DENIC

Operatorwechsel bei DNSSEC-Domains

Inhaltsverzeichnis

Einführung DNSSEC 3
- Voraussetzung 3
- Rollen 4
- Form der Darstellung 4
- Ausgangssituation 6

Fallbeispiele DNSSEC 8
- Erläuterung 8
- Vorbereitungsphase 8
- Operatorwechsel unter Beteiligung des alten Operators ohne Providerwechsel 9
- Operatorwechsel unter Beteiligung des alten Operators mit Providerwechsel 15
- Operatorwechsel ohne Beteiligung des alten Operators ohne Providerwechsel 17
- Operatorwechsel ohne Beteiligung des alten Operators mit Providerwechsel 21

Einführung DNSSEC

In der Regel wird beim DNSSEC-Betrieb die „Verfügungsgewalt“ über den ZSK und ggf. auch über den KSK beim Zonenverwalter liegen. Dies ist in vielen Fällen der Operator der Nameserver-Infrastruktur, im folgenden Operator genannt.

Ein Wechsel dieses Operators setzt einen Schlüsselwechsel (Key Rollover) des bzw. der betroffenen Schlüssel und einen Wechsel der DNS-Delegation an eine vom alten Operator unabhängige Infrastruktur (Satz von Nameservern) voraus.

In diesem Dokument werden für die relevanten Szenarien die Schritte aufgezeigt, damit ein koordinierter Schlüssel- und Operatorwechsel ohne Inkonsistenzen möglich ist.

Wenn diese Ablaufpläne befolgt werden, werden Validierungsfehler ausgeschlossen, da es während des laufenden Wechselverfahrens unerheblich ist, ob der validierende Resolver seine Schlüssel vom alten oder vom neuen Operator bezogen hat.

> **Achtung!**
>
> Ein Operatorwechsel in einem Schritt, d.h. Wechsel der Delegation mit einem Auftrag, wird zu Validierungsfehlern führen!

Ein Wechsel des RegAccs ohne Operatorwechsel ist auch bei DNSSEC-Domains weiterhin problemlos mit einem einzelnen CHPROV möglich.

Voraussetzung

Für die Nutzung werden Kenntnisse zum Ablauf des Umzugs einer unsignierten .de-Domain zu einem anderen Operator sowie Grundkenntnisse von DNSSEC (Bedeutung des KSK und ZSK sowie zum Ablauf der Signierung einer Domain) vorausgesetzt.

Rollen

In diesem Dokument werden zwei Rollen unterschieden:

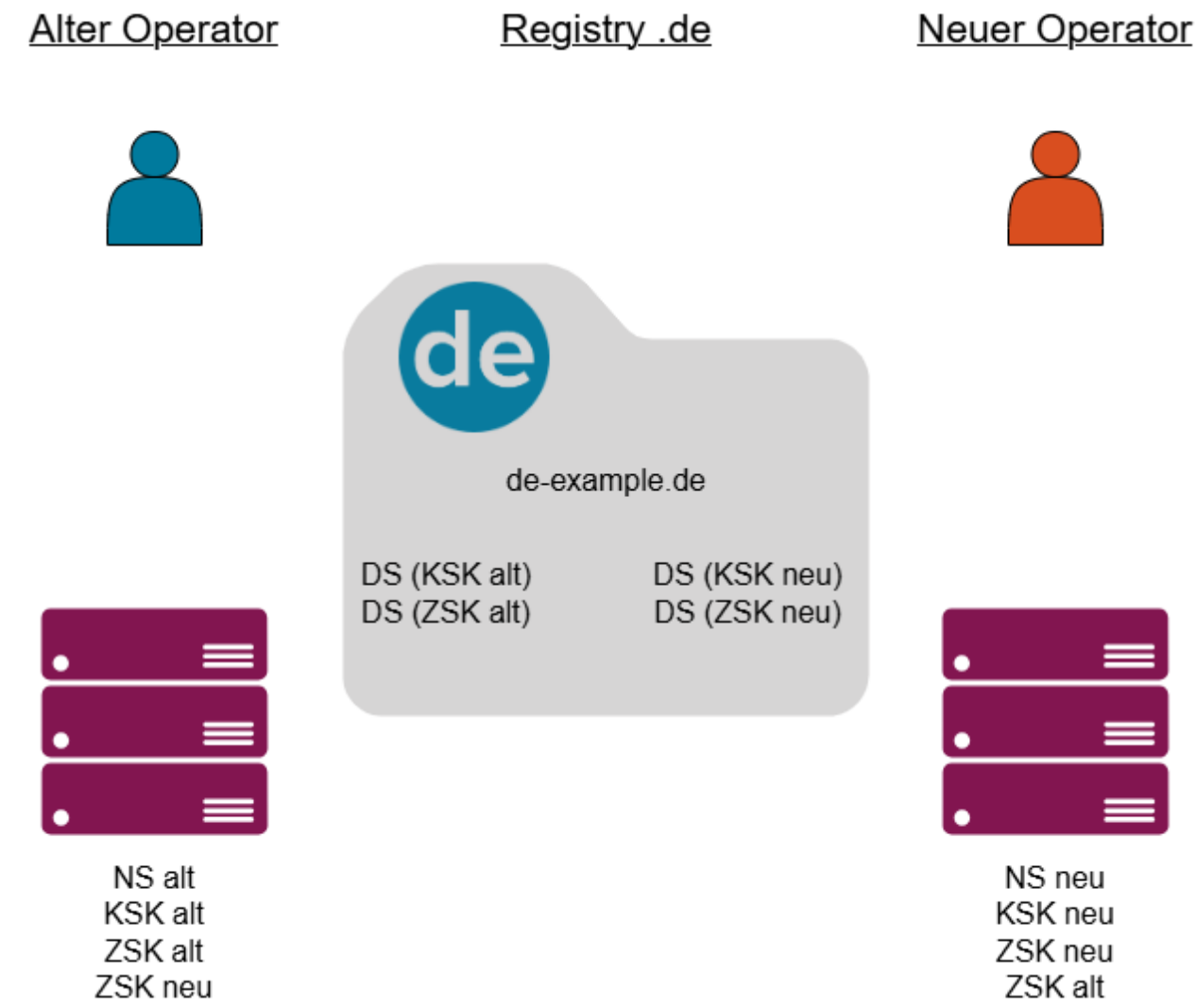
- Operator
- RegAcc

Das RegAcc ist dabei das DENIC-Mitglied, welches die Domain verwaltet und die Änderungen an der Datenbank (Registry .de) vornimmt, wäh¬rend der Operator die Nameserver-Infrastruktur bereitstellt.

Form der Darstellung

Die folgende Form der Darstellung wird verwendet:

Bild 1: Beispieldarstellung



Erläuterung: Für alle Fallbeispiele im Dokument wird die Domain „de-example.de“ verwendet. Für diese Domain soll ein Operatorwechsel durchgeführt werden. Die beim alten und neuen Operator abgebildeten zwei Server stellen lediglich eine bildliche Vereinfachung und keine Vorgabe dar. „NS alt“ bzw. „NS neu“ stehen dabei für die NS Resource Records der Domain de-example.de.

Es wird davon ausgegangen, dass für die Zone (de-example.de) mit separatem KSK und ZSK gearbeitet wird. Die Zusätze bei den Delegation Signern (DS) für „alt“ und „neu“ beziehen sich auf die autoritative Quelle der Informationen. Diese Quelle kann der alte oder der neue Operator sein.

Die Karteikarte der Abbildung stellt einen Auszug aus der .de-Zone für die Domain de-example.de mit den jeweils relevanten Daten dar. Auch für den alten und neuen Operator werden lediglich die in dessen Zone für den Operatorwechsel relevanten Daten dargestellt. Dabei gilt es zu beachten, dass es sich bei den dargestellten Schlüsseln um die öffentlichen Schlüssel handelt und aus Vereinfachungsgründen relevante DNSSEC-Signaturen nicht dargestellt sind. Wo nötig, wird im Text erwähnt, mit welchem Schlüssel welche Information signiert ist. In diesen Fällen versteht es sich, dass man den privaten Schlüsselteil einsetzt.

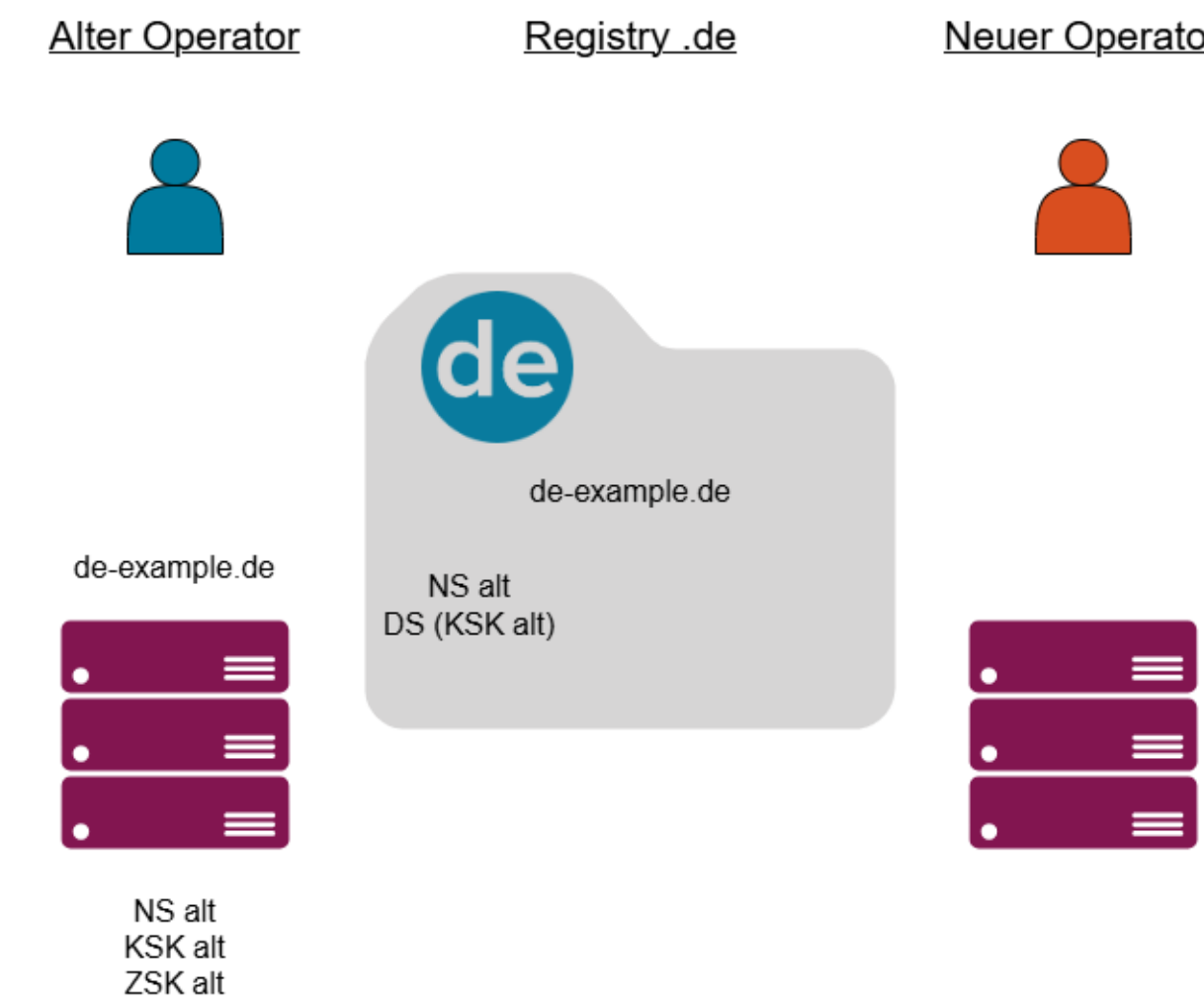
DS(KEY) steht für einen von der Registry erstellten DS-RR auf Basis der im Domainobjekt hinterlegten Schlüssel.

Ausgangssituation

Die Nameserver-Informationen und der gültige KSK des alten Operators für die Domain, z.B. de-example.de, sind in der Registry .de abgelegt. Der ZSK des alten Operators ist mit dessen KSK signiert und im DNS publiziert. Die Zone de-example.de ist an die Nameserver des Operators delegiert.

Die beteiligten Operatoren müssen in der Lage sein mit DNSSEC zu signieren.

Bild 2: Situation vor dem Operatorwechsel


Alter Operator
Registry .de
Neuer Operator
de-example.de
NS alt
DS (KSK alt)
de-example.de
NS alt
KSK alt
ZSK alt

Fallbeispiele DNSSEC

Erläuterung

Für den Wechsel des Operators werden folgende Fallbeispiele zur Verfügung gestellt:

- Ohne Providerwechsel unter Beteiligung des alten Operators
- Mit Providerwechsel unter Beteiligung des alten Operators
- Ohne Providerwechsel ohne Beteiligung des alten Operators
- Mit Providerwechsel ohne Beteiligung des alten Operators

Allen Fällen ist gemeinsam, dass sie ohne den Austausch privater Schlüssel auskommen und zwischen den beteiligten Operatoren kein direkter, gesicherter Kommunikationskanal bestehen muss.

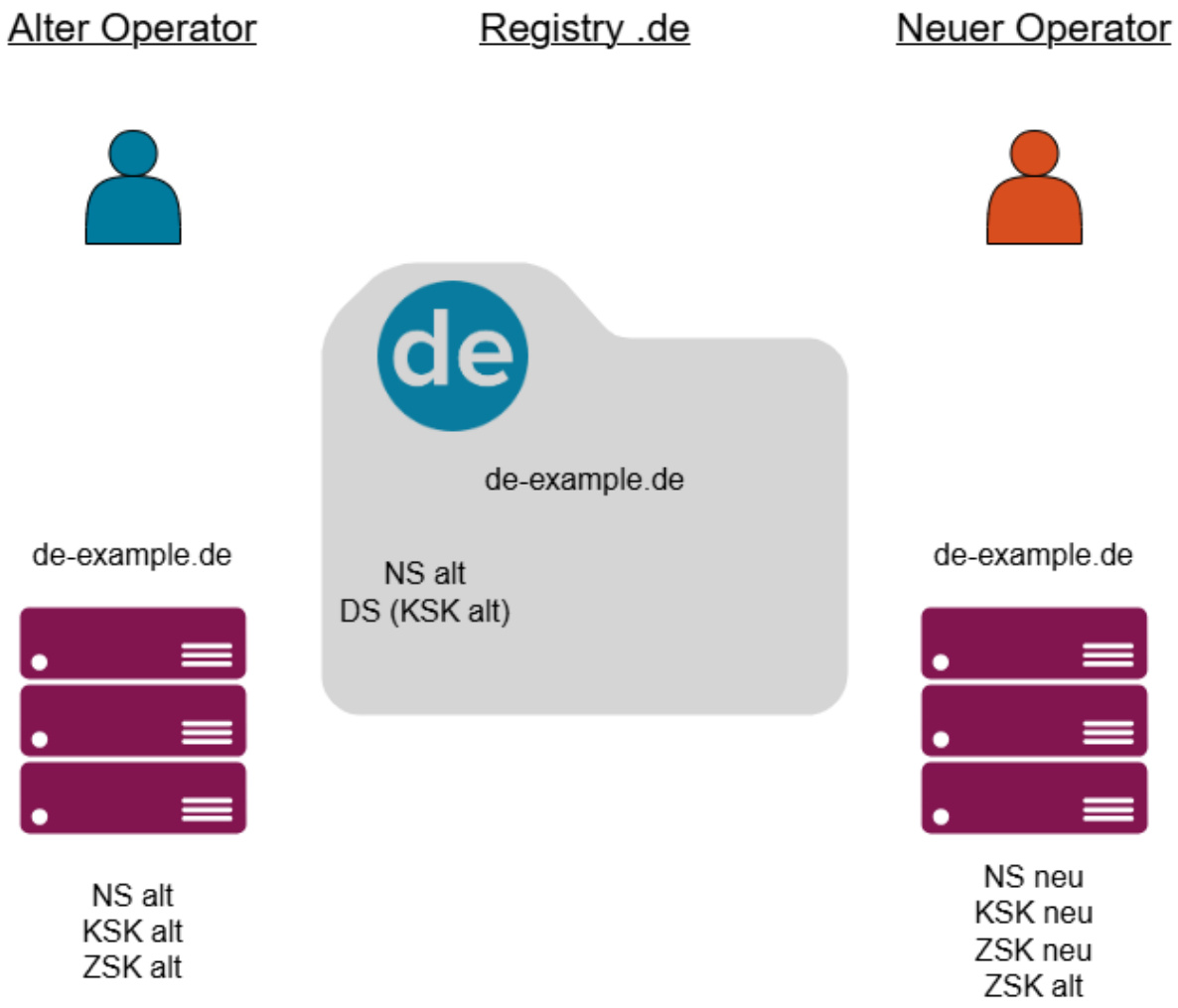
Bei den Fällen wird vorausgesetzt, dass während des laufenden Operatorwechsels keine weiteren gleichzeitigen substanziellen Änderungen durch RegAccs und Operator, wie z.B. ein Algorithmenwechsel oder ein gleichzeitiger Schlüsselwechsel beim alten Operator vorgenommen wird. Konkret bedeutet dies, dass beide Operatoren denselben DNSKEY-Algorithmus, nicht aber dieselbe Schlüssellänge, einsetzen müssen.

Vorbereitungsphase

Zunächst sind in allen hier beschriebenen Fällen in einem ersten Schritt die Voraussetzungen für einen Operatorwechsel beim neuen Operator zu schaffen. Hierzu ist, falls noch nicht erfolgt, durch den neuen Operator seine Version der Zone mit „ZSK neu“ zu signieren, „ZSK neu“ und „KSK neu“ sind dort zu publizieren.

Dann ist der „ZSK alt“ aus dem DNS zu ermitteln, zu validieren und in seiner eigenen signierten Zone zu publizieren. Damit ergibt sich folgender Zustand:

Bild 1: Neuer Operator hat die Voraussetzung abgeschlossen



Operatorwechsel unter Beteiligung des alten Operators ohne Providerwechsel

Aufgabenstellung

Beim Wechsel des Operators ist ein Schlüsselwechsel (Key Rollover) des bzw. der betroffenen Schlüssel erforderlich. Der Schlüsselwechsel darf nicht zu Validierungsfehlern führen.

Ziel ist es beide ZSKs für den Operatorwechsel über beide KSKs validierbar zu machen. Alle Änderungen werden von ein- und demselben RegAcc in der Registry vorgenommen. Das System, auf dem NAST installiert werden soll, muss folgende Voraussetzungen erfüllen

Lösung

Die Registry dient als Mittler, um dem alten Operator einen Zugriff auf den ZSK des neuen Operators zu ermöglichen.

Schritt 1

Das RegAcc hinterlegt den „KSK neu“ und „ZSK neu“ im Domainobjekt der Registry behält aber dabei auch „NS alt“ und „KSK alt“ (UPDATE 1).

Tipp

ZSK neu: Es wird empfohlen, für den ZSK das SEP-Bit nicht zu setzen. Damit wird dem alten Operator die Differenzierung zwischen ZSK und KSK vereinfacht.

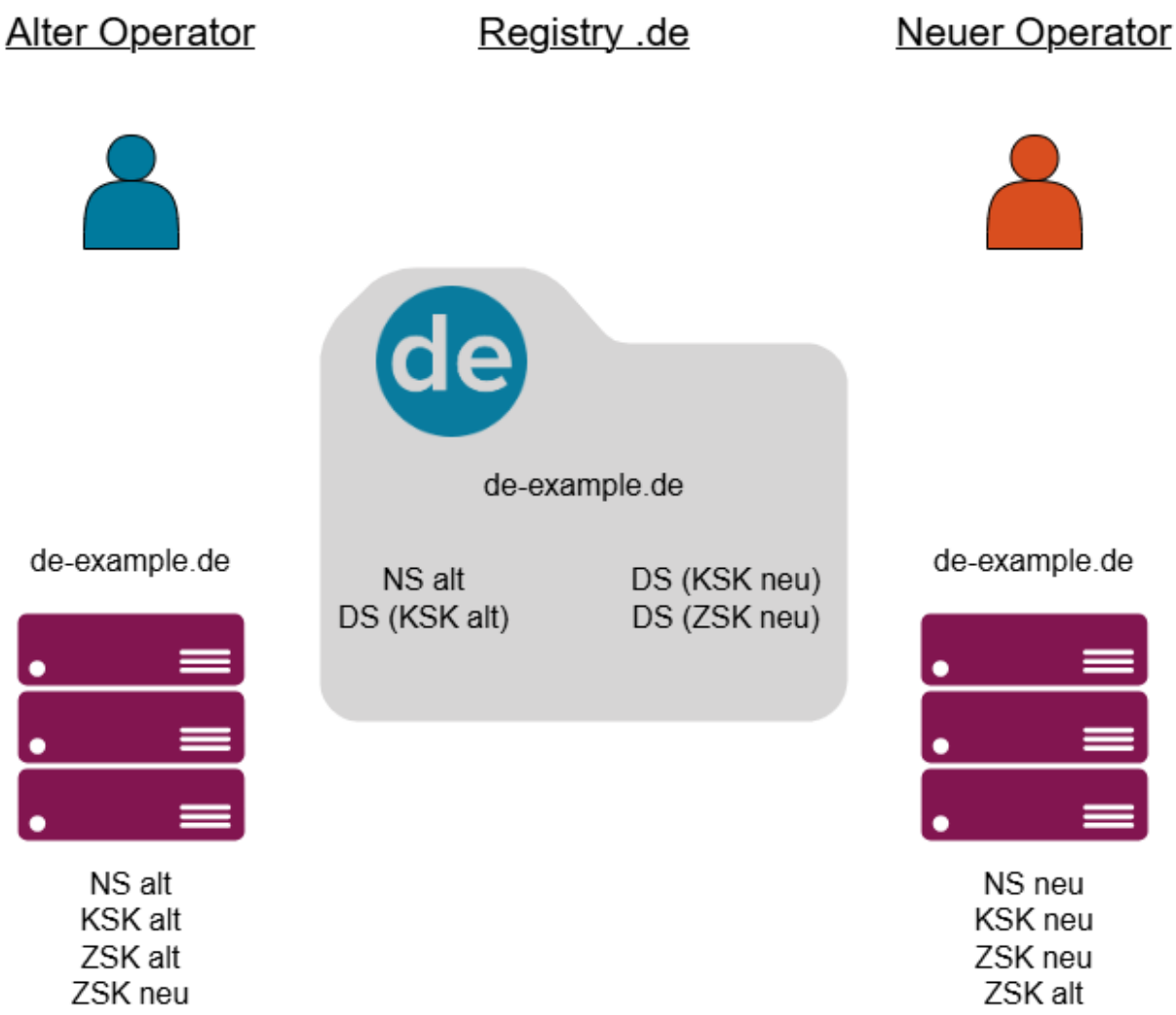
Hinweis

ZSK neu: Es ist zu beachten, dass gemäß 3.6.1.1 DNSKEY: Flags, Punkt 3, für den ZSK we¬gen des fehlenden SEP-Bits eine Warnung zurückgegeben wird.

Schritt 2

Der alte Operator greift nun auf diese Information, falls möglich über RRI oder alternativ über whois zu, und legt den „ZSK neu“ in seiner Zone ab. Dann signiert er seinen DNSKey-RRSet („ZSK neu“, „ZSK alt“, „KSK alt“) mit dem „KSK alt“.

Bild 2: RegAcc hat die neuen Daten in der Registry hinterlegt und der alte Operator die Voraussetzungen abgeschlossen



Da beide Operatoren danach jeweils den eigenen und den fremden ZSK signiert und publiziert haben, hat jeder validierende Resolver Zugriff auf beide Schlüssel und kann diese nutzen. Während der Umschaltung können somit sowohl Daten des alten als auch des neuen Operators validiert werden und es kommt zu keinen Validierungsfehlern.

Schritt 3

Danach ist zunächst abzuwarten, bis die aktualisierte Zone auf den Nameservern des alten Operators verfügbar ist. Ziel ist sicher zu stellen, dass kein DS-RRSet ohne Verweis auf „KSK neu“ im DNS (inklusive Caches) zu finden ist und ebenfalls

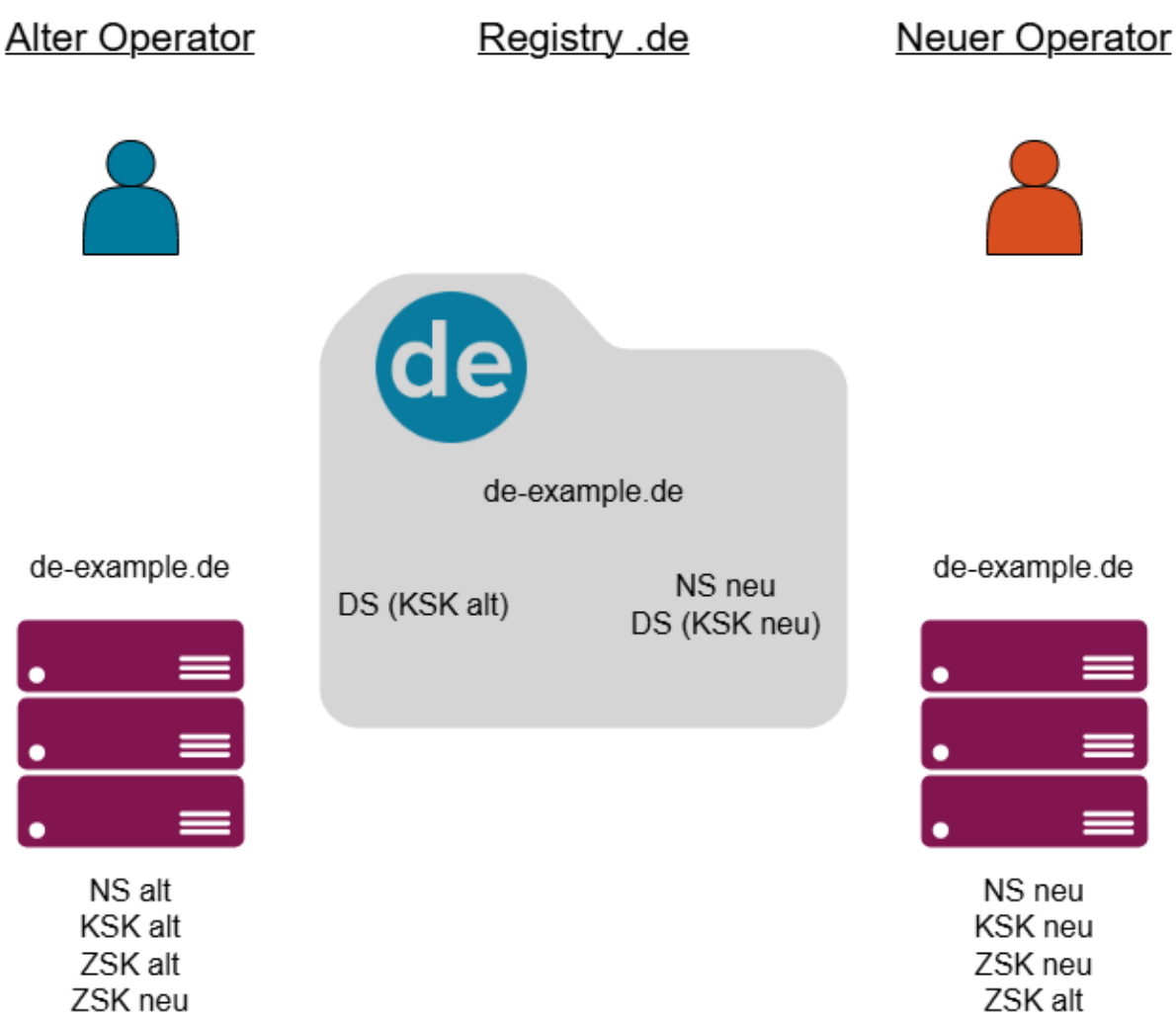
kein DNSKEY-RRSet ohne „ZSK neu“. Dafür muss seit der Veröffentlichung in der .de-Zone mindestens die TTL des DS-RRSet abgelaufen sein und seit der Verfügbarkeit vom „ZSK neu“ auf dem Setup des alten Operators mindestens die TTL vom DNSKEY-RRSet abgelaufen sein. Relevant dabei ist allerdings die TTL des vorherigen DNSKEY-RRSet (ohne „ZSK neu“). Es wird empfohlen eine TTL dafür zu wählen, die der TTL des DS-RRSet ähnlich ist.

Bei einer TTL in der .de-Zone von 24 Stunden, einem regulären Abstand der .de-Zonenveröffentlichungen von zwei Stunden und einer zügigen Übernahme vom alten Operator des „ZSK neu“ ergäbe sich eine Wartezeit von etwa 36 Stunden.

Schritt 4

Der neue Operator veranlasst, dass das RegAcc die Nameserver-Information in der Registry auf den neuen Operator ändert (UPDATE 2). Die Ablage von „ZSK neu“ bei der Registry ist nicht mehr nötig und dieser Key kann entfernt werden. Der „KSK alt“ darf dabei noch nicht gelöscht werden.

Bild 3: RegAcc hat in der Registry „NS alt“ durch „NS neu“ ersetzt und den ZSK neu entfernt



Schritt 5

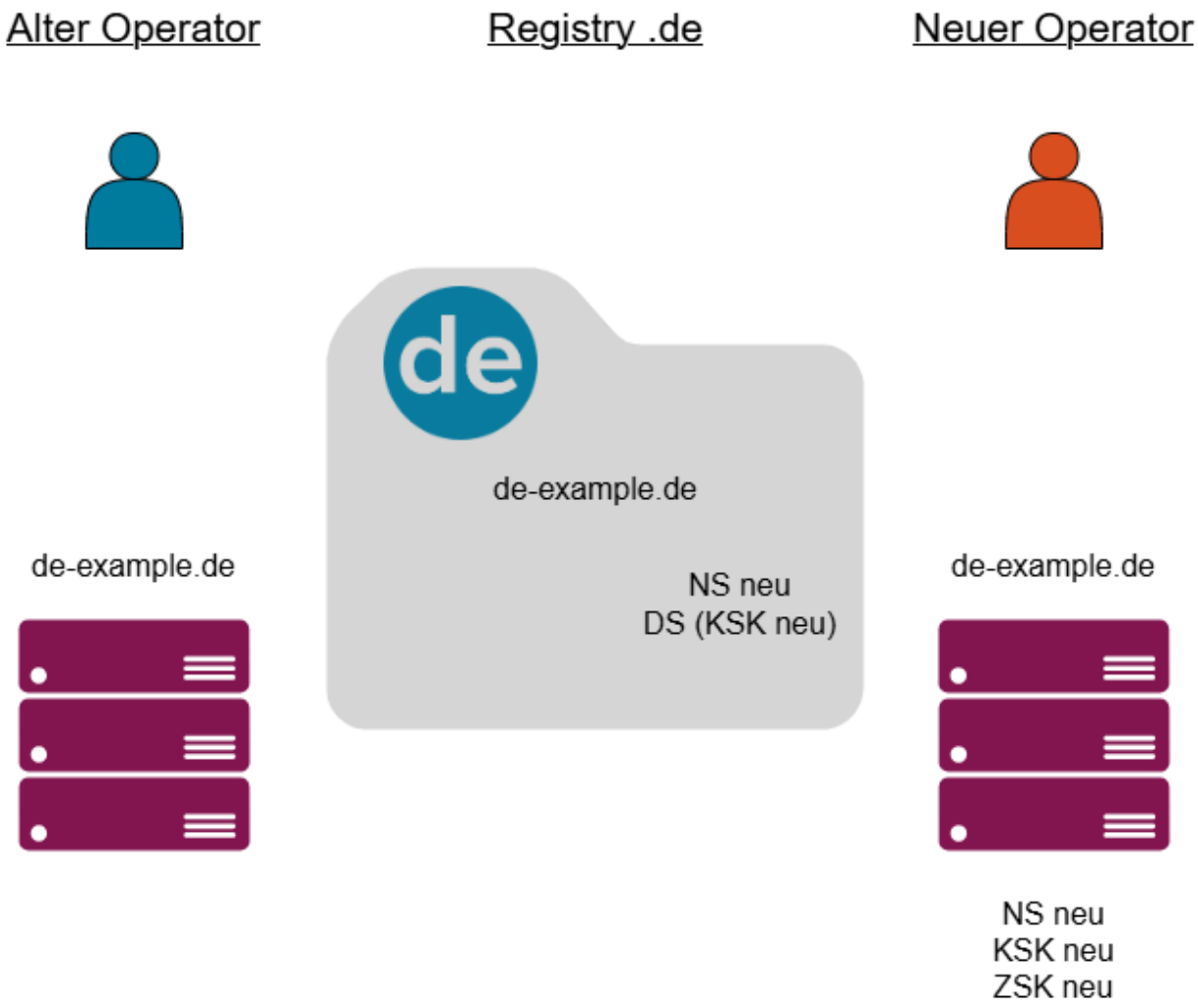
Jetzt ist eine neue Wartezeit einzuhalten. Ziel ist sicherzustellen, dass kein DNSKEY-RRSet mit „KSK alt“ im DNS (inklusive Caches) zu finden ist, insbesondere dass keine DNS-Anfragen an die Infrastruktur des alten Operators geschickt werden. Dafür muss seit der Veröffentlichung des neuen NS-RRSet in der .de-Zone mindestens die Summe der TTLs des NS-RRSet in der .de-Zone, der TTL des NS-RRSet in der delegierten Zone und der TTL des DNSKEY-RRSet des alten Ope-

rators abgelaufen sein. Bei der TTL des DNSKEYs auf der Seite des alten Operators ist jetzt die aktuelle TTL relevant (nachdem „ZSK neu“ hinzugefügt worden ist).

Schritt 6

Nach dieser Wartezeit löscht das RegAcc den „KSK alt“ aus der Registry (UPDATE 3).

Bild 4: RegAcc hat den KSK alt in der Registry gelöscht



Nun sind in der Registry nur noch die Daten des neuen Operators registriert und die Zone de-example.de muss vom alten Operator nicht mehr unterstützt werden.

> **Achtung!**
>
> Falls die aktualisierte Zone mit „ZSK neu“ nach der Wartezeit von Schritt 1 nicht auf den Nameservern des alten Operators verfügbar ist, ist davon auszugehen, dass dieser sich nicht am Operatorwechsel beteiligt. In diesem Fall ist zu verfahren wie in beschrieben "Operatorwechsel ohne Beteiligung des alten Operators ohne Providerwechsel" auf Seite 17.

Operatorwechsel unter Beteiligung des alten Operators mit Providerwechsel

Aufgabenstellung

Beim Wechsel des Operators ist ein Schlüsselwechsel (Key Rollover) des bzw. der betroffenen Schlüssel erforderlich. Der Schlüsselwechsel darf nicht zu Validierungsfehlern führen.

Ziel ist es beide ZSKs für den Operatorwechsel über beide KSKs validierbar zu machen.

Alle Änderungen werden von ein- und demselben RegAcc in der Registry vorgenommen.

Lösung

Auch bei einem gleichzeitigen Providerwechsel dient die Registry wieder als Mittler, um dem alten Operator einen Zugriff auf den ZSK des neuen Operators zu ermöglichen.

Schritt 1

Das RegAcc des neuen Operators führt zunächst einen Providerwechsel durch und hinterlegt den „KSK neu“ und „ZSK neu“, den er vom neuen Operator erhält, im Domainobjekt der Registry, behält aber dabei „NS alt“ und „KSK alt“. Statt des UPDATE 1 im vorherigen Fall erfolgt hier ein CHPROV mit Dnskey-Einträgen.

Tipp

ZSK neu: Es wird empfohlen, für den ZSKs das SEP-Bit nicht zu setzen. Damit wird dem alten Operator die Differenzierung zwischen ZSK und KSK vereinfacht.

Hinweis

ZSK neu: Es ist zu beachten, dass gemäß 3.6.1.1 DNSKEY: Flags, Punkt 3, für den ZSK wegen des fehlenden SEP-Bits eine Warnung zurückgegeben wird.

Schritt 2

Der RegAcc des alten Operators erhält die Benachrichtigung über das vollendete CHPROV. Ab diesem Zeitpunkt ist er in der Lage, den hinterlegten „ZSK neu“ aus der Registry .de zu ermitteln. Da in der Registry bei den DNSKEYs nicht zwischen ZSK und KSK unterschieden werden kann, ist hierzu der DNSKEY zu ermitteln, der nicht der eigene ist und wo das SEP-Bit im Flags-Feld nicht gesetzt ist.

Schritt 3

Wie auch im vorigen Fallbeispiel beschrieben sind nun nach Ablauf der entsprechenden Wartezeiten UPDATE 2 und UPDATE 3 abzuarbeiten.

Achtung!

Falls nach dieser Wartezeit die aktualisierte Zone mit „ZSK neu“ nicht auf den Nameservern des alten Operators verfügbar ist, wird der Wechsel ohne die Beteiligung des alten Operators durchgeführt. In diesem Fall ist zu verfahren wie im Abschnitt "Operatorwechsel ohne Beteiligung des alten Operators mit Providerwechsel" auf Seite 21 beschrieben.

Operatorwechsel ohne Beteiligung des alten Operators ohne Providerwechsel

Aufgabenstellung

Falls nach dem vorher beschriebenen UPDATE 1 die aktualisierte Zone mit „ZSK neu“ nicht auf den Nameservern des alten Operators verfügbar ist, wird der Wechsel ohne dessen Unterstützung durchgeführt.

Dadurch gibt es technisch keine andere Lösung, als die Domain zunächst vorübergehend in den Zustand „insecure“ zu versetzen.

Alle Änderungen werden von ein- und demselben RegAcc in der Registry vorgenommen.

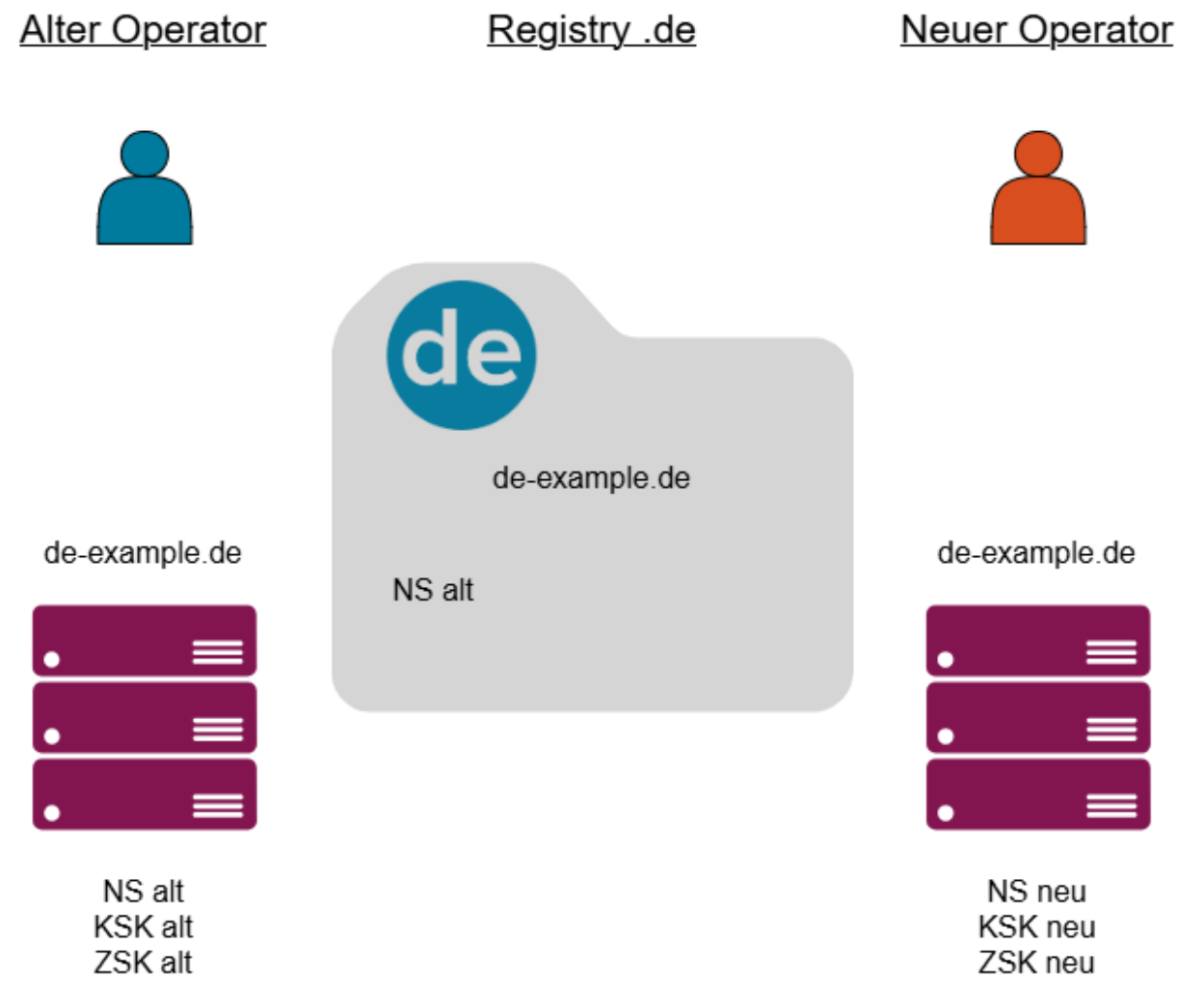
Lösung

folgende Schritte

Schritt 1

Das RegAcc löscht „KSK alt“, „KSK neu“ und „ZSK neu“ im Domainobjekt der Registry und versetzt die Domain damit in den Zustand insecure (UPDATE 2A).

Bild 5: RegAcc hat die Domain in den Zustand insecure gesetzt



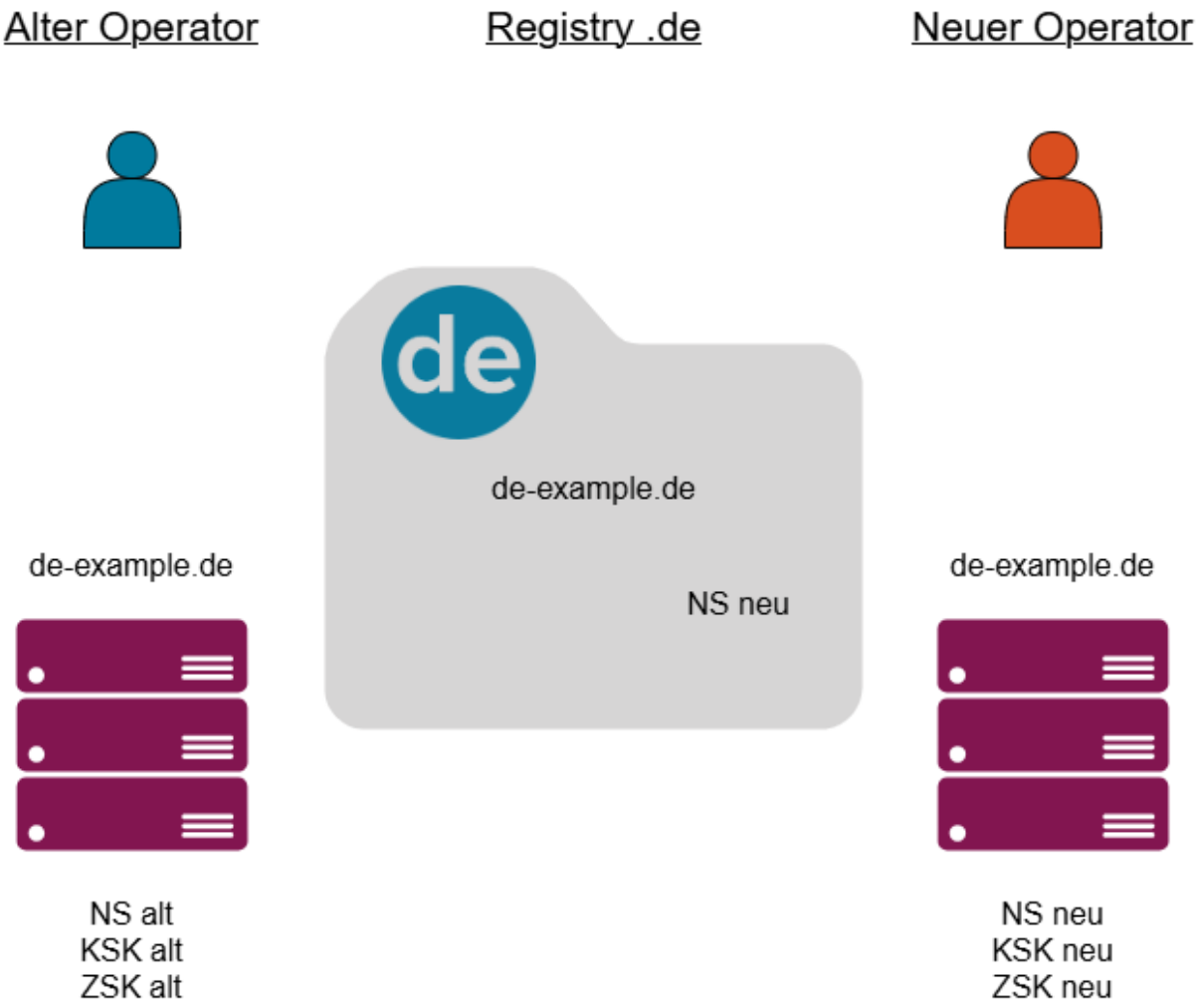
Schritt 2

Dann ist zunächst abzuwarten, bis die Information über die unsignierte Zone de-example.de auf den Resolvern verfügbar ist. Ziel ist sicherzustellen, dass kein DS-RRSet mehr im DNS (inklusive Caches) zu finden ist. Dafür muss seit der Veröffentlichung in der .de-Zone mindestens die TTL des DS-RRSets abgelaufen sein. Bei einer TTL in der .de-Zone von 24 Stunden und einem regulären Abstand der .de-Zonenveröffentlichungen von zwei Stunden ergäbe sich eine Wartezeit von etwa 26 Stunden.

Schritt 3

Das RegAcc ändert die Nameserver-Information in der Registry auf den neuen Operator (UPDATE 2B).

Bild 6: RegAcc hat in der Registry „NS alt“ in „NS neu“ geändert



Schritt 4

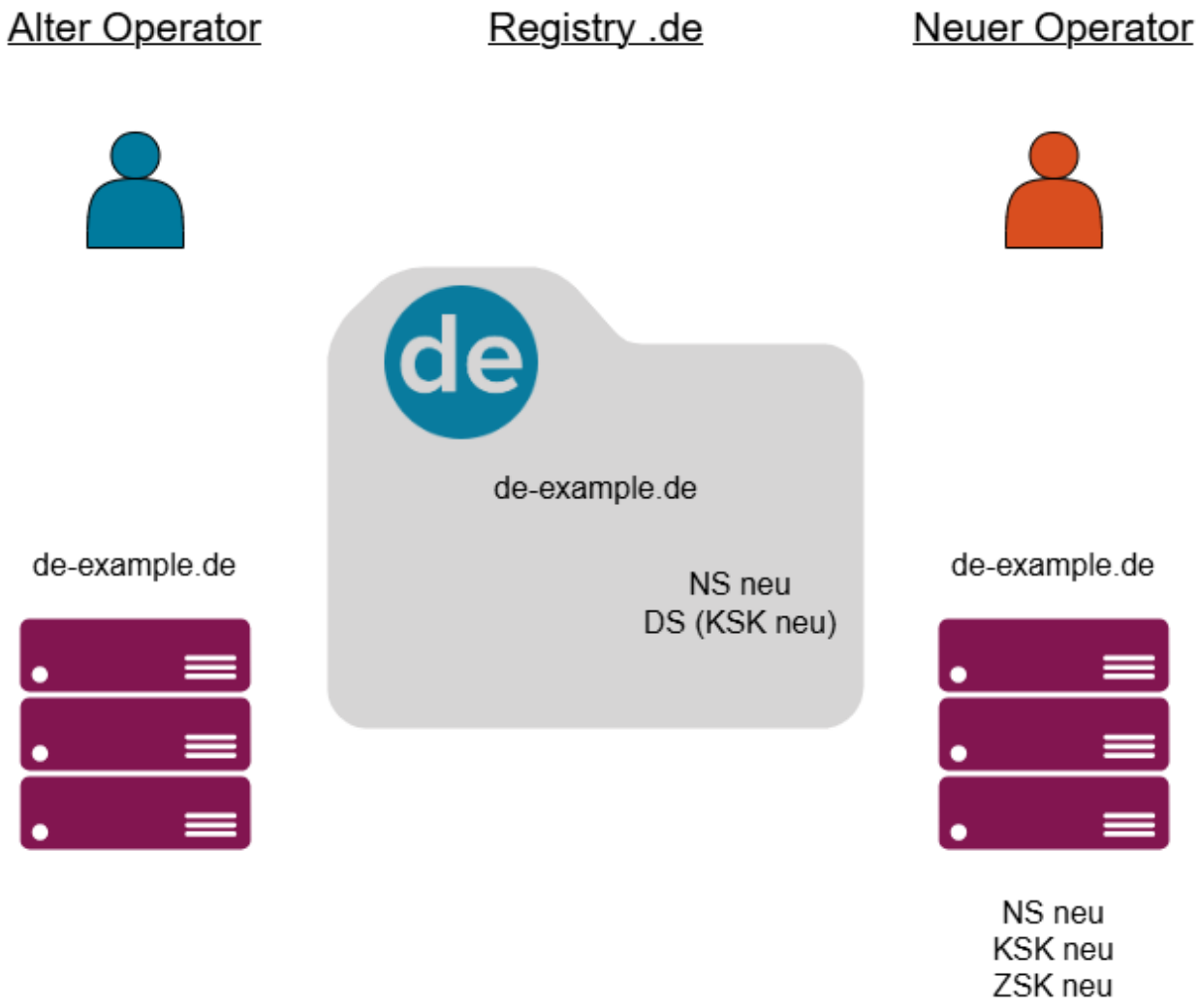
Dann ist zunächst wieder abzuwarten, bis die Information zu den nun gültigen Nameservern („NS neu“) des neuen Operators allen Resolvern bekannt ist. Ziel ist sicherzustellen, dass keine DNS-Anfragen an die Infrastruktur des alten Ope-

rators geschickt werden. Dafür muss seit der Veröffentlichung des neuen NS-RRSet in der .de-Zone mindestens die Summe der TTLs des NS-RRSet in der .de-Zone und der TTL des NS-RRSet in der delegierten Zone abgelaufen sein.

Schritt 5

Nach dieser Wartezeit wird das Schlüsselmaterial des neuen Operators durch den RegAcc in der Registry abgelegt (UPDATE 3).

Bild 7: RegAcc hat den KSK neu in der Registry hinterlegt



Der Operatorwechsel ist nun abgeschlossen und die Zone de-example.de muss vom alten Operator nicht mehr unterstützt werden.

Operatorwechsel ohne Beteiligung des alten Operators mit Providerwechsel

Aufgabenstellung

Falls nach dem vorher beschriebenen UPDATE 1 die aktualisierte Zone mit „ZSK neu“ nicht auf den Nameservern des alten Operators verfügbar ist, wird der Wechsel ohne dessen Unterstützung durchgeführt.

Dadurch gibt es technisch keine andere Lösung, als die Domain zunächst vorübergehend in den Zustand insecure zu versetzen.

Alle Änderungen werden von ein- und demselben RegAcc in der Registry vorgenommen.

Lösung

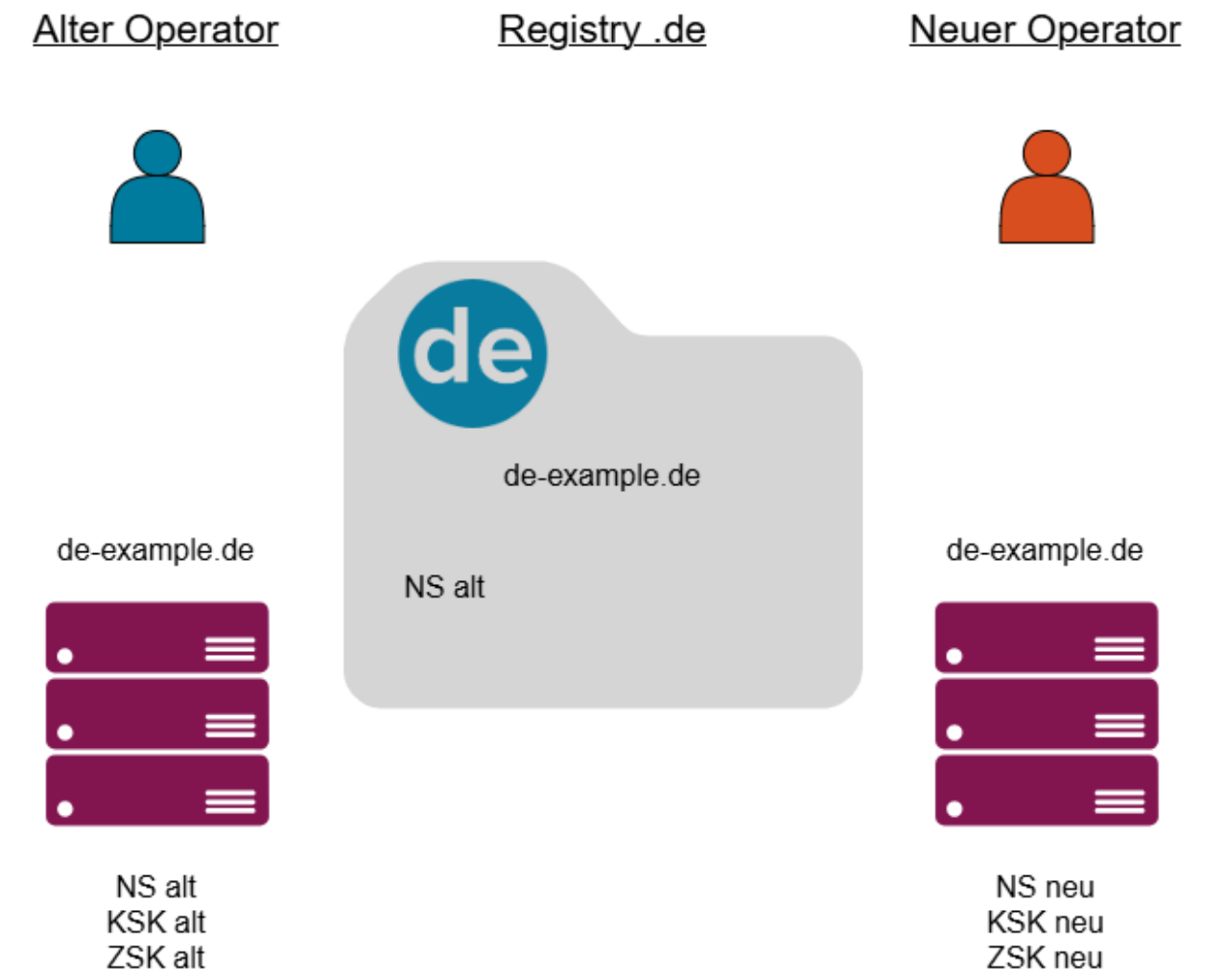
Falls nach dem vorher beschriebenen UPDATE 1 die aktualisierte Zone mit „ZSK neu“ nicht auf den Nameservern des alten Operators verfügbar ist, wird der Wechsel ohne dessen Unterstützung durchgeführt.

Dadurch gibt es technisch keine andere Lösung, als die Domain zunächst vorübergehend in den Zustand insecure zu versetzen.

Schritt 1

Das RegAcc löscht „KSK alt“, „KSK neu“ und „ZSK neu“ im Domainobjekt der Registry und versetzt die Domain damit in den Zustand insecure (UPDATE 2A).

Bild 8: RegAcc hat die Domain in den Zustand insecure gesetzt



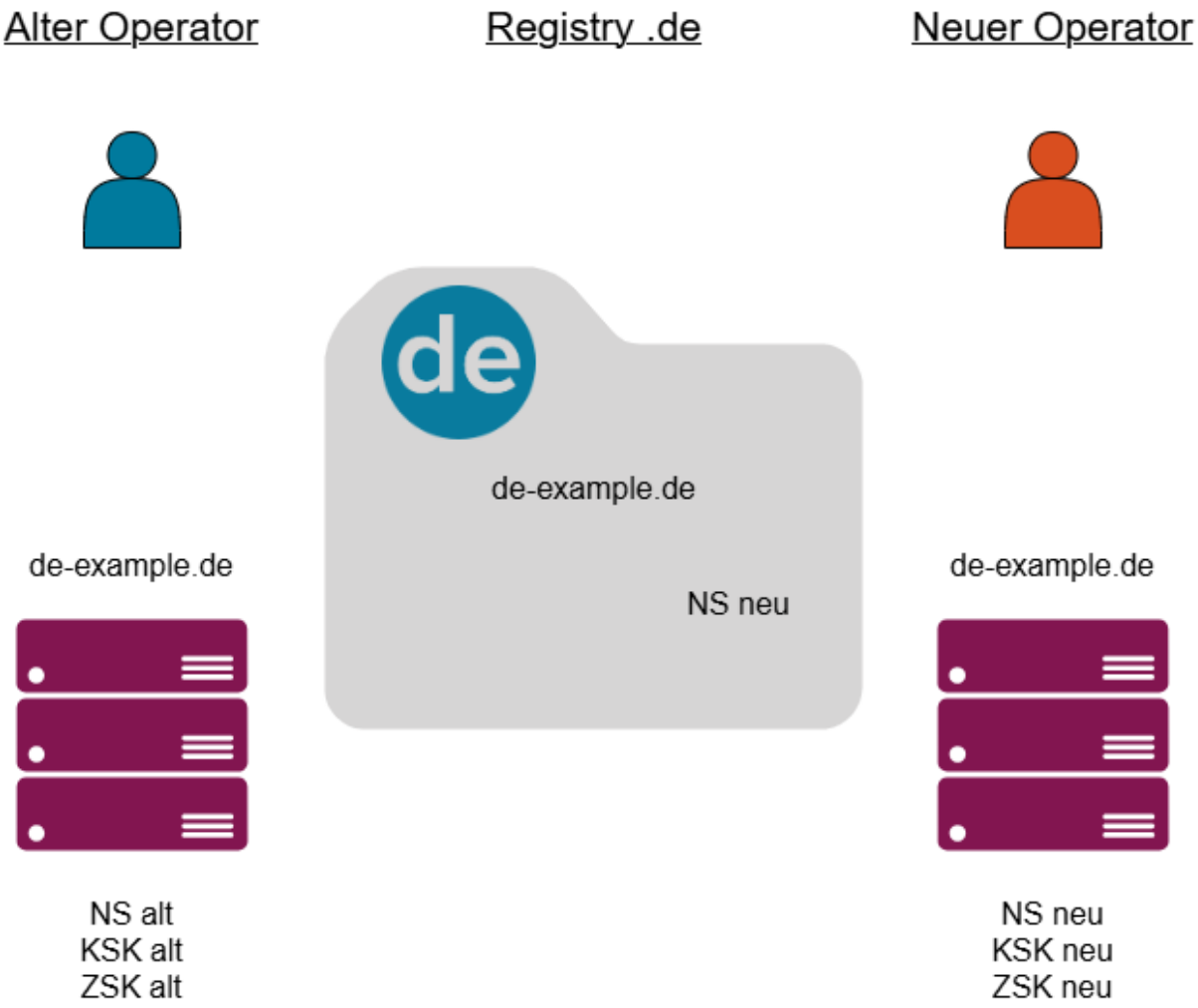
Schritt 2

Dann ist zunächst abzuwarten, bis die Information über die unsignierte Zone de-example.de auf den Resolvern verfügbar ist. Ziel ist sicherzustellen, dass kein DS-RRSet mehr im DNS (inklusive Caches) zu finden ist. Dafür muss seit der Veröffentlichung in der .de-Zone mindestens die TTL des DS-RRSets abgelaufen sein. Bei einer TTL in der .de-Zone von 24 Stunden und einem regulären Abstand der .de-Zonenveröffentlichungen von zwei Stunden ergäbe sich eine Wartezeit von etwa 26 Stunden.

Schritt 3

Das RegAcc ändert die Nameserver-Information in der Registry auf den neuen Operator (UPDATE 2B).

Bild 9: RegAcc hat in der Registry „NS alt“ in „NS neu“ geändert



Schritt 4

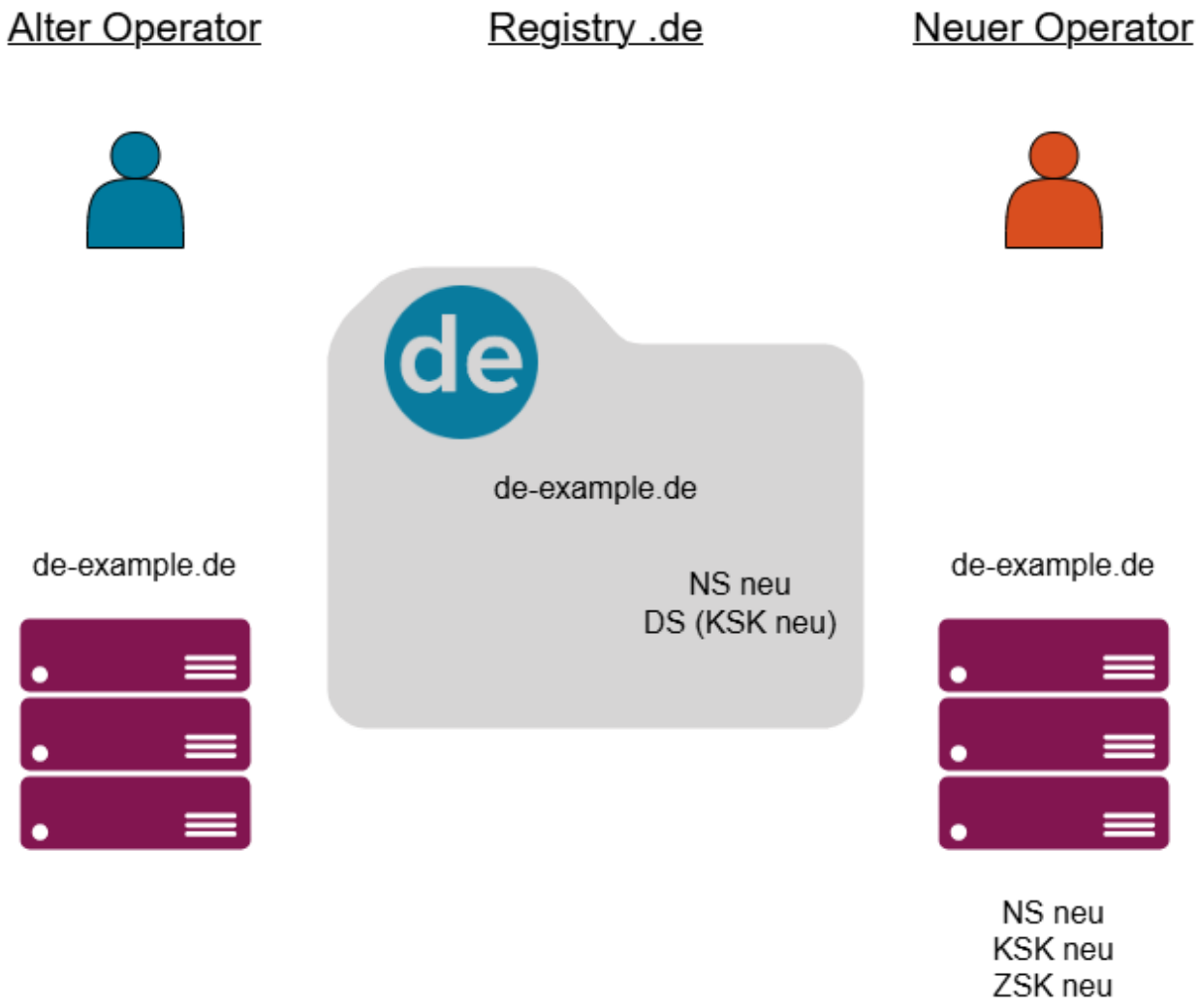
Dann ist zunächst wieder abzuwarten, bis die Information zu den nun gültigen Nameservern („NS neu“) des neuen Operators allen Resolvern bekannt ist. Ziel ist sicherzustellen, dass keine DNS-Anfragen an die Infrastruktur des alten Ope-

rators geschickt werden. Dafür muss seit der Veröffentlichung des neuen NS-RRSet in der .de-Zone mindestens die Summe der TTLs des NS-RRSet in der .de-Zone und der TTL des NS-RRSet in der delegierten Zone abgelaufen sein.

Schritt 5

Nach dieser Wartezeit wird das Schlüsselmaterial des neuen Operators durch den RegAcc in der Registry abgelegt (UPDATE 3).

Bild 10: RegAcc hat den KSK neu in der Registry hinterlegt



Der Operatorwechsel ist nun abgeschlossen und die Zone de-example.de muss vom alten Operator nicht mehr unterstützt werden.