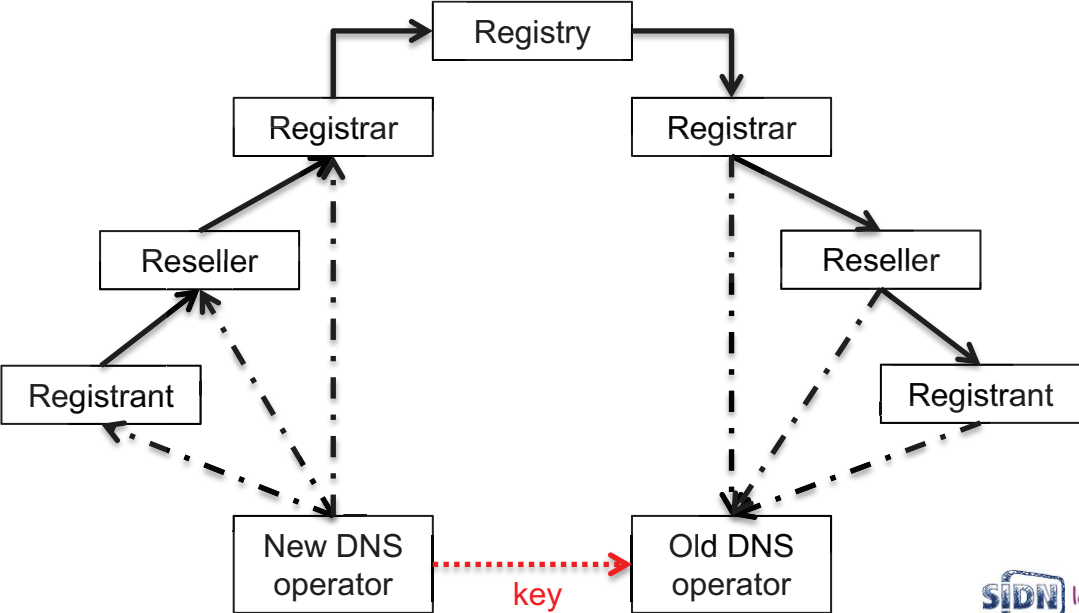
DNS operator changes with DNSSEC

- The problem of DNS operator changes with DNSSEC have been discussed, also in this workshop.
- See [draft-koch-dnsop-dnssec-operator-change](#)
- Not going to repeat, I assume it is understood.
- Let's talk solutions.

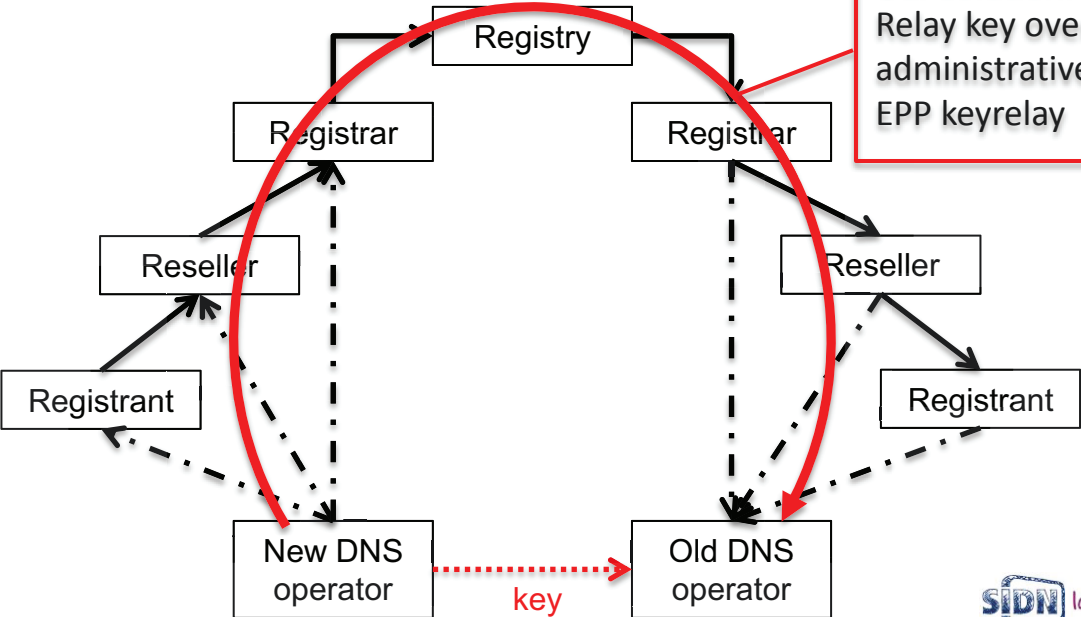
Solutions so far

- Go insecure. Not acceptable for some, certainly not in the future.
- Copy zone with AXFR and set real small TTL's. Will still break DNSSEC for seconds.
- Pre-publish new ZSK in old zone. Needs the old DNS operator to cooperate, and the new key to travel from new to old DNS operator.

Transferring a key



Transferring a key



Our solution:
Relay key over existing
administrative channel:
EPP keyrelay

EPP keyrelay

- Simple extra process before initiating transfer/NS change
- Step1: Gaining DNS operator sends key upwards to registry
- Step2: Registry puts key in current registrar's EPP poll queue
- Step3: Losing DNS operator receives key from above
- <https://datatracker.ietf.org/doc/draft-gieben-epp-keyrelay/>

Gaining operator
configures zone with
old ZSK included

Losing operator receives
new ZSK, includes ZSK in
zone and resigns

Keyrelay
(new ZSK
+token)

Gaining operator
configures zone with
old ZSK included

Losing operator receives
new ZSK, includes ZSK in
zone and resigns

Wait TTL old DNSKEY
RRset after seeing
new ZSK in old zone

Keyrelay
(new ZSK
+token)

Transfer

secure

Add DS

Gaining operator
configures zone with
old ZSK included

Losing operator receives
new ZSK, includes ZSK in
zone and resigns

Wait TTL old DNSKEY
RRset after seeing
new ZSK in old zone

Wait TTL NS
RRset old zone

Keyrelay
(new ZSK
+token)

Transfer

secure

Add DS

NS change

Remove
old DS

Gaining operator
configures zone with
old ZSK included

Losing operator receives
new ZSK, includes ZSK in
zone and resigns

Wait TTL old DNSKEY
RRset after seeing
new ZSK in old zone

Wait TTL NS
RRset old zone

Keyrelay
(new ZSK
+token)

Transfer

secure

Add DS

NS change

Remove
old DS

insecure

Losing operator
uncooperative

Gaining operator
configures zone with
old ZSK included

Losing operator receives
new ZSK, includes ZSK in
zone and resigns

Wait TTL old DNSKEY
RRset after seeing
new ZSK in old zone

Wait TTL NS
RRset old zone

Keyrelay
(new ZSK
+token)

Transfer

secure

Add DS

NS change

Remove
old DS

insecure

Remove
all DS

NS change

Add DS

Losing operator
uncooperative

Wait TTL DS RRset
parent zone

Wait TTL NS
RRset old zone

Requirements met for EPP keyrelay

Feedback from registries, registrars, DNS operators:

- Must work with losing operator uncooperative
- Gaining registrar/registrant/operator in control
- No state/timers at registry
- Must be fully automatable, no manual steps
- No changes/undefined state in registry database
- Must work with all combinations of DNS operators
- Registrant must approve changes to zone
- Relayed key removed when transfer abandoned
- Must also work when no transfer, only operator change
- Easy to implement, no major changes to current processes

Running code !

- .nl registrars support this method
- Independent of (non)existing business roles or processes
- Scalable existing secure channel through registry
- Easy to implement extension

- .nl will implement EPP keyrelay in May 14 release
- Implemented in EPP clients (Net::DRI release)

Questions

Antoin Verschuren
antoin.verschuren@sidn.nl

www.sidn.nl | www.sidnlabs.nl



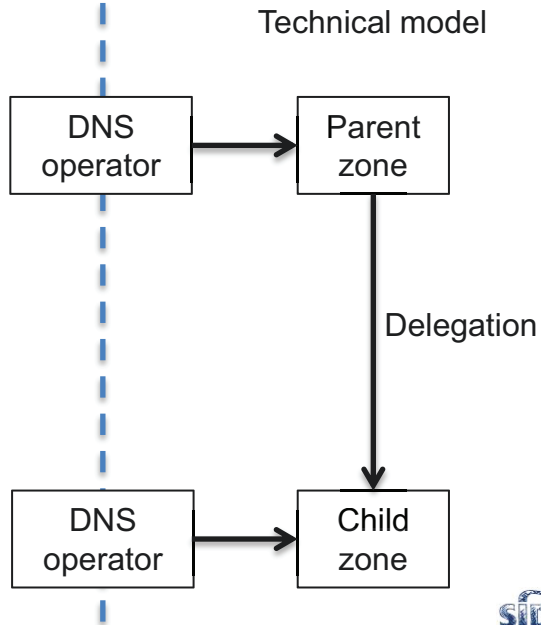
Why is transferring a key such a hassle?

- DNS operators are not defined in the administrative model
- DNS operators are entities that can have multiple hats (registrars, registrants, resellers, 3th party hosters) that confuses people in the discussions
- DNS operators don't talk to each other directly, only DNS was used so far, there is no direct administrative channel.
- With DNSSEC, only the DNS operator owning the delegation and DS at the parent can be queried securely over DNS.
- DNS operators are often competitors

The model

Administrative model

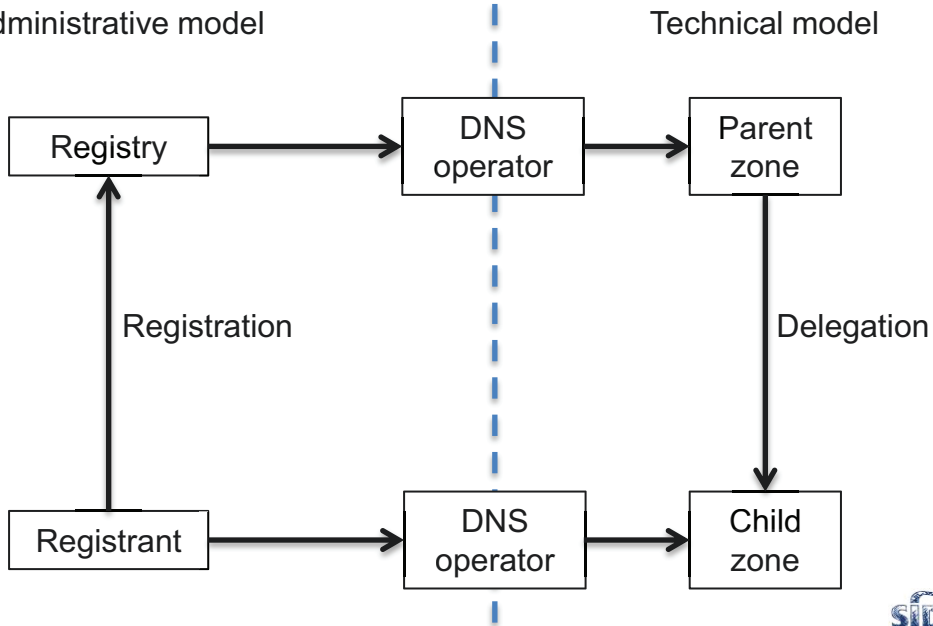
Technical model



The model

Administrative model

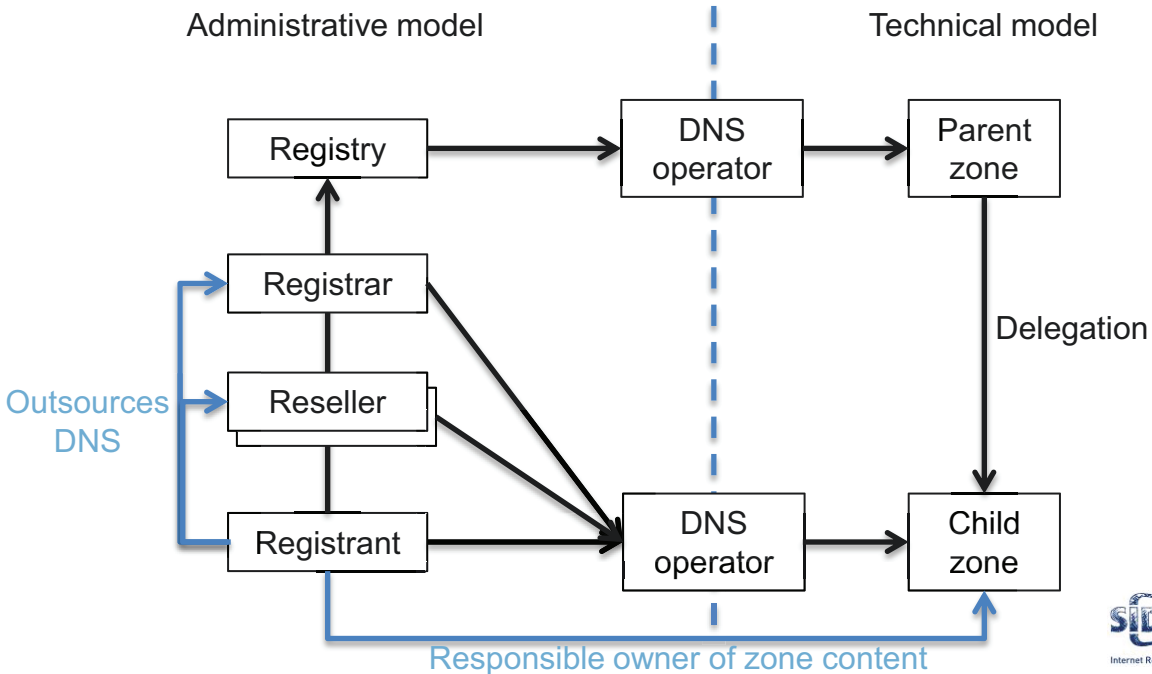
Technical model



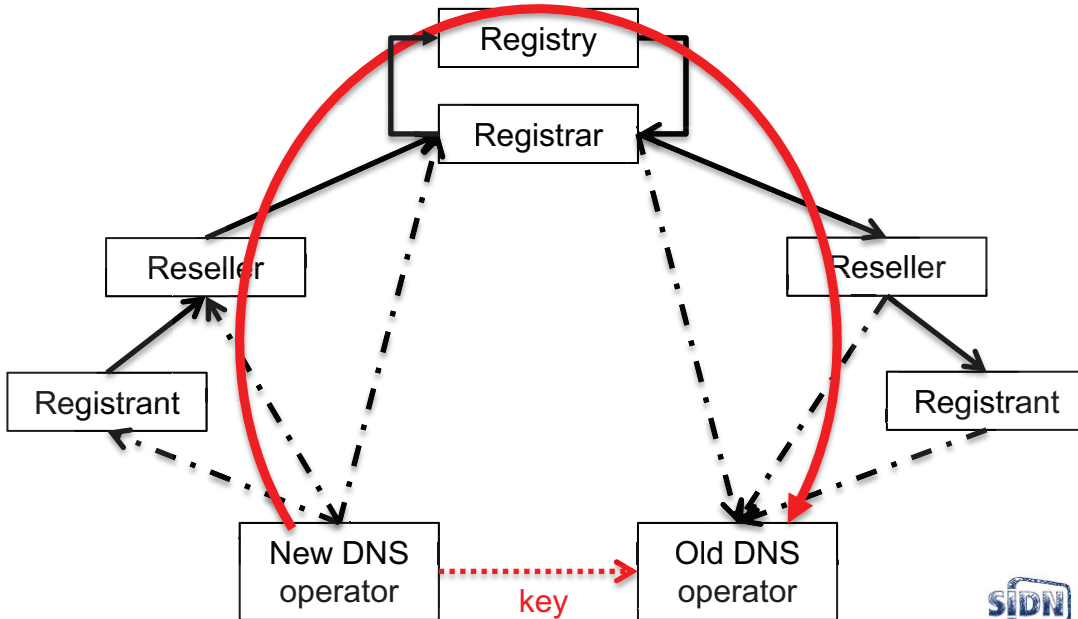
The model

Administrative model

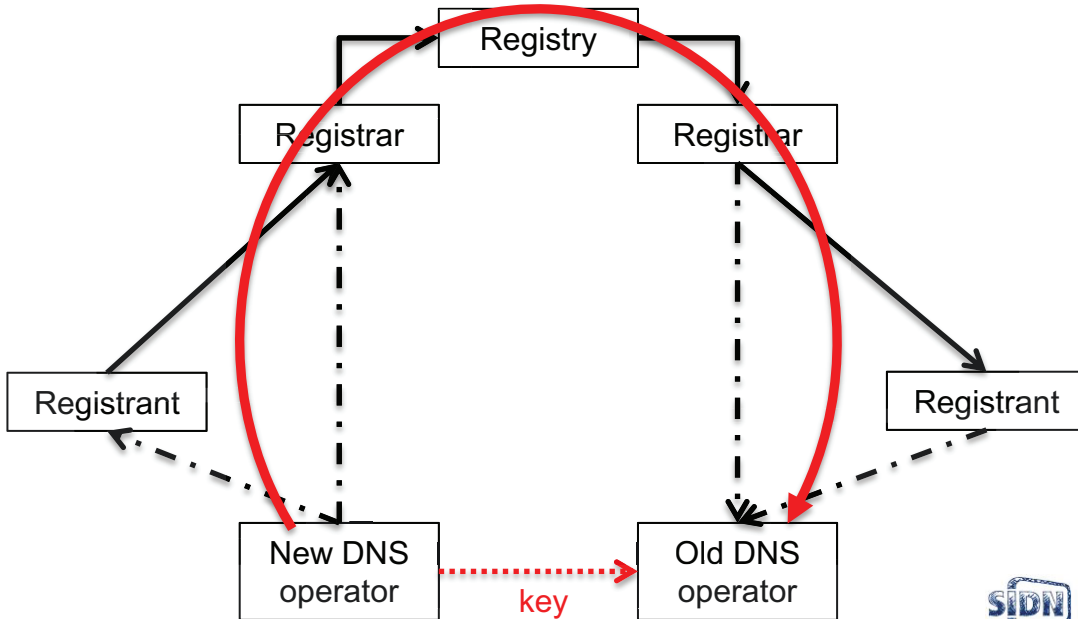
Technical model



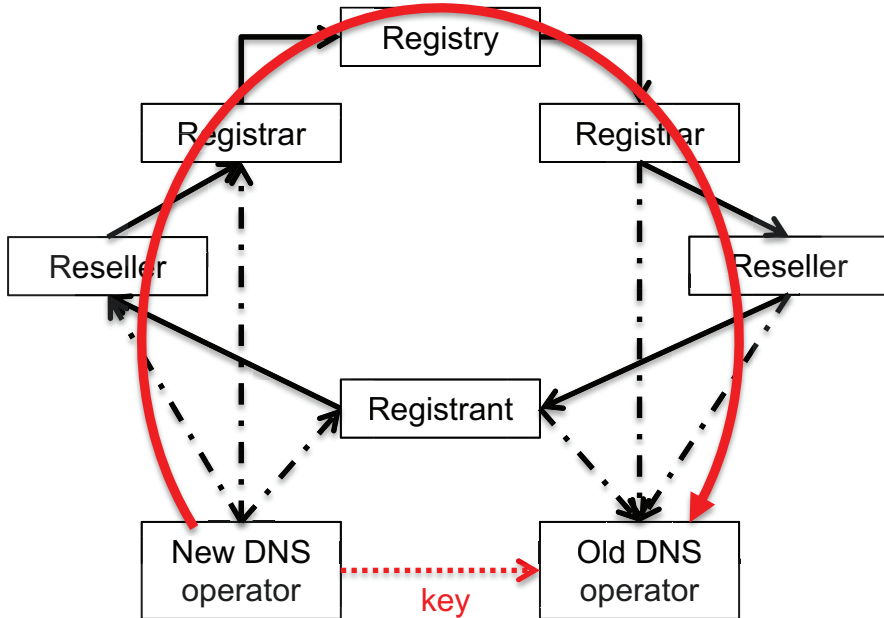
Transferring a key



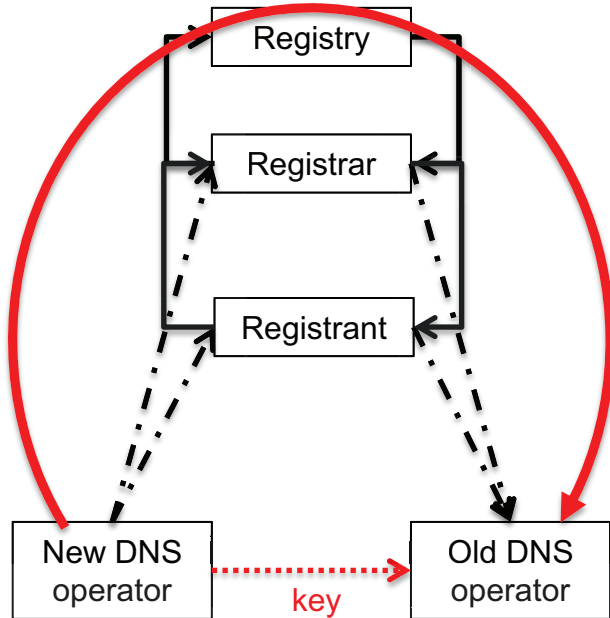
Transferring a key



Transferring a key



Transferring a key



Transferring a key (for Ed)

