DNSSEC Secure transfers: It can be done

Antoin Verschuren, SIDNLabs.

When SIDN started to seriously prepare the operational implementation of DNSSEC back in 2008, one of the problems we encountered did not have to do so much with DNSSEC as a technology, but had much more to do with the administrative registry-registrar-reseller-registrant-dns-operator channel that was used for the registration of domain names. How could you transfer a domain name without interrupting validation from one dns-operator to another without them knowing of each others private keys to be used to sign the zone.

When we first discussed this with DNS-guru's, they were a bit deaf for this operational dilemma, but soon we found bystanders that saw the possible drawback for adoption of DNSSEC when this could not be solved. This has led to an internet draft which describes the procedure to follow when wanting to securely transfer a domain between 2 dns-operators: http://tools.ietf.org/html/draft-koch-dnsop-dnssec-operator-change-04

We wanted to know how this works in practice. We recently created a new network for our R&D activities, and we wanted to use the domain sidnlabs.nl that so far was controlled by our IT department. This would be an ideal test case to use, because it involved 2 different operational teams, but still with very short lines in communication. The domain name needed to be transferred from our IT department to our R&D department, and the domain had been DNSSEC signed in a production environment since SIDN's friend and fans faze for DNSSEC.

We followed the draft that we helped to develop, and we performed the dns-operator change in 14 steps. The zone sidnlabs.nl was delegated to ns1.sidn.nl and ns2.sidn.nl, both controlled by our IT department, and needed to be delegated to proteus.sidnlabs.nl controlled by our R&D department. These are the steps we took:

1. **Create new primary zone sidnlabs.nl on the new nameserver proteus.sidnlabs.nl**

2. **Create new DNSSEC keys for the zone sidnlabs.nl by the new operator**

3. **Enter the old ZSK from the old operator in the new unsigned zone by the new operator**

   We entered the DNSKEY record for the existing public ZSK from the old operator (key-tag 49698) into the new unsigned zone for sidnlabs.nl:

```
@               IN      SOA     proteus hostmaster.sidn.nl. (
                                1339658203      ; Serial
                                14400           ; Refresh (4 hours)
                                3600            ; Retry (1 hour)
                                604800          ; Expire (1 week)
                                3600            ; Negative caching (1 hour)
                                )

                IN      NS      proteus
                IN      NS      ns2.sidn.nl.
                IN      A       213.136.31.221
                IN      AAAA    2001:7b8:c05::80:4
                IN      DNSKEY  256 3 8 (
                                AwEAAdTI1IY5X1Caa/7P8xNWjjFU7SPUvlbA+UOGKong
                                Y/qELtpdk1qOx/lMrpqM/b6S4UoH9tBI/QAuiXTxMZFD
                                +QFZKNfluA/50gj59/k3XqSk3fQp8u5k1OBvUn68MiRR
                                w3ghzKcN9kQwJ5dTMOO1YRQZNtwVReYSuOjKFR9NvsZj
                                ) ; key id = 49689
www             IN      A       213.136.31.221
```

4. Sign the new zone with the new KSK/ZSK by the new operator.

Bind generates a warning when signing the new zone:

```
20-Jun-2012 08:49:43.310 general: warning: dns_dnssec_keylistfromrdataset:
error reading private key file sidnlabs.nl/RSASHA256/49689: file not found
```

Bind starts looking for the private key with key-tag 49689, the old ZSK from the old operator we inserted into the unsigned zone. Off course it cannot be found on the new system, since the new operator does not have that private key. Bind does sign the zone, but only with the new keys. The warning will remain every time Bind signs the zone, until the old key is removed from the zone.

Key-tags 55720 and 20853 are the new KSK and ZSK by the new operator. Key-tag 49698 is the old ZSK by the old operator. This is the zone created on the new nameserver proteus.sidnlabs.nl by the new operator:

```
sidnlabs.nl.          86400 IN DNSKEY 257 3 8 (
                          AwEAAaHexfzeKtEA3eEVxiJQUURcnqmN+kEJT0Zpr/qb
                          0Wzc3QnBvswopwP/Z+NIQFp0v30CK9FNT8cZTy4Qj7xV
                          eGLMAZqKO1yWSh0YXDhXhgLsbx1bToMkFyoYPvEk2qx1
                          CU0AWfVxSvs7eGaxaVJIv9K4yJwiyIf7wPFptWqLHf9M
                          lvUWDWpI2YwwjL0tULDZJ/OXnc2wmv9ZAztYZa2k7jqy
                          oBb1G/M0Y1ATRCcvZvc+QdEv8Qls8P3nMsREg3Ko5JAi
                          txFaibOvaz6ROQSe20SmrrddaMs4Dm5brXmWhfq25tRN
                          UIHaczUMJPxtLNEUqmgqewdDNAIPv4Y207zCWh0=
                          ) ; key id = 52720
sidnlabs.nl.         86400 IN DNSKEY 256 3 8 (
                          AwEAAdN5P6Ktkl4l3yxC/maZ2xza0Dq5oCBGYCif6ORP
                          NX2ZnYyIfCMZW4KvaOjFYeuNvpySJFliIc1UjM+OlWvj
                          LjK6xhX7HMXlWg/b2Rpgw3rwVDCEnK1PsCVg68S9KkT4
                          k93g/qlTvjqKcbH8bVZL6WOY+W6eKlCMdJFPeBpqnrmn
                          ) ; key id = 20853
sidnlabs.nl.         86400 IN DNSKEY 256 3 8 (
                          AwEAAdTI1IY5X1Caa/7P8xNWjjFU7SPUvlbA+UOGKong
                          Y/qELtpdk1qOx/lMrpqM/b6S4UoH9tBI/QAuiXTxMZFD
                          +QFZKNfluA/50gj59/k3XqSk3fQp8u5k1OBvUn68MiRR
                          w3ghzKcN9kQwJ5dTMOO1YRQZNtwVReYSuOjKFR9NvsZj
                          ) ; key id = 49689
sidnlabs.nl.         86400 IN RRSIG    DNSKEY 8 2 172800 20120714124942 (
                          20120614114942 52720 sidnlabs.nl.
                          eCvoYUCl9q6/z0UbHFGolUVLPAxwSdv2rJif20ML2BlC
                          k+0clGx4ALGEZoeYj+8oHmDp6Oq//p3457L5pBbPU35A
                          gYN/hKbT9hpIwhOU6cRZsd5iTnw7GQ9Bt4kMwxTBtURf
                          GpcDlmlK0bHM5Lr03RhMYFZGvIraNQ41kP0Bn8bjzLIq
                          dmkEgjMrwBdnRZdEWOPGCNr+IHu+KCbdKssyYCVx2w2g
                          ZyFMupSrcfDAA2XPITLC2ys4gJdIVcR4ArLx28us8Kv8
                          AurQzdQPDmsymsJdHIEcoTc0WasMizxBuHulVV0mgFHY
                          3fHEsP7kmUOaZNVYW2J3gIwXgj3FJJCMEQ== )
```

5. Enter the new ZSK in the old zone by the old operator

We emailed the new ZSK with key-tag 20853 pgp signed to the old operator who then entered the key in their version of the unsigned zone sidnlabs.nl on ns1.sidn.nl. The same as we did in step 3

6. Sign the old zone with the old KSK by the old operator

When the old operator resigned his version of the zone, the Bind signer tools generated the same warning as we had in step 4. The warning now complained about the private key with key-tag 20853 not being present, and that's correct, because the old operator does not have that new private key. Eventually the zone is signed with signatures from only the old keys, and this is the zone on ns1.sidn.nl:

```
sidnlabs.nl.        86400 IN DNSKEY     257 3 8 (
                          AwEAAbERFtxN3BuVMP6OKYe/Ca1S9jrzivoyKdN3XfTQ
                          OwSv4MbSOhXoJLdN5UuvXC7OzmJaUORLWvfJ7rc25yIp
                          MppjWJ6B7bT0dh89Hy2N7ntSZWxZzON3wK4us2Xeusyb
                          NmFMCeTtORsyMrSX6/jD/kApAG3RXcJh9upAoJMWWcFc
                          Rn51js/GUbwxrccGZWYtMi6knqWNXL7pC+uG5Kb8EKt6
                          C0Am8STCC6UKcWptd8PKgCBPkiDh5CJCbU68vWiPYLkh
                          2l+WSqTCQz+6CgdHQyxpF4mmgALmeSsNQIJevXVL8A2E
                          klD8x3aUaoEoplGS9Ox6IV91nV6u7+kbVijitMU=
                          ) ; key id = 61462
sidnlabs.nl.        86400 IN DNSKEY     256 3 8 (
                          AwEAAdN5P6Ktkl4l3yxC/maZ2xza0Dq5oCBGYCif6ORP
                          NX2ZnYyIfCMZW4KvaOjFYeuNvpySJFliIc1UjM+OlWvj
                          LjK6xhX7HMXlWg/b2Rpgw3rwVDCEnK1PsCVg68S9KkT4
                          k93g/qlTvjqKcbH8bVZL6WOY+W6eKlCMdJFPeBpqnrmn
                          ) ; key id = 20853
sidnlabs.nl.        86400 IN DNSKEY     256 3 8 (
                          AwEAAdTI1IY5X1Caa/7P8xNWjjFU7SPUvlbA+UOGKong
                          Y/qELtpdk1qOx/lMrpqM/b6S4UoH9tBI/QAuiXTxMZFD
                          +QFZKNfluA/50gj59/k3XqSk3fQp8u5k1OBvUn68MiRR
                          w3ghzKcN9kQwJ5dTMOO1YRQZNtwVReYSuOjKFR9NvsZj
                          ) ; key id = 49689
sidnlabs.nl.        86400 IN RRSIG DNSKEY 8 2 86400 20120721061503 (
                          20120621061503 61462 sidnlabs.nl.
                          rX6kn2AAIPzbbG89sf//+lV+dwr13qslZwqFF0pAoGa6
                          OGGKW5GtGbBFsosN8ZNlf7JisNkYfOKmif0apS0ecNQp
                          oCdkbWcVwXjO6zMdKRKoBVtCU/sGZFIXUOhE0hxphKB8
                          v8sIjQCHgnj+JOSpcdpFJfq55nAlGNxOBqjDmNeJmwAl
                          Vcs0g9IpfGpc8iJ8ALp0ve9HDsPYoHaJv6+FV+8mKEvs
                          uGFECBBjhaTxTNFowL0I+Ufor3rRTL4Dm8ybk8p8qBbE
                          j8/Zryy4iOUbF9ayuz490OlzaMQVF9q/A7rYldsPlrEP
                          wSEmLdyDBe3WVK+Fu6WSpR6QfYKiPR8nSg== )
```

7. Add a DS for the new KSK to the delegation at the registry

We then need to add the new KSK to the chain-of-trust by adding it's DS to the parent zone, so both versions of the zone can be validated. So there are temporarily a minimum of 2 DS records in the .nl zone for sidnlabs.nl. One DS from the old, and one DS from the new operator:

```
sidnlabs.nl.        7200 IN      DS 61462 8 2 (
                          D8A9F1AC8431429292E437DE7737AFCA8BA7A07529F0
                          87FB329503248289CAEA )
sidnlabs.nl.        7200 IN      DS 52720 8 2 (
                          ADA4B036E9BC9F5854A201329DFB04D376153A616C22
                          DD9E3B12CB4566CCC5DF )
```

8. **Wait for propagation of your new chain-of-trust for a minimum of 1 DNSKEY RRset TTL (old sidnlabs.nl zone) and 1 DS TTL (.nl zone)**

   Since it now was friday, we waited 2 days for propagation. We should have waited for at least 84600 seconds after step 6 and 7200 seconds after step 7, so 2 days was sufficient.

9. **ns2.sidn.nl had to run slave for sidnlabs.nl with proteus.sidn.nl as master in stead of ns1.sidn.nl**

   We kept the same slave server for sidnlabs.nl, so now that both versions of the zone could be validated we could configure ns2.sidn.nl to get the zone from proteus.sidnlabs.nl in stead of the version from ns1.sidn.nl.

10. **Change the delegation at the registry to the new NS set**

    Now that both new nameservers were configured, and both the new and old zone could be validated, we could at last change the nameservers in the .nl zone:

```
sidnlabs.nl.        7200 IN             NS proteus.sidnlabs.nl.
sidnlabs.nl.        7200 IN             NS ns2.sidn.nl.
```

11. **Wait 1 NS RRset TTL (old sidnlabs.nl zone) for propagation**

    We then had to wait 84600 seconds for propagation to make sure that all caching resolvers, both parent and child sticky and non-sticky resolvers had expired the old NS set in their cache.

12. **Remove the old DS for the old KSK at the registry**

    We could now delete the old DS from the old operator from the .nl zone, because the old zone would now not be queried anymore:

```
sidnlabs.nl.        7200 IN       DS 52720 8 2 (
                          ADA4B036E9BC9F5854A201329DFB04D376153A616C22
                          DD9E3B12CB4566CCC5DF )
```

13. **Remove the old zone from ns1.sidn.nl**

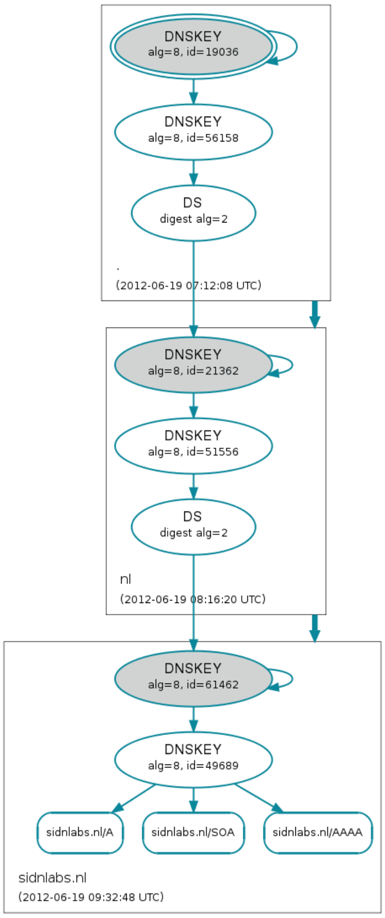
    We could now remove the old zone and old keysfrom ns1.sidn.nl..

14. **Remove the old ZSK from the DNSKEY RRset in the new sidnlabs.nl zone**

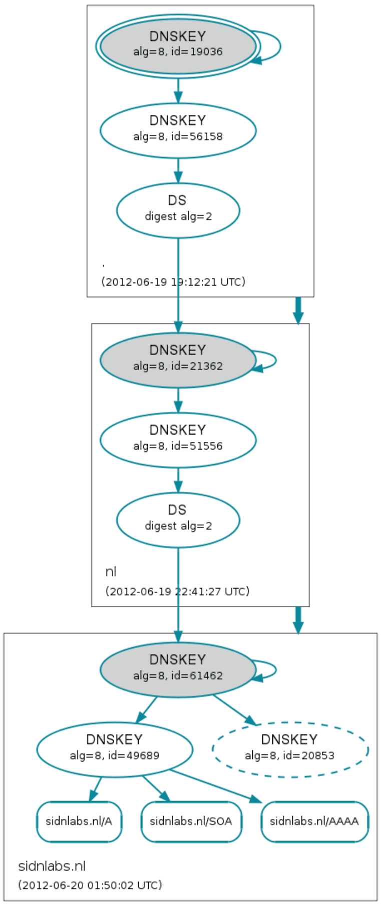
    And finaly we could remove the old ZSK from the new zone on proteus.sidnlabs.nl and the transfer was complete.

During the whole process, we checked the validation of the zone using different validating resolvers. Some resolvers had their cache flushed after each step, others were left untouched. The zone has also been monitored carefully with DNSVIZ (http://dnsviz.net/) to see if validation would remain intact.

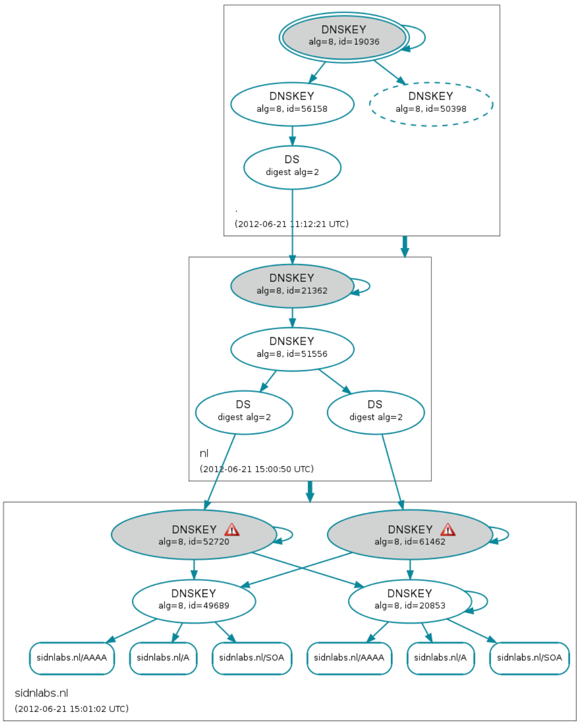
We have not seen any interruption in validation. We did see some interesting graphics that prove that the chain of trust remains intact. Especially the DNSVIZ 3 picture below which was taken just seconds after the first .nl server was updated with the new NS set for sidnlabs.nl but some other slaves were not yet, proves that even in those situations the entire zone remained secure:



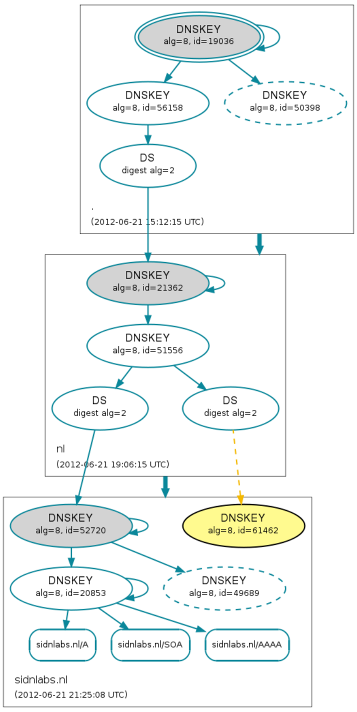
DNSVIZ 1: Step 1 to 5



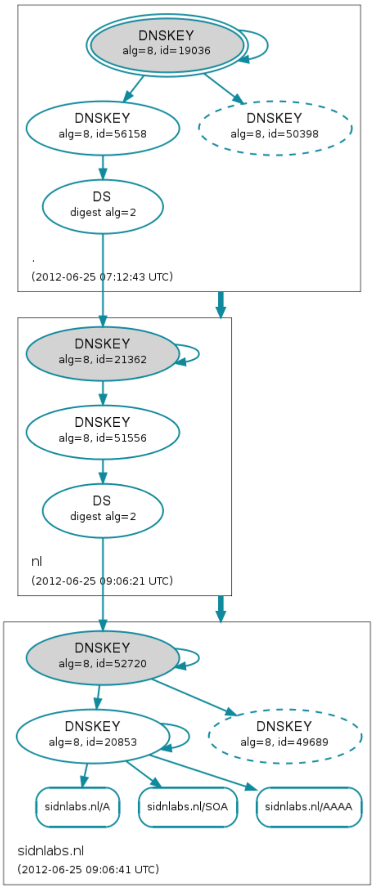
DNSVIZ 2: After step 6



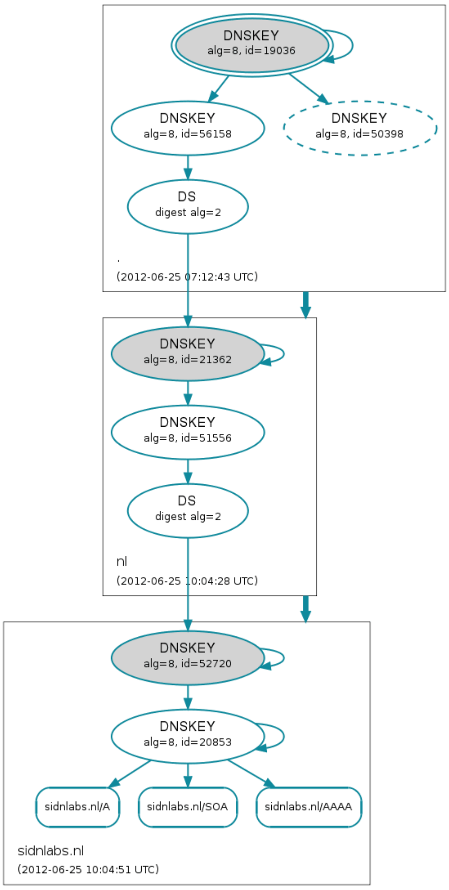
DNSVIZ 3: After step 10



DNSVIZ4: After step 11



DNSVIZ 5: After step 12



DNSVIZ 6: After step 14

So, secure DNSSEC transfers can be done. The only step in this process which is hard to automate is step 5 where the new operator needs to send his new ZSK to the old operator in a secure manner. The only safe channel that exists today is the administrative registry-registrar-reseller-registrant-dns-operator channel to get the key from one side to the other. It’s the same channel that is used to bootstrap a (secure) delegation when a domain is registered or secured with DNSSEC for the first time. It’s almost impossible to define a many-to-many communication protocol between dns-operators. So that’s why in the draft RFC we suggest to have the registry as a central point in the administrative chain function as a sort of trusted dropbox to get the key from the new to the old operator.