EPP keyrelay:
A solution for
DNS operator changes with DNSSEC
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.
Transfering a key
Transfering 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

Add DS
Keyrelay
(new ZSK + token)

Transfer

Add DS

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

Wait TTL NS RRset old zone

Gaining operator configures zone with old ZSK included

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

secure

NS change

Remove old DS

Wait TTL NS RRset old zone

Gaining operator configures zone with old ZSK included

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

secure

NS change

Remove old DS

Wait TTL NS RRset old zone

Gaining operator configures zone with old ZSK included

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

secure

NS change

Remove old DS

Wait TTL NS RRset old zone
Gaining operator configures zone with old ZSK included

Keyrelay (new ZSK + token)

Transfer

Add DS

Secure

insecure

Losing operator uncooperative

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

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

NS change

Wait TTL NS RRset old zone

Remove old DS
Gaining operator configures zone with old ZSK included

Keyrelay (new ZSK + token)

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

Transfer  ->  secure  ->  Add DS

Losing operator uncooperative

insecure

Remove all DS  ->  insecure  ->  Add DS

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

Remove old DS

Wait TTL NS RRset old zone

NS change

Wait TTL NS RRset old zone

NS change

Wait TTL DS RRset parent 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, 3rd 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

Parent zone

Delegation

Technical model

DNS operator

Child zone
The model

Administrative model

- Registry
  - Registration

Technical model

- DNS operator
  - Delegation

- Parent zone
- Child zone
  - DNS operator
  - Registrant
The model

**Administrative model**

- Registry
- Registrar
- Reseller
- Registrant

**Delegation**

**Technical model**

- DNS operator
- Parent zone
- Child zone

- Responsible owner of zone content

Outsources DNS
Transferring a key

1. **Reseller** -> **Registrant** -> **Registrant**
   - New DNS operator
2. **Reseller** -> **Registrant** -> **Registrant**
   - Old DNS operator
3. **Registry**
4. **Registrar**
Transfering a key

Registry

Registrar

Registrant

New DNS operator

key

Old DNS operator

Registrant

Registrar
Transferring a key

- Registry
- Registrar
- Reseller
- Registrant
- New DNS operator
- Old DNS operator

Key transfer process:
1. New DNS operator requests the key from the old DNS operator.
2. The old DNS operator sends the key to the new DNS operator.
3. The new DNS operator verifies the key with the registry.
4. The registry forwards the key to the reseller.
5. The reseller forwards the key to the registrar.
6. The registrar forwards the key to the registrant.
7. The registrant forwards the key to the new DNS operator.
Transferring a key

Registry
Registrar
Registrant
New DNS operator
Old DNS operator

key
Transfering a key (for Ed)

- Registry
- Registrar
- Registrant
- Reseller
- New DNS operator
- Old DNS operator

Key