DENIC

Operator Change for DNSSEC Domains

Table of Contents

Introduction DNSSEC 3
- Requirements 3
- Roles 4
- Form of Presentation 4
- Initial situation 6

Case Studies DNSSEC 8
- Explanation 8
- Preparation Phase 8
- Operator Change Involving the Old Operator Without Provider Change 9
- Operator Change Involving the Old Operator With Provider Change 15
- Operator Change not Involving the Old Operator Without Provider Change 17
- Operator Change Not Involving the Old Operator With Provider Change 21

Introduction DNSSEC

Normally, "control" over the ZSK and possibly also over the KSK in a DNSSEC-enabled infrastructure will rest with the zone administrator. Often, the zone administrator is identical with the operator of the name server infrastructure, hereinafter referred to as "operator".

To change this operator, you must roll over the key(s) concerned and transfer DNS delegation to an infrastructure (set of name servers) that is independent of the "old" operator.

In this document, we explicate the steps which are necessary in the relevant scenarios to enable a key rollover and operator change without inconsistencies.

If you strictly follow the work schedules, no validation errors will occur because during the rollover procedure the validating resolver can retrieve its keys from both the old and the new operator.

> **Caution!**
>
> If you carry out an operator change in one single step, i.e. execute a change of delegation by only one single request, this will lead to validation errors!

A change of RegAcc not including an operator change, however, will remain feasible through one single CHPROV request without causing problems, even with DNSSEC domains.

Requirements

To use you must know the procedure of moving an unsigned .de domain from one operator to another and you must have basic knowledge about DNSSEC (meaning of KSK and ZSK and steps of domain signing procedure).

Roles

In this document, two roles will be distinguished:

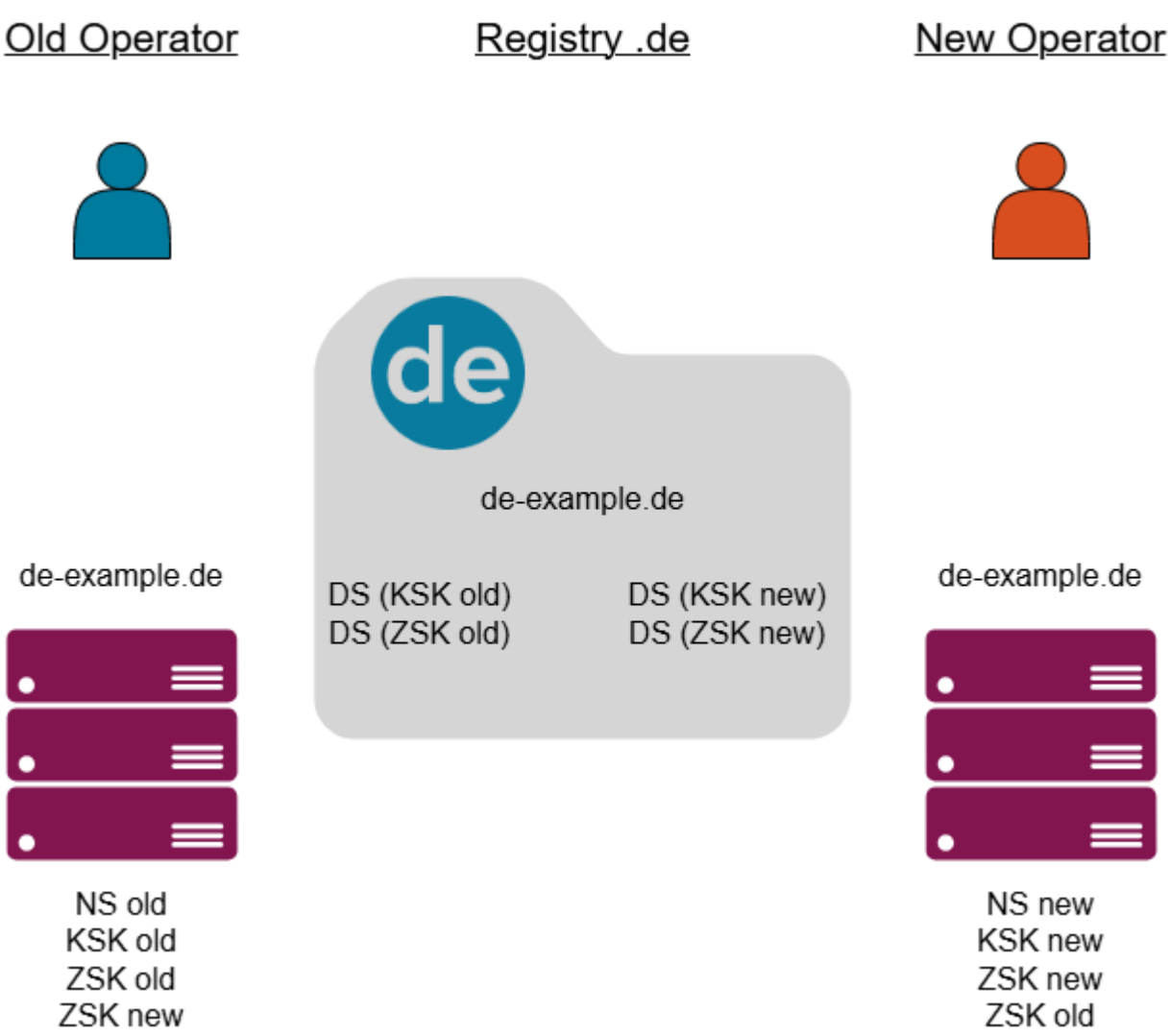
- Operator
- RegAcc

The RegAcc will be the DENIC member who administers the domain and who will make the changes in the database (Registry .de), whilst the operator will provide the name server infrastructure.

Form of Presentation

We have chosen the following form of presentation:

Figure 1: Example illustration



Explanation: All case studies in this document are based on the domain "de-example.de". We want to carry out an operator change for this domain. The two servers shown for the old and the new operator are just examples; they are not requirements. "NS old" and "NS new" represent the NS resource records of the de-example.de domain.

It is assumed that you are working with separate KSK and ZSK for the zone (de-example.de). The additions to the Delegation Signer (DS) "old" and "new" refer to the authoritative data origin. This origin may either be the old or the new operator.

The index card in the picture displays an extract from the .de zone for the de-example.de domain with the respective relevant data. Also, for the old and the new operator we display only the data needed in the respective operator's zone for the operator change. Please note that the displayed keys are the public keys and that, for reasons of clarity, the relevant DNSSEC signatures are not shown. When necessary, we explain in the text which data is signed with which key. It goes without saying that the private section of the key is used in such cases.

DS(KEY) stands for a DS-RR generated by the registry based on the key stored in the domain object.

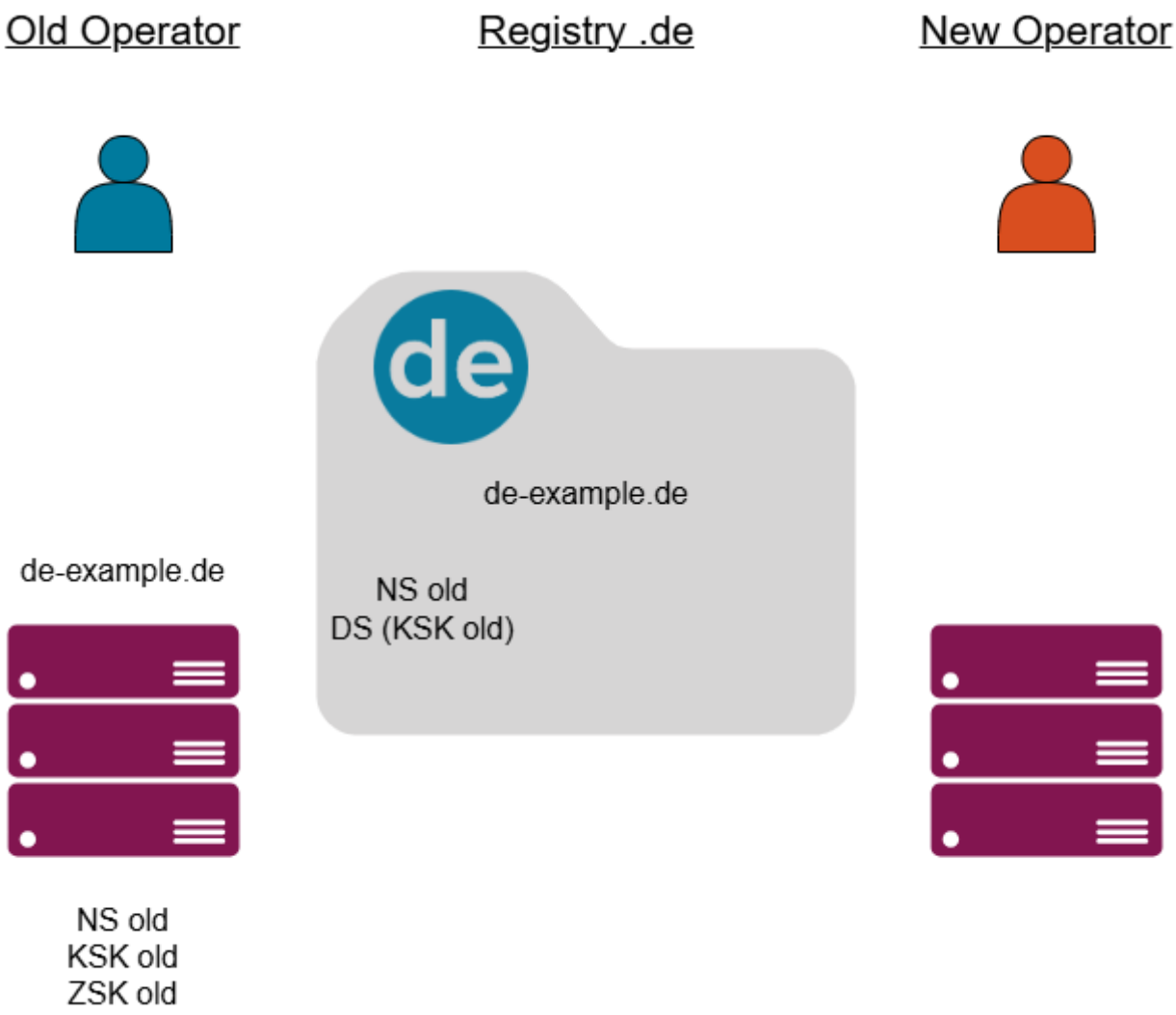
If request types are mentioned in the text, they are written in a different font (Courier New).

Initial situation

The name server information and the valid KSK of the old operator of the domain, e.g. de-example.de, are stored in the registry .de. The ZSK of the old operator is signed with this operator's KSK and published in the DNS. The zone de-example.de is delegated to the name servers of the operator.

The operators involved must be capable to sign with DNSSEC.

Figure 2: Situation before operator change


Old Operator
Registry .de
New Operator
de-example.de
NS old
DS (KSK old)
de-example.de
NS old
KSK old
ZSK old

Case Studies DNSSEC

Explanation

The operator change is explicated by means of the following case studies:

- Without provider change with the old operator being involved
- With provider change with the old operator being involved
- Without provider change without the old operator being involved
- With provider change without the old operator being involved

What all these cases have in common is that no private keys need to be exchanged and no direct secure communication channel between the operators involved is necessary.

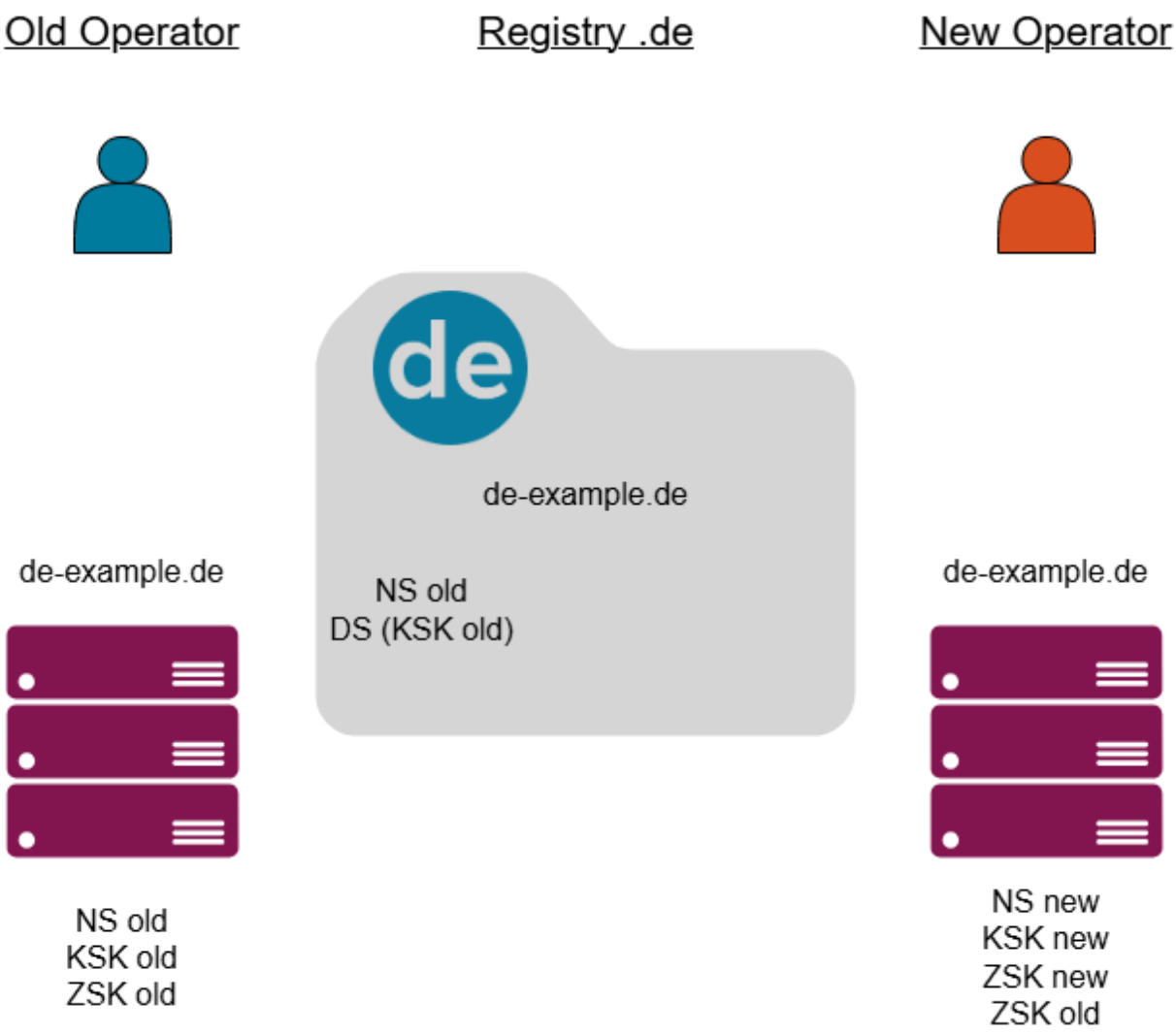
It is assumed for all case studies that during the ongoing operator change neither the RegAcc nor the operator carry out any other substantial changes, such as a change of algorithm or a simultaneous change of keys at the old operator. In concrete terms, this means that both operators must use the same DNSKEY algorithm, but not the same key length.

Preparation Phase

First of all, in all cases described in this manual, you must create the conditions at the future (new) operator that make an operator change possible. To this end, the new operator must sign their version of the zone with "ZSK new", if this has not yet been done. "ZSK new" and "KSK new" must be published in this zone.

Then you must identify the "ZSK old" from the DNS, validate it and publish it in its own signed zone. The following situation results:

Figure 1: New operator has created the necessary conditions



Operator Change Involving the Old Operator Without Provider Change

Task

When you change operators, you must also roll over the key(s) concerned. The key rollover must not entail validation errors.

The goal is to enable validation of both ZSKs via both KSKs for the operator change.

All changes are carried out by one and the same RegAcc in the registry (database).

Solution

The registry serves as an "agent" to enable the old operator to access the ZSK of the new operator.

Step 1

The RegAcc stores the "KSK new" and the "ZSK new" in the domain object of the registry but also maintains "NS old" and "KSK old" (UPDATE 1).

Hint

ZSK new: We recommend not to set the SEP bit for the ZSK. This makes it easier for the old operator to differentiate between ZSK and KSK.

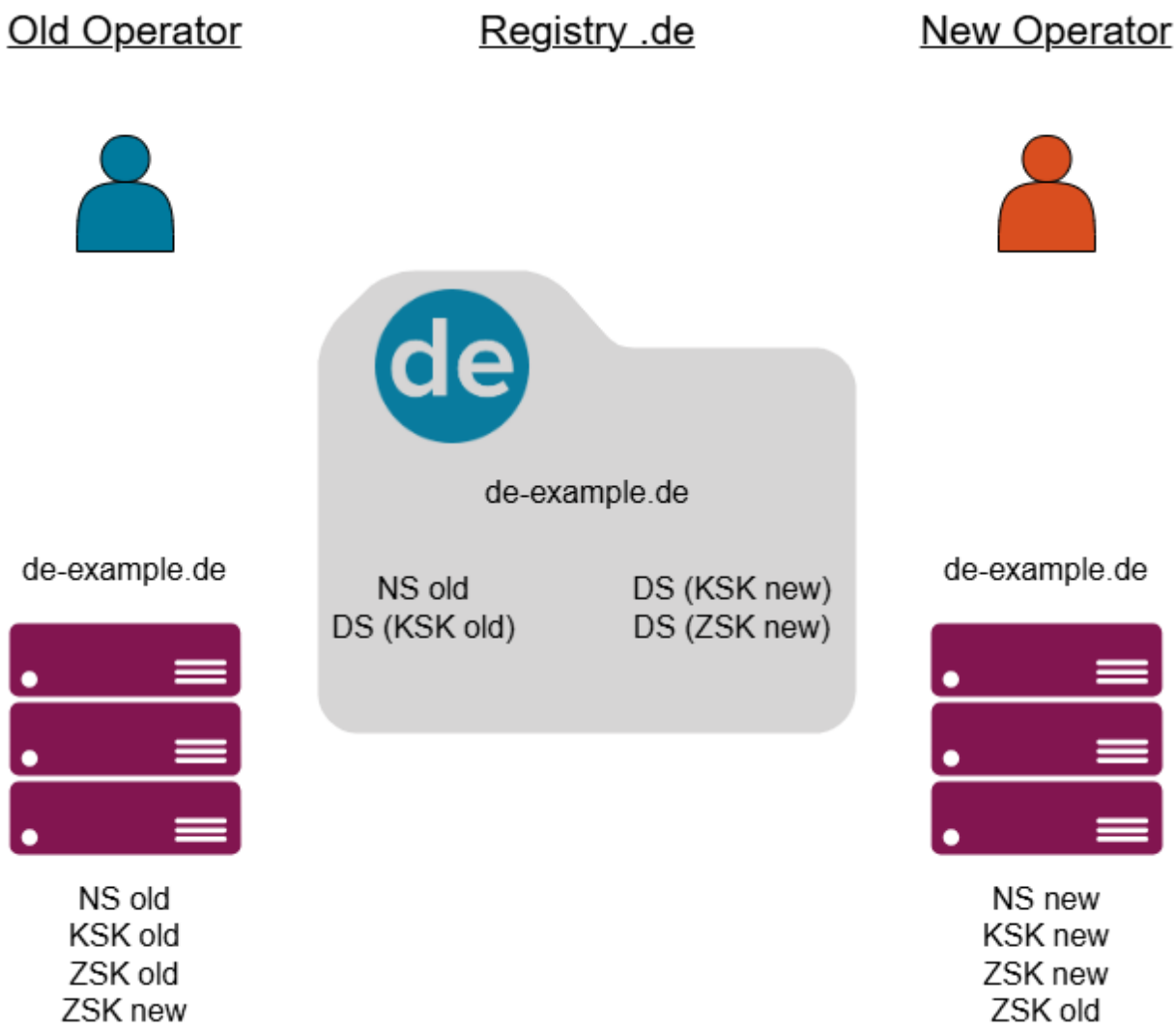
Notice

ZSK new: Please note that according to 3.6.1.1 DNSKEY: Flags, item 3, a warning will be sent for the ZSK because of the missing SEP bit.

Step 2

The old operator then accesses this data, if possible, via RRI or alternatively via whois and stores the "ZSK new" in their zone. Then, they sign their DNSKey-RRSet ("ZSK new", "ZSK old", "KSK old") with the "KSK old".

Figure 2: RegAcc has stored the new data in the registry and the old operator has completed all preparations to meet the requirements



When these steps are complete, both operators have signed and published their own as well as the other's ZSK ("ZSK old" and "ZSK new"). Thus, every validating resolver now has access to and can use both keys. Consequently, during the switch-over phase both data of the old and of the new operator can be validated; no validation errors will occur.

Step 3

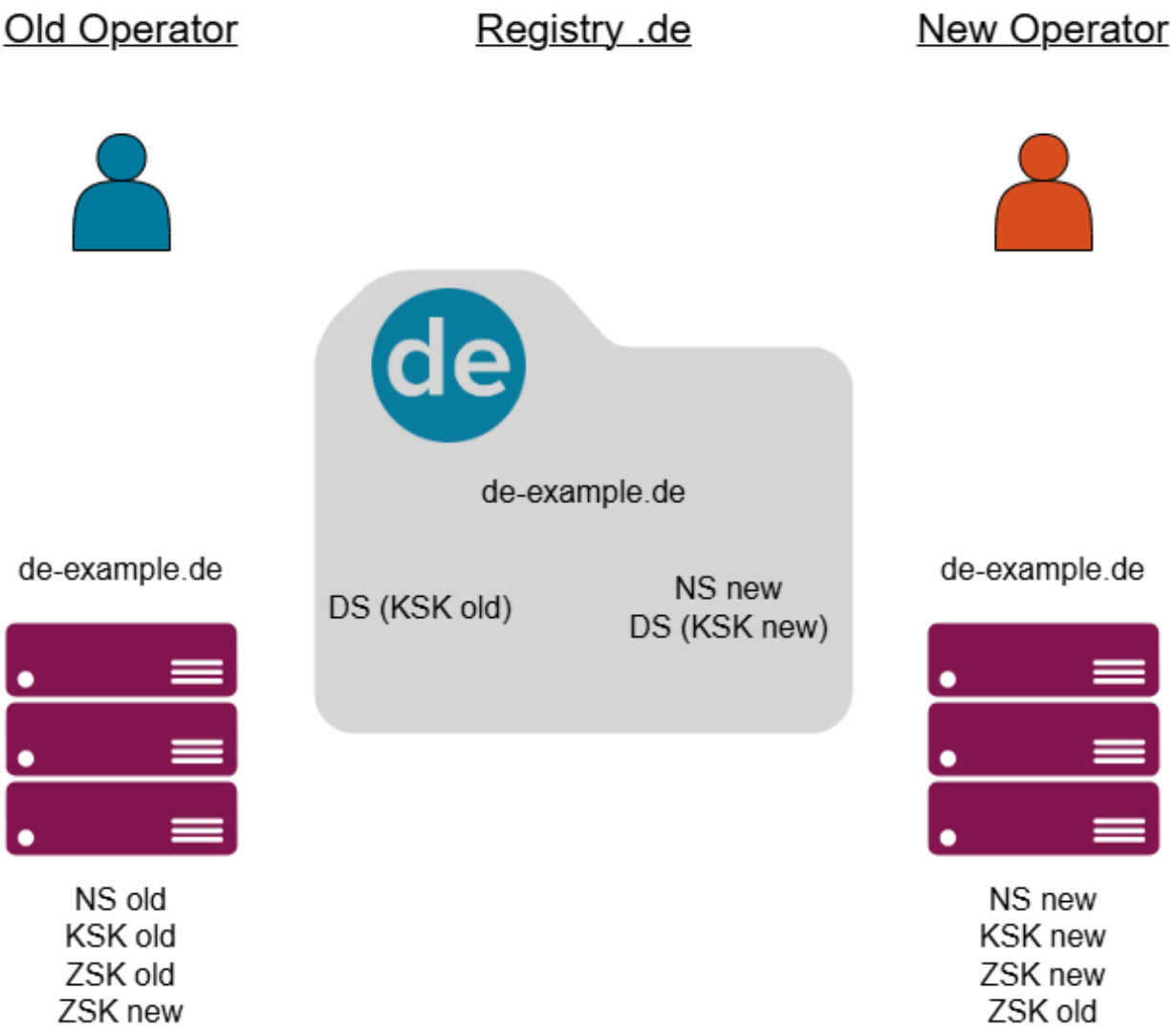
Then you have to wait until the updated zone is available on the name servers of the old operator. The goal is to ensure that neither a DS-RRSet without reference to "KSK new" nor a DNSKEY-RRSet without "ZSK new" is in the DNS (or in the caches). To achieve this, at least the TTL of the DS-RRSet must have expired since the keys were published in the .de zone, and at least the TTL of the DNSKEY-RRSet since the "ZSK new" has been available on the setup of the old operator. The decisive TTL, however, is the TTL of the previous DNSKEY-RRSet (without "ZSK new"). We recommend to choose a TTL similar to the TTL of the DS-RRSet.

Assuming a TTL of 24 hours in the .de zone, a zone publication interval of two hours and quick takeover of the "ZSK new" by the old operator, the waiting time would add up to about 36 hours.

Step 4

The new operator arranges for the RegAcc to update the name server data in the registry so that the new operator data is stored (UPDATE 2). The key "ZSK new" is no longer required in the registry and can be removed. Make sure not to delete the "KSK old" in this process.

Figure 3: RegAcc has replaced "NS old" by "NS new" in the registry and has removed the "ZSK new"



Step 5

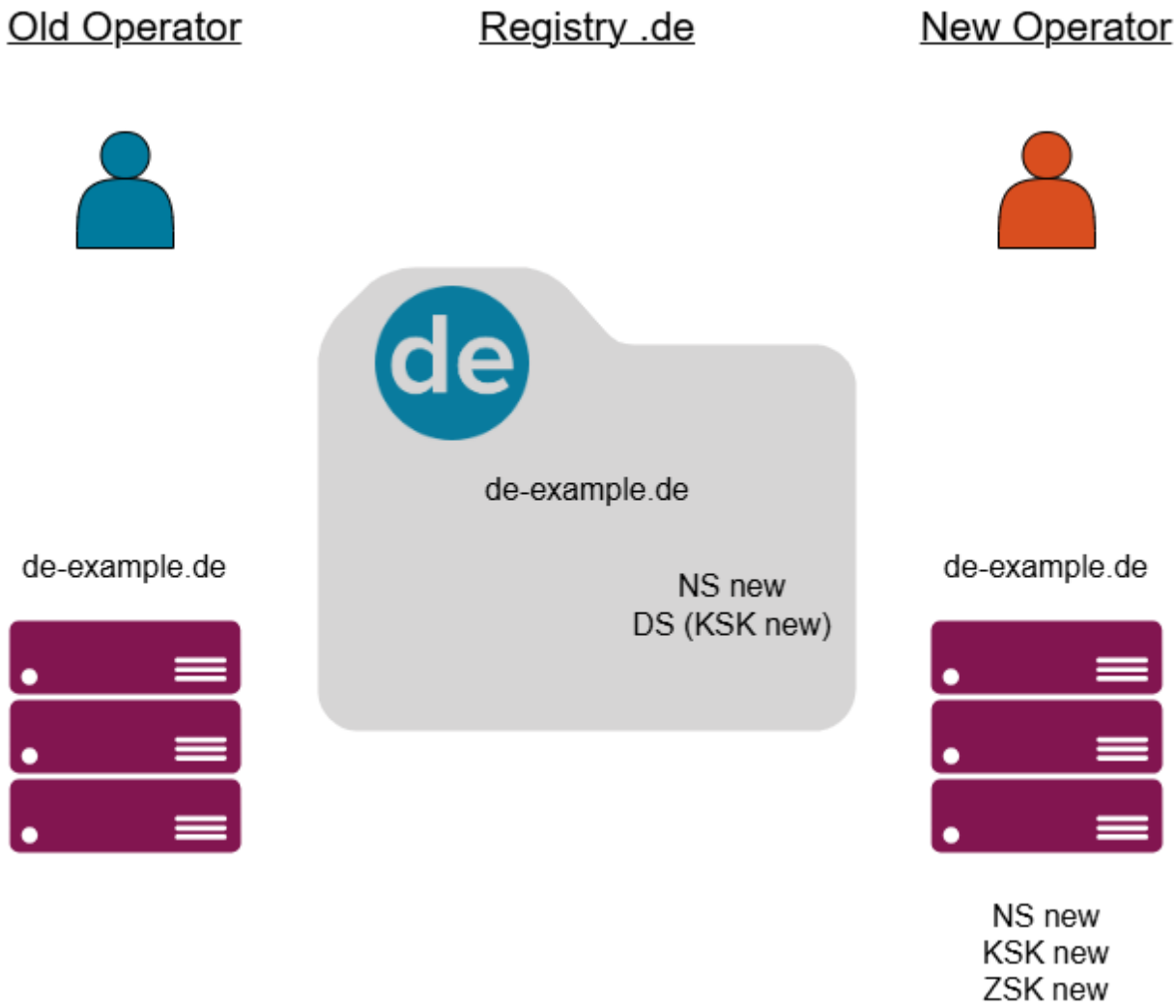
Now you must wait again. The waiting time serves to ensure that no DNSKEY-RRSet with "KSK old" can be found in the DNS (or in the caches) any more, and in particular that no DNS queries are directed to the infrastructure of the old operator. To achieve this, at least the aggregate time of all TTLs of the NS-RRSet in the .de zone, the TTL of the NS-RRSet in the delegated zone and the TTL of the DNSKEY-RRSet of the old operator must have expired since the new NS-RRSet

was published in the .de zone. As regards the TTL of the DNSKEY on the side of the old operator, the updated TTL is now applicable (after "ZSK new" has been added).

Step 6

When this waiting time has expired, the RegAcc deletes the "KSK old" from the registry (UPDATE 3).

Figure 4: RegAcc has deleted "KSK old" in the registry



Now the registry contains only the data of the new operator, and the de-example.de zone need no longer be supported by the old operator.

> **Caution!**
>
> f the updated zone with the "ZSK new" is not available on the name servers of the old operator when the waiting time of step 1 has expired, it must be assumed that the old operator does not support the operator change. In such case follow the procedure described in "Operator Change not Involving the Old Operator Without Provider Change" on page 17.

Operator Change Involving the Old Operator With Provider Change

Task

When you change operators you must also roll over the key(s) concerned. The key rollover must not entail validation errors.

The goal is to enable validation of both ZSKs via both KSKs for the operator change.

All changes are carried out by one and the same RegAcc in the registry (database).

Solutions

Also when the operator change is combined with a provider change the registry serves as an "agent" to enable to old operator to access the ZSK of the new operator.

Step 1

First of all, the RegAcc of the new operator carries out a provider change and stores the "KSK new" and the "ZSK new" they have received from the new operator in the domain object of the registry. "NS old" and "KSK old", however, must also be maintained. Instead of the UPDATE 1 carried out in the case described above, this type of operator change needs a CHPROV which must include the Dnskey records.

Hint

ZSK new: We recommend not to set the SEP bit for the ZSK. This makes it easier for the old operator to differentiate between ZSK and KSK.

Notice

ZSK new: Please note that according to 3.6.1.1 DNSKEY: Flags, item 3, a warning will be sent for the ZSK because of the missing SEP bit.

Step 2

The RegAcc of the old operator is notified about the completed CHPROV. From then on they can find the newly recorded "ZSK new" in the registry. Since it cannot be distinguished in the registry between ZSK and KSK as far as the DNSKEYs are concerned, you must determine the DNSKEY which is not your own and which has no SEP bit set in the flag field to identify the "ZSK new".

Step 3

As described in the preceding case study, here too UPDATE 2 and UPDATE 3 must be carried out once the necessary waiting times have expired.

Caution!

If after this waiting time the updated zone with "ZSK new" is not available on the name servers of the old operator, the operator change will be carried out without involving the old operator. In this case, please proceed as described in "Operator Change Not Involving the Old Operator With Provider Change" on page 21.

Operator Change not Involving the Old Operator Without Provider Change

Task

If after the UPDATE 1 described above the updated zone with "ZSK new" is not available on the name servers of the old operator, the operator change will be carried out without involving the old operator.

In this case the only possible technical solution is to preliminarily put the domain in the insecure status.

All changes are carried out by one and the same RegAcc in the registry (database).

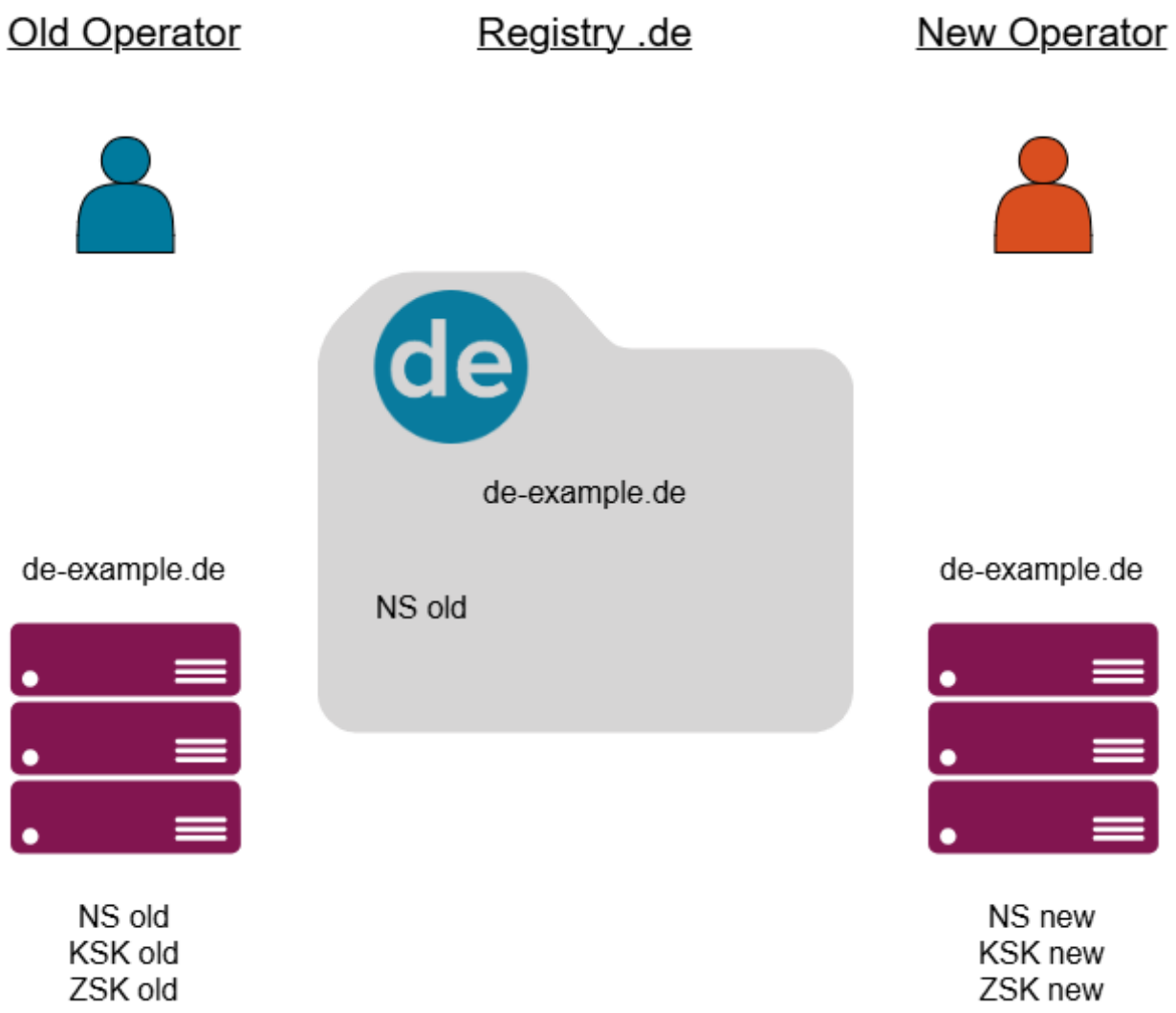
Solution

The following steps

Step 1

The RegAcc deletes "KSK old", "KSK new" and "ZSK new" in the domain object of the registry and thus puts the domain in the insecure status (UPDATE 2A).

Figure 5: RegAcc has put the domain in insecure status



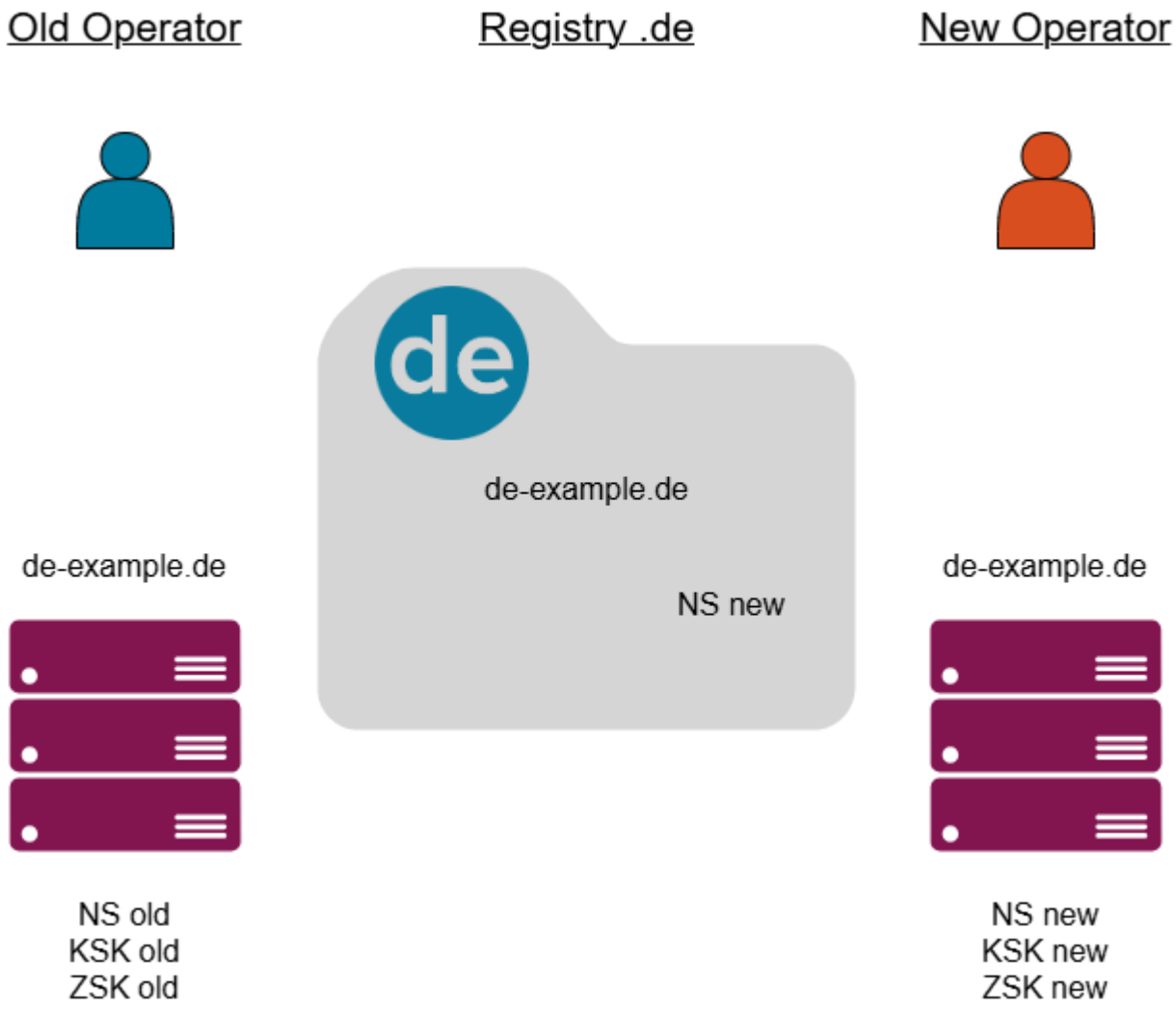
Step 2

Then you must wait until the data of the unsigned de-example.de zone is available on the resolvers. The goal is to ensure that no DS-RRSet can be found in the DNS (or in the caches) any longer. To achieve this, at least the TTL of the DS-RRSet must have expired since the data was published in the .de zone. Assuming a TTL of 24 hours in the .de zone and a zone publication interval of two hours, the waiting time would add up to about 26 hours.

Step 3

The RegAcc updates the name server data in the registry to the data of the new operator (UPDATE 2B).

Figure 6: RegAcc has changed "NS old" to "NS new" in the registry



Step 4

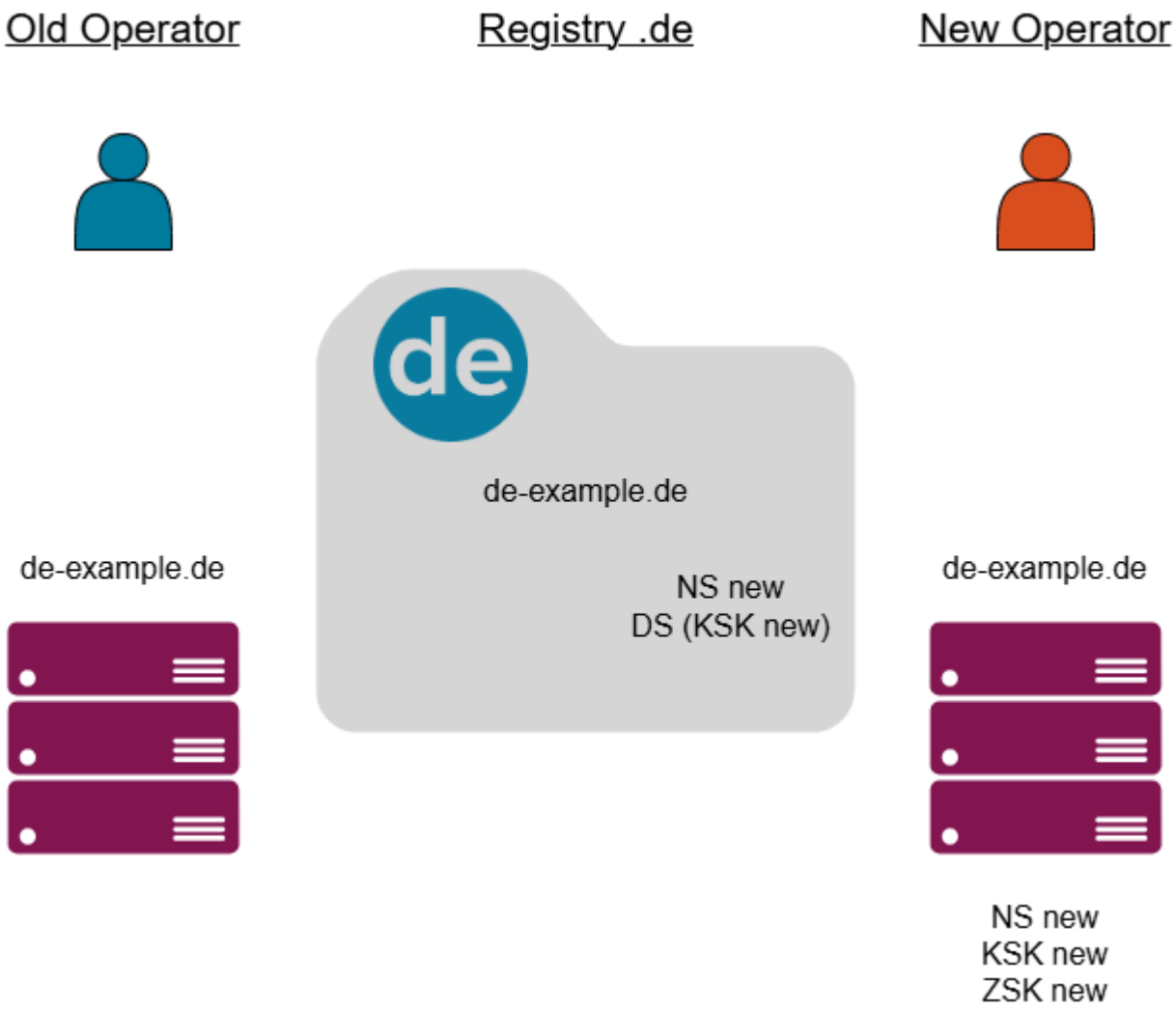
Then you must wait again until all resolvers have received the data of the now valid name servers ("NS new") of the new operator. The goal is to ensure that no

DNS queries are directed to the infrastructure of the old operator. To achieve this, at least the aggregate time of all TTLs of the NS-RRSet in the .de zone and of the TTL of the NS-RRSet in the delegated zone must have expired.

Step 5

When this waiting time has expired the RegAcc stores the keys of the new operator in the registry (UPDATE 3).

Figure 7: RegAcc has stored the "KSK new" in the registry



Now the operator change is complete, and the old operator no longer needs to support the de-example.de zone.

Operator Change Not Involving the Old Operator With Provider Change

Task

If after the UPDATE 1 described above the updated zone with "ZSK new" is not available on the name servers of the old operator, the operator change will be carried out without involving the old operator.

In this case the only possible technical solution is to preliminarily put the domain in the insecure status.

All changes are carried out by one and the same RegAcc in the registry (database).

Solution

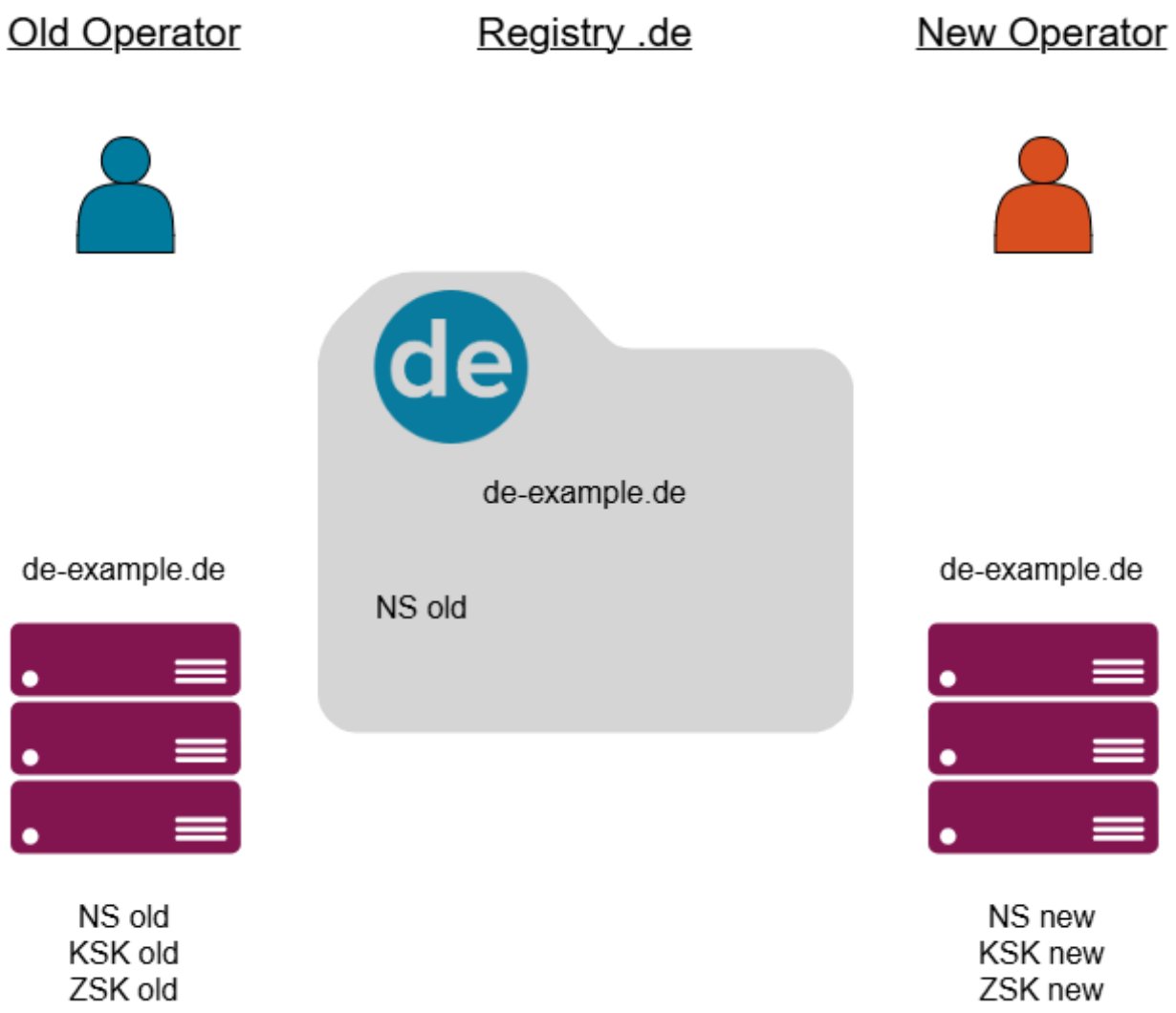
If after the UPDATE 1 described above the updated zone with "ZSK new" is not available on the name servers of the old operator, the operator change will be carried out without involving the old operator.

In this case the only possible technical solution is to preliminarily put the domain in the insecure status.

Step 1

The RegAcc deletes "KSK old", "KSK new" and "ZSK new" in the domain object of the registry and thus puts the domain in the insecure status (UPDATE 2A).

Figure 8: RegAcc has put the domain in insecure status



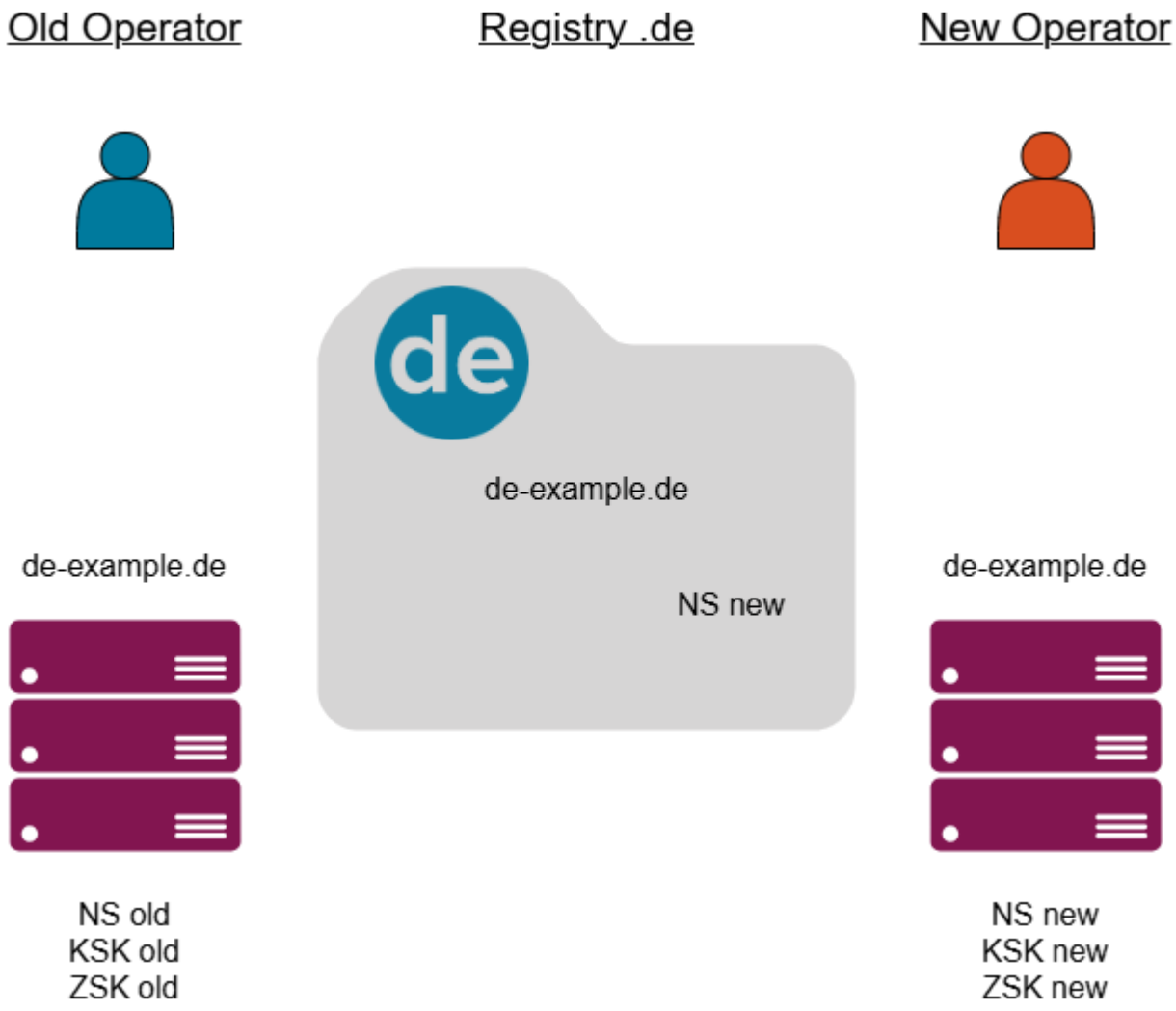
Step 2

Then you must wait until the data of the unsigned de-example.de zone is available on the resolvers. The goal is to ensure that no DS-RRSet can be found in the DNS (or in the caches) any longer. To achieve this, at least the TTL of the DS-RRSet must have expired since the data was published in the .de zone. Assuming a TTL of 24 hours in the .de zone and a zone publication interval of two hours, the waiting time would add up to about 26 hours.

Step 3

The RegAcc updates the name server data in the registry to the data of the new operator (UPDATE 2B).

Figure 9: RegAcc has changed "NS old" to "NS new" in the registry



Step 4

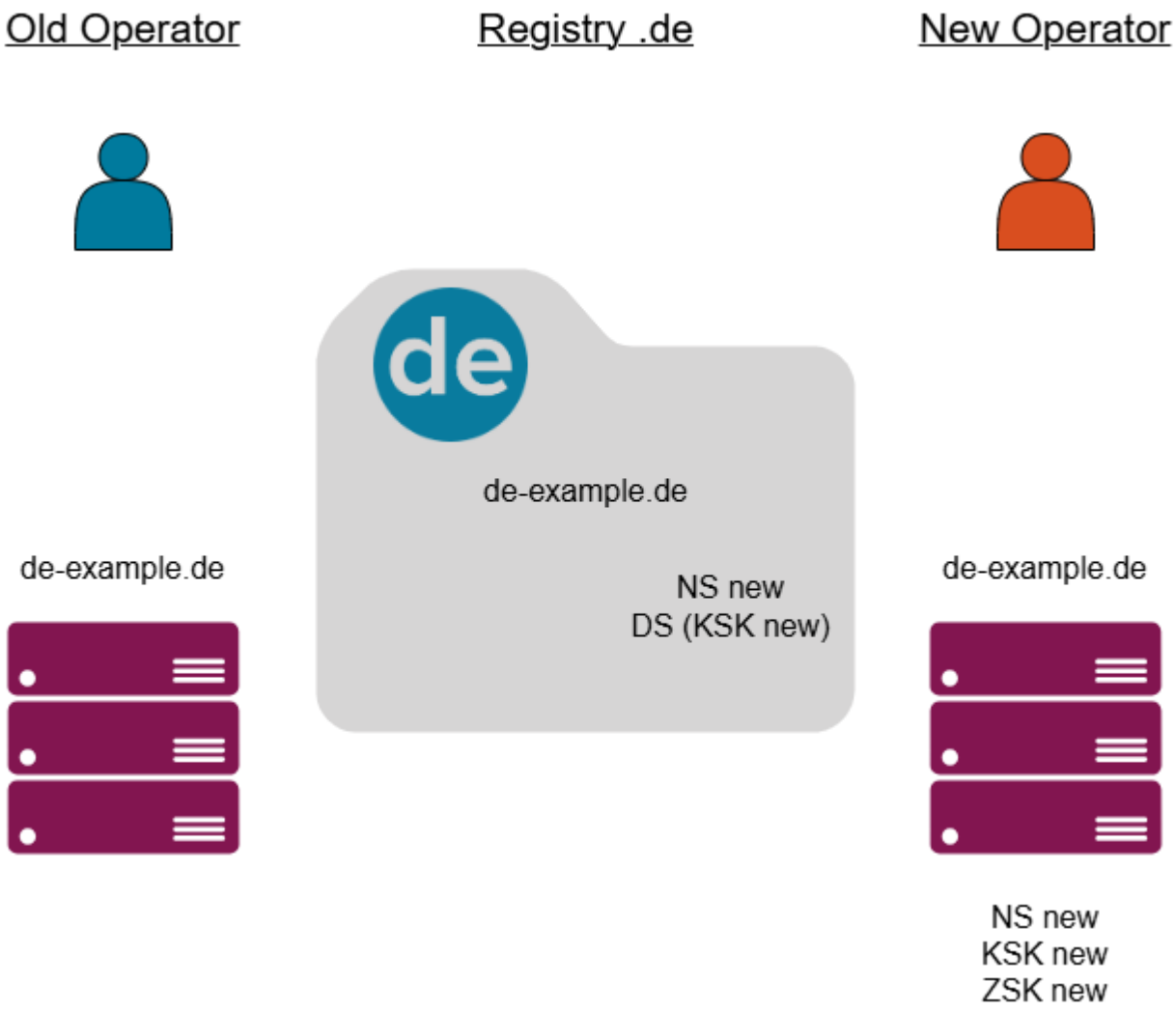
Then you must wait again until all resolvers have received the data of the now valid name servers ("NS new") of the new operator. The goal is to ensure that no

DNS queries are directed to the infrastructure of the old operator. To achieve this, at least the aggregate time of all TTLs of the NS-RRSet in the .de zone and of the TTL of the NS-RRSet in the delegated zone must have expired.

Step 5

When this waiting time has expired the RegAcc stores the keys of the new operator in the registry (UPDATE 3).

Figure 10: RegAcc has stored the "KSK new" in the registry



Now the operator change is complete, and the old operator no longer needs to support the de-example.de zone.