

DNSSEC - Einführung

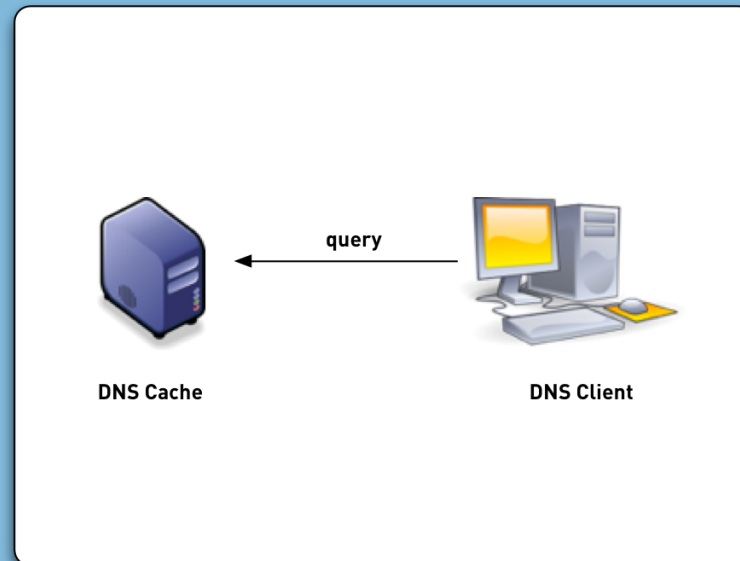
Patrick Koetter und Carsten Strotmann, sys4 AG

Agenda

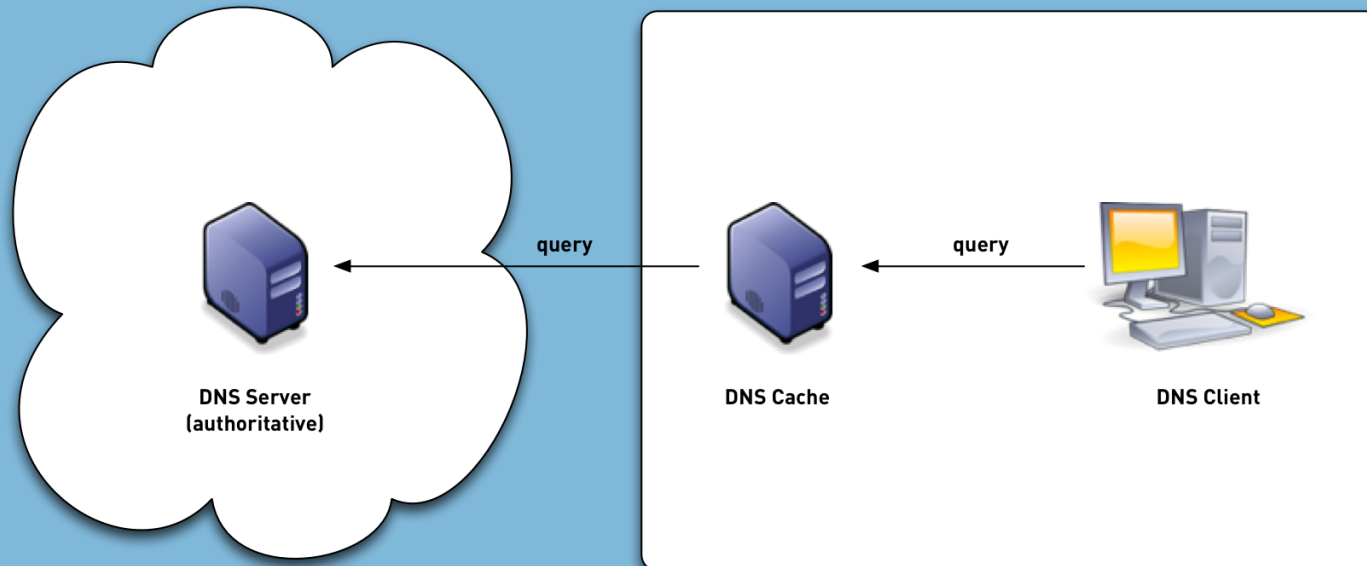
1. DNS Sicherheit (oder Nicht-Sicherheit)
2. Was ist DNSSEC
3. DNSSEC Geschichte
4. DNSSEC Validierung Grundlagen
5. DNSSEC Resource Records
6. DNSSEC Validierung (vereinfacht)

DNS Sicherheit (oder die Abwesenheit derselben)

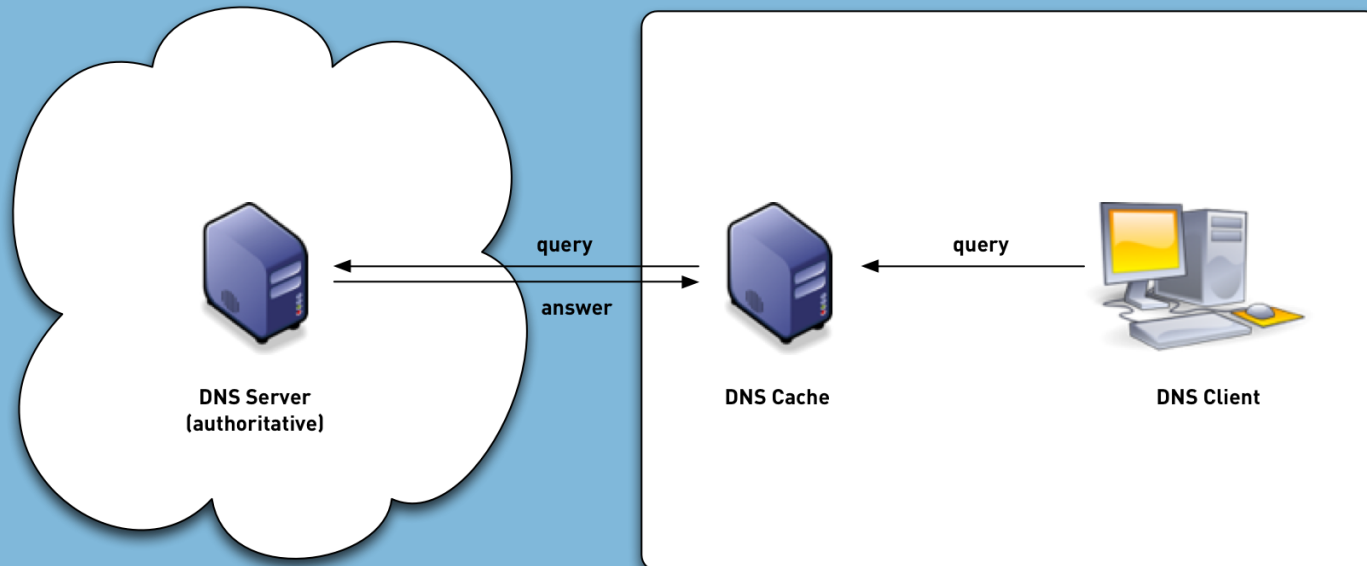
DNS Sicherheit - Grundlagen



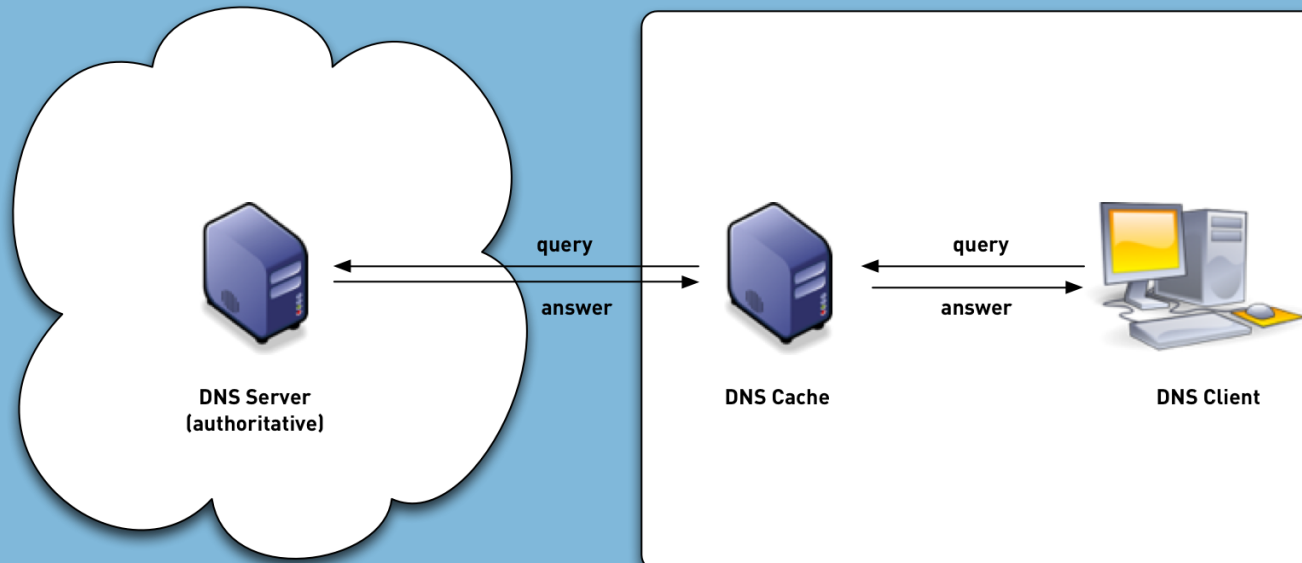
DNS Sicherheit - Grundlagen



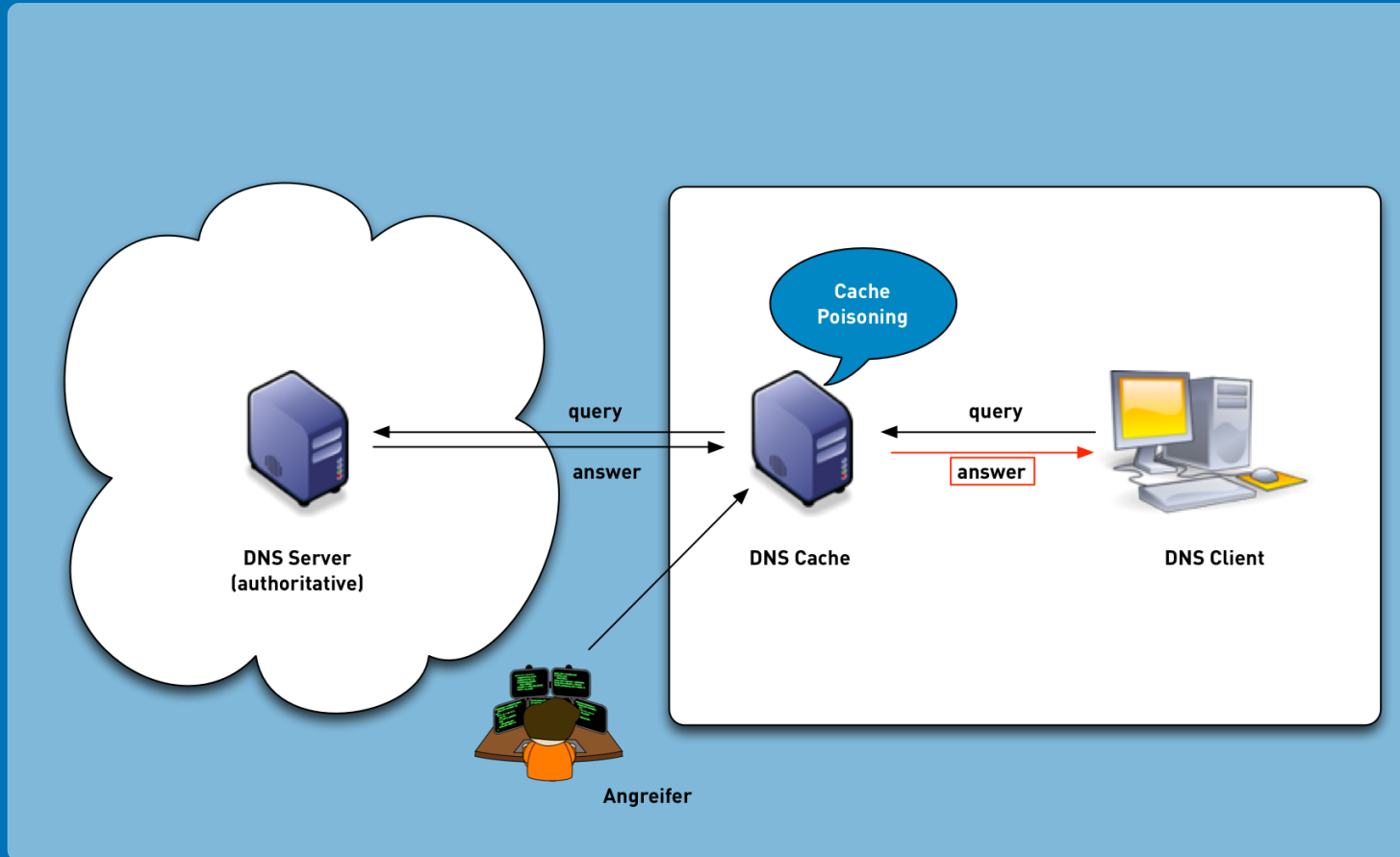
DNS Sicherheit - Grundlagen



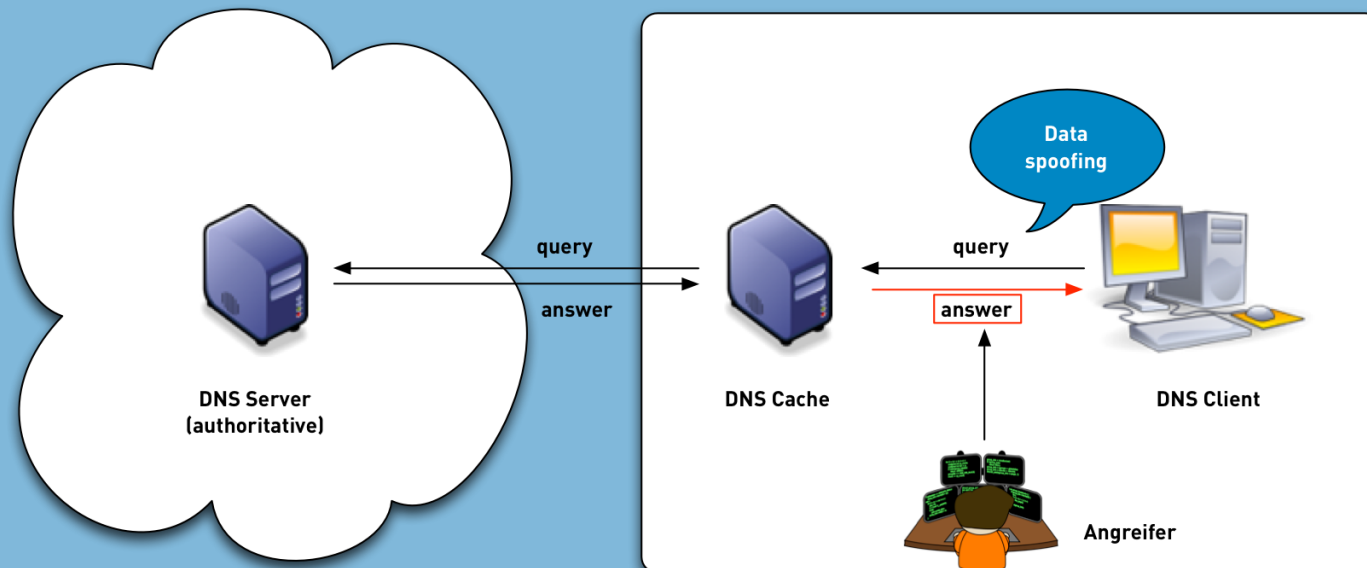
DNS Sicherheit - Grundlagen



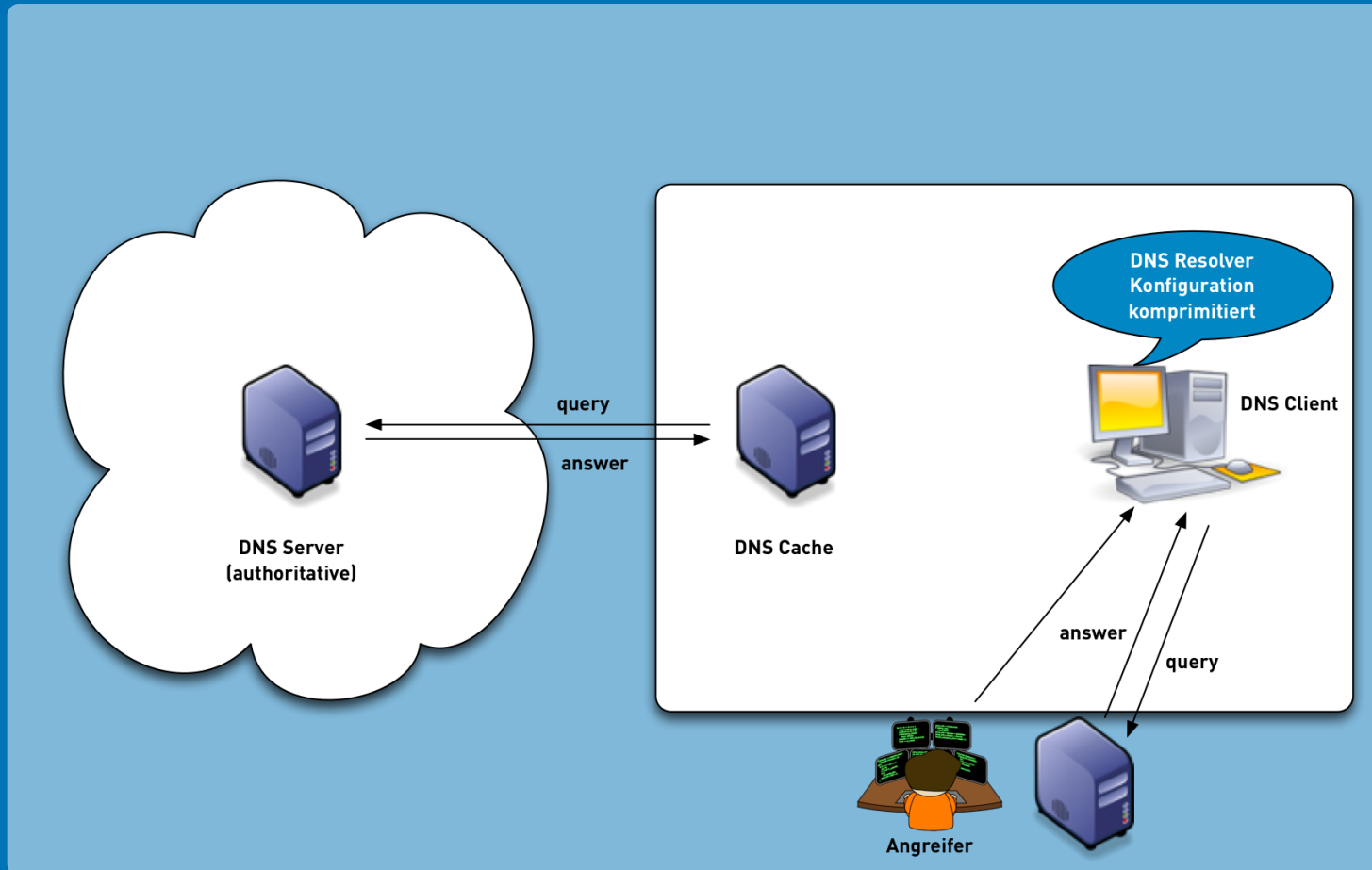
DNS Sicherheit - Angriffe



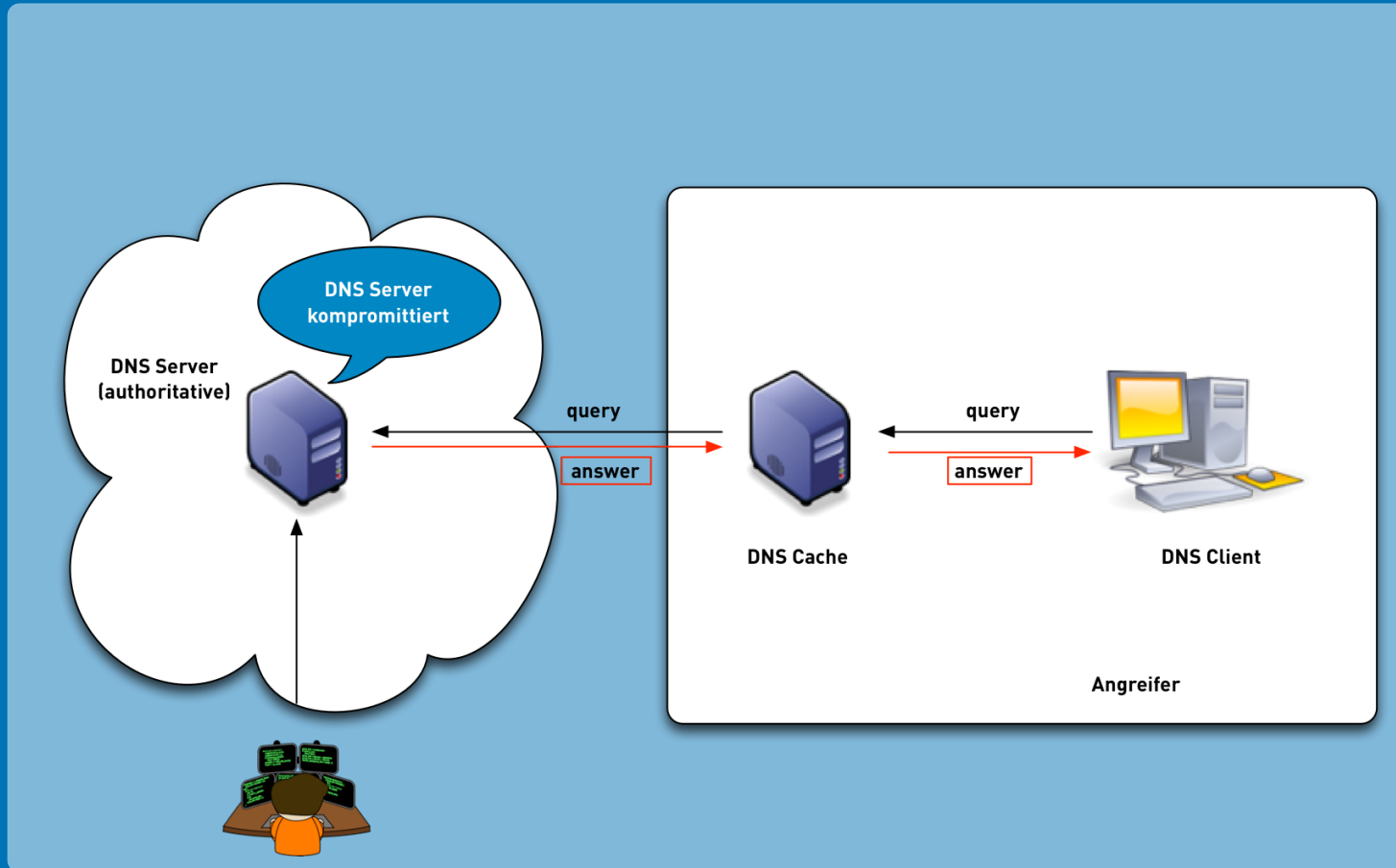
DNS Sicherheit - Angriffe



DNS Sicherheit - Angriffe



DNS Sicherheit - Angriffe



DNSSEC

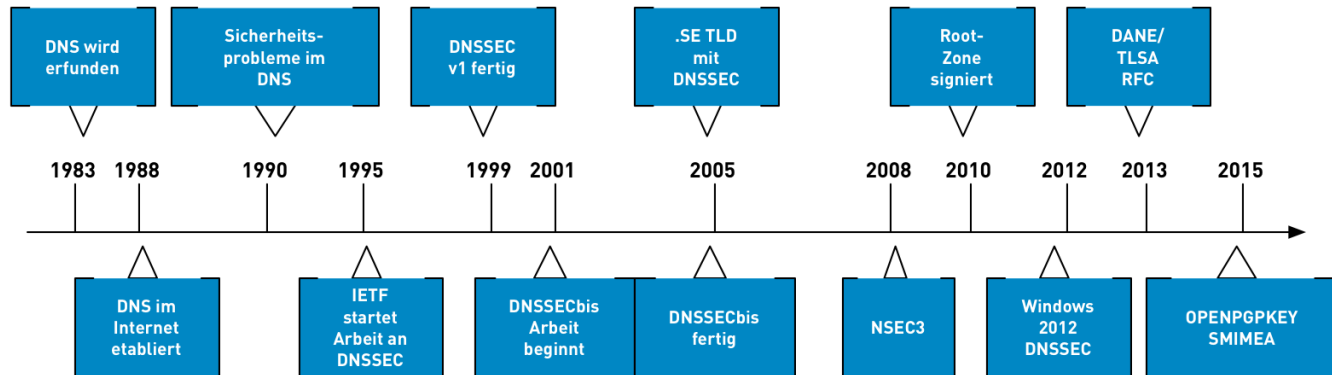


Was ist DNSSEC

- Absicherung von DNS Daten mittels kryptografischer Signaturen
- Asymmetrische Verschlüsselung
- Der Empfänger von DNS Daten kann prüfen (validieren) das
 - Die Daten vom Besitzer des privaten Schlüssels der Zone kommen
 - Die Daten seit dem Einstellen in die Zone nicht geändert wurden

DNSSEC Geschichte

DNSSEC Geschichte



DNSSEC Validierung Grundlagen

Zone "de"

Zone "sys4.de"

www.sys4.de.
www.sys4.de.

```
3600 IN      A 194.126.158.154
3600 IN      RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QP0/JkQ1TIpqW9k421nw9rXey
P5E58z1ufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBF9vNoGidY= )
```

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Zone "de"

Zone "sys4.de"

```
sys4.de.      3600 IN      DNSKEY 256 3 8 (
               AwEAAZFu5qBo0tXH2VN1sxjKyrp+1sc/wyyw2Cn7guV
               7RMe4D1X/vU/dvF4Zy2yvv98ZHscBwqBRMbspr33fu28
               n27dEZrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg
               ThYt2Y54H607wuUP2ulhJjz2aQfmTbENLNL18gt8zIOP
               ) ; key id = 57438
sys4.de.      3600 IN      DNSKEY 257 3 8 (
               AwEAAex3DFQLs4HRlgaKwBr1bcRuxR+0kZ/aUIW71lrh
               ma9XxQsrd796veMR00ET2sKVsfAk4RbbFH+OcUMkN/H1
               94jCV3HPhlw5tIoABfzm7PytlsmYg3k3oNwT6CnhYw3Z
               aGXbfjW2g3/yuPIY1iH3aB1hm2W1aqaZuuB5SRs0PDgP
               90dvmq8Ceh0+2SFS0Qp2M4p9u4eMWWueRAwaaNv11+e
               bXf4L/LnkXXYnEnqFFawanLRmsxoQhz9rLAIpFrL4QtX
               +1EaI7QWk9oQzcrCga/9cyhuVcIcxbKXrQVrjpDqXrD6
               +WQZ+qlQgXwzQ094fQPB8PGK9eN0hjKeENRXVcE=
               ) ; key id = 47579
sys4.de.      3600 IN      RRSIG DNSKEY 8 2 3600 20151009200043 (
               20151002141517 47579 sys4.de.
               2nTsIWmc9Id/jjyDXQFOXXRuPbsnG6HsIQkA7JkYRw1F
               VhiKdhorJA9tSIIbafwnlVWnmFHfgj4uic15lP3SHpty
               hFaSeqWIUN+6fxRnLA8ZZeHyH/YtzY2UKORVbePNG8ra
               3Rfq00yPNe3g+0Byi/1esXxymu+MQPo8zHAM9sysXx5W
               4rjbbdPJ9mbCrT/9SWiHxQv/nu2cUxKXn1ao8NpsxUsZ
               ZNYg956af0BJ3lcS1tCxIGv315FMVxySciZneKJvhv1x
               H25wAXo0dSOBUEbxImPUz1Fb09dYgKYuxUB7fS848c5L
               11yFrrZFsg4khSuMbbXlw+UcaFzvNCjumQ== )
www.sys4.de.  3600 IN      A 194.126.158.154
www.sys4.de.  3600 IN      RRSIG A 8 3 3600 20151009061215 (
               20151002141517 57438 sys4.de.
               NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
               P5E58z1ufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
               QutK3GhXh5R+RtFhkPP0R87cvRy60026p1/R8Bm5QX6P
               H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBF9vNoGidY= )
```

Zone Signing
Key (ZSK)

Key Signing Key
(KSK)

Signatur der
Schlüssel
erstellt mit dem
KSK

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Zone "de"

```
sys4.de.      86400 IN DS 47579 8 2 (
              47D772EA1CE9CFBFB1A38BE335372F44C28878C93BF0
              70E2855F7659DA935887 )
sys4.de.      86400 IN RRSIG DS 8 2 86400 20151011080000 (
              20151004080000 52896 de.
              FXaMfucwDnkuoYVXHlax+I00zwPEoAYCrGJ7mQmjl1IN
              nVhlwEpH3oco++wpSgqY0Af8dXBcN9nbXaTayCA5rt1u
              aC+3P0hSKvjKPM1rFDrk2WZdz36pArtPyYglT2Lr29Yo
              o1UTieSEpaYdiC3Boq1S3q03+FwVqYLQAYQH0rI= )
```

Hash des
sys4.de KSK

Signatur des DS-
Record erstellt
mit dem ZSK der
DE Zone

Zone "sys4.de"

```
sys4.de.      3600 IN      DNSKEY 256 3 8 (
              AwEAAAdZFu5qBo0tXH2VN1sxjKyrp+lsc/wyyw2Cn7guV
              7RMe4D1X/vU/dvF4Zy2yvv98ZHscBwqBRMbspr33fu28
              n27dEzrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg
              ThYt2Y54H607wuUP2ulhJjz2aQfmTBENLNL18gt8zIOP
              ) ; key id = 57438
sys4.de.      3600 IN      DNSKEY 257 3 8 (
              AwEAAex3DFQLs4HRlgaKwBr1bcRuxR+0kZ/aUIW71lRh
              ma9XxQsrd796veMR00ET2sKVsFAk4RbbFH+OcUMkN/H1
              94jCV3HPhlw5tIoABfzm7PytlsmYg3k3oNwT6CnhYw3Z
              aGXbfjw2g3/yuPIY1iH3aB1hM2W1aqaZuuB5SRs0PDgP
              90dvmq8Ceh0+2SFS0q2M4p9u4eMWWueRAwaaNv11+e
              bXf4L/LnkXXYnEnqFFawanLRmsxoQhZ9rLAIpFrL4QtX
              +1EaI7QWk9oQzcrCga/9cyhuVcIcxbKXrQVrjPdqXrD6
              +WQZ+qlQXwzQ094fQPB8PGK9eN0hjKeENRXVcE=
              ) ; key id = 47579
sys4.de.      3600 IN      RRSIG DNSKEY 8 2 3600 20151009200043 (
              20151002141517 47579 sys4.de.
              2nTsIWmc9Id/jjyDXQFOXXRuPbsnG6HsIQkA7JkYRw1F
              VhiKdhorJA9tSIIbafwnlVWnmFHfgj4uic151P3SHpty
              hFaSeqWIUN+6fxRn1A8ZZeHyH/YtzY2UKORVbePNG8ra
              3Rfq00yPNe3g+0Byi/1esXxymu+MQPo8zHAM9sysXx5W
              4rjbbdPJ9mbCrT/9SWiHxQv/nu2cUxKXn1ao8NpsxUsZ
              ZNYg956af0BJ3lcS1tCxIGv315FMVxySciZneKJvhv1x
              H25wAXo0dSOBUEbxImPUz1Fb09dYgKYuxUB7fS848c5L
              11yFrrZFsg4khSuMbbXlw+UcaFzvNCjumQ== )

www.sys4.de.  3600 IN      A 194.126.158.154
www.sys4.de.  3600 IN      RRSIG A 8 3 3600 20151009061215 (
              20151002141517 57438 sys4.de.
              NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
              P5E58z1ufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
              QutK3GhXh5R+RtFhkPP0R87cvRy60026p1/R8Bm5QX6P
              H/Fn9EgucVnhJDn0bmyWzQv/YgdNVBF9vNoGidY= )
```

Zone Signing
Key (ZSK)

Key Signing Key
(KSK)

Signatur der
Schlüssel
erstellt mit dem
KSK

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Zone "de"

Hash des
sys4.de KSK

Signatur des DS-
Record erstellt
mit dem ZSK der
DE Zone

Zone "sys4.de"

Key Signing Key
(KSK)

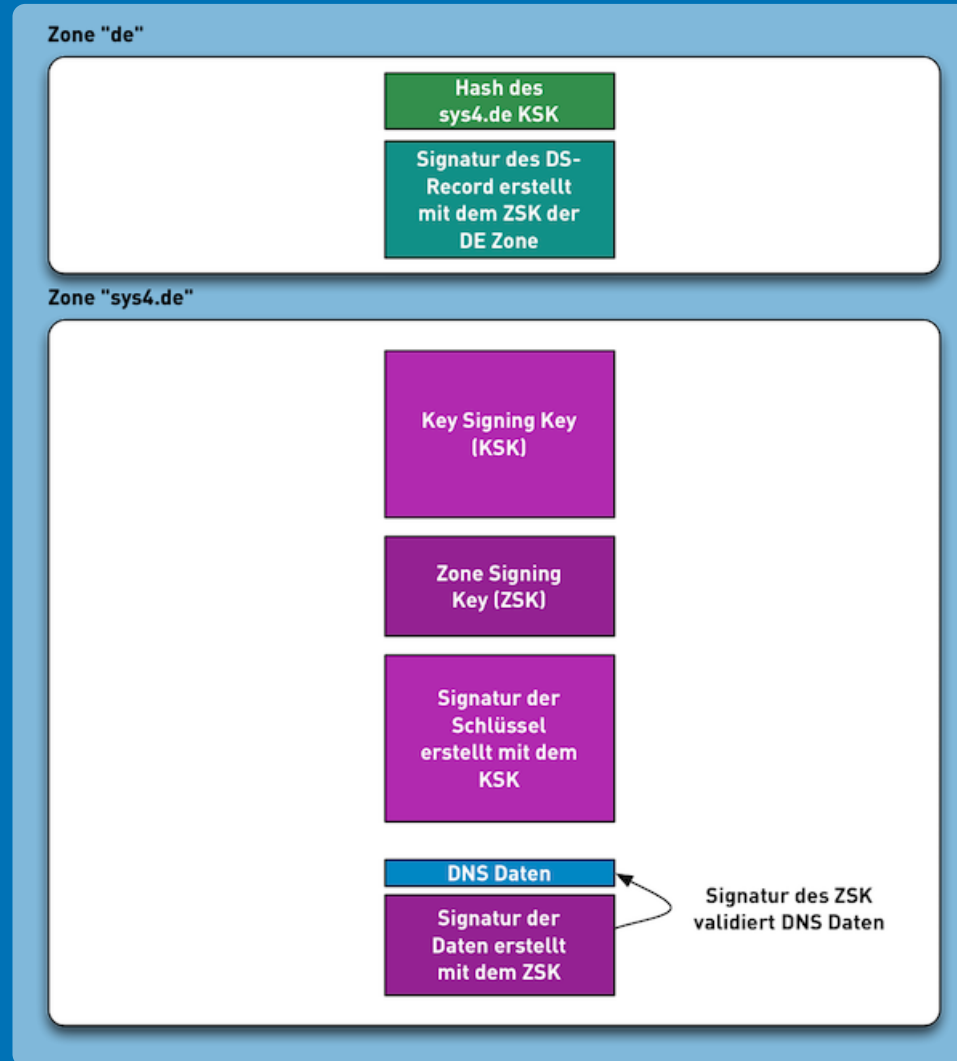
Zone Signing
Key (ZSK)

Signatur der
Schlüssel
erstellt mit dem
KSK

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Signatur des ZSK
validiert DNS Daten



Zone "de"

Hash des
sys4.de KSK

Signatur des DS-
Record erstellt
mit dem ZSK der
DE Zone

Zone "sys4.de"

Key Signing Key
(KSK)

Zone Signing
Key (ZSK)

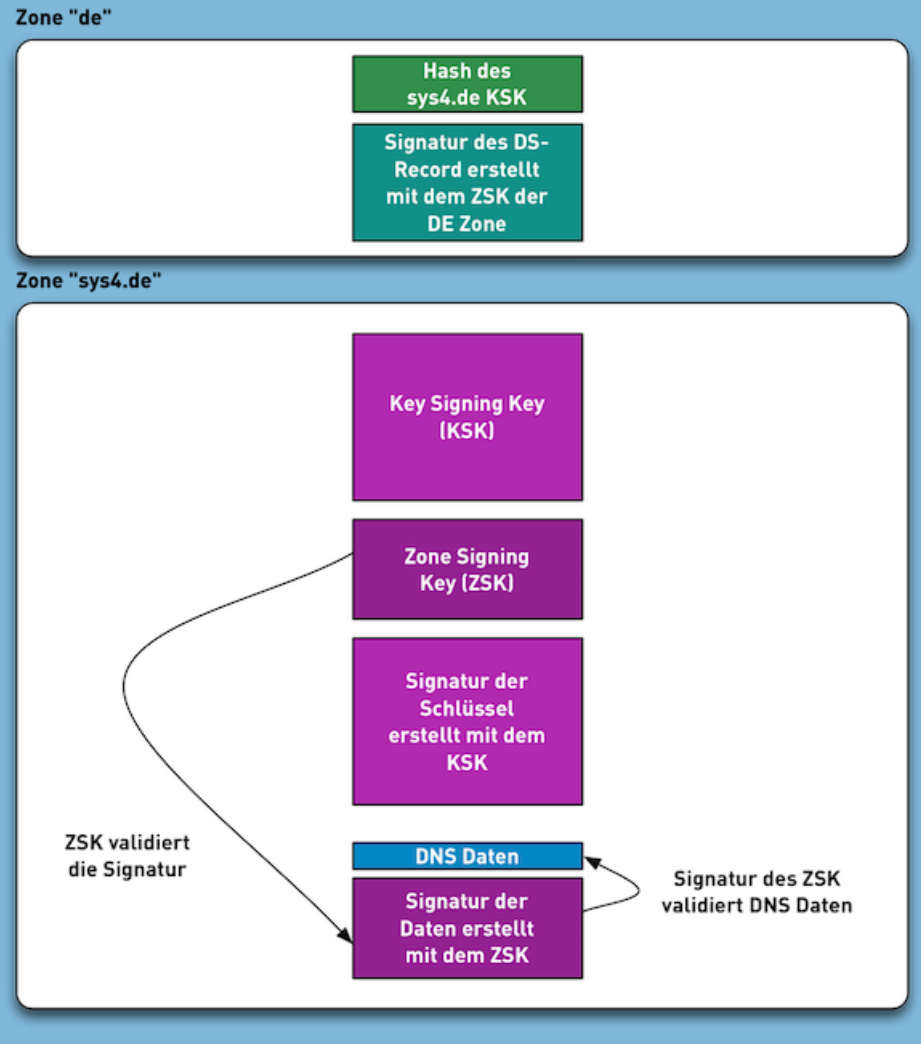
Signatur der
Schlüssel
erstellt mit dem
KSK

ZSK validiert
die Signatur

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Signatur des ZSK
validiert DNS Daten



Zone "de"

Hash des
sys4.de KSK

Signatur des DS-
Record erstellt
mit dem ZSK der
DE Zone

Zone "sys4.de"

Key Signing Key
(KSK)

Zone Signing
Key (ZSK)

Signatur des KSK
validiert ZSK

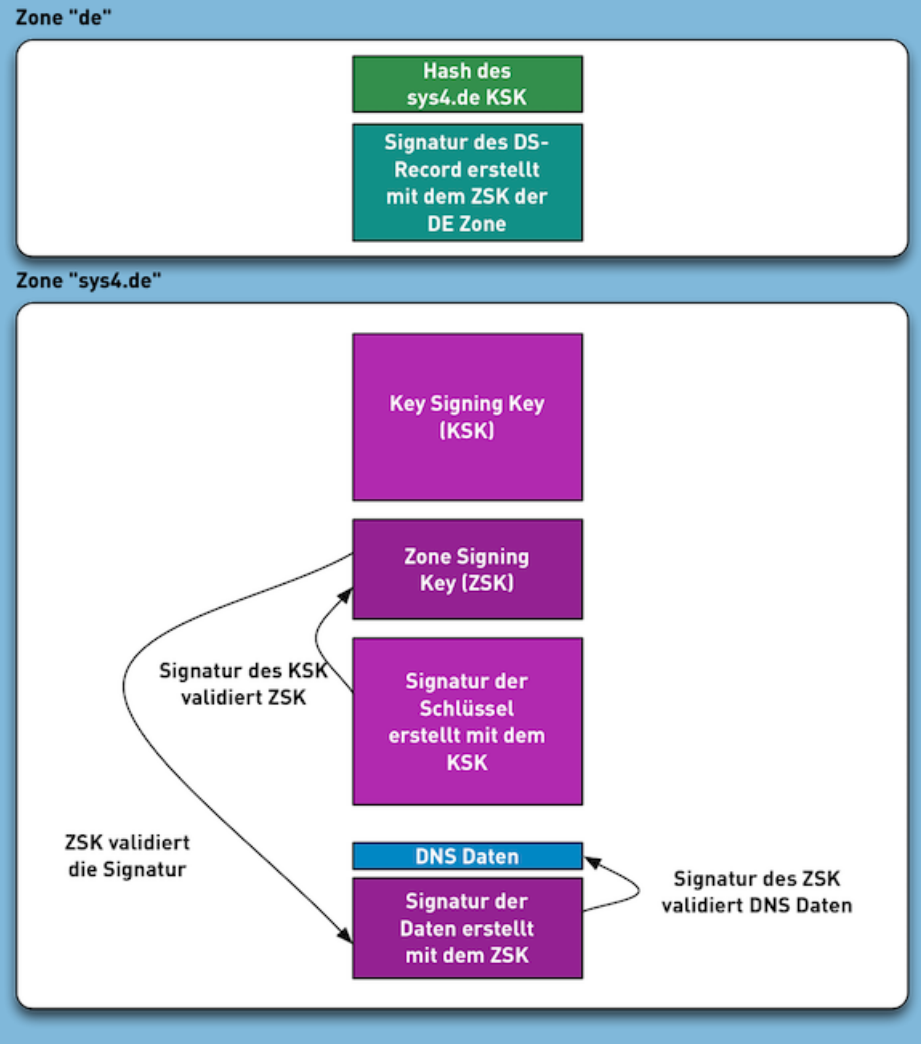
Signatur der
Schlüssel
erstellt mit dem
KSK

ZSK validiert
die Signatur

DNS Daten

Signatur der
Daten erstellt
mit dem ZSK

Signatur des ZSK
validiert DNS Daten

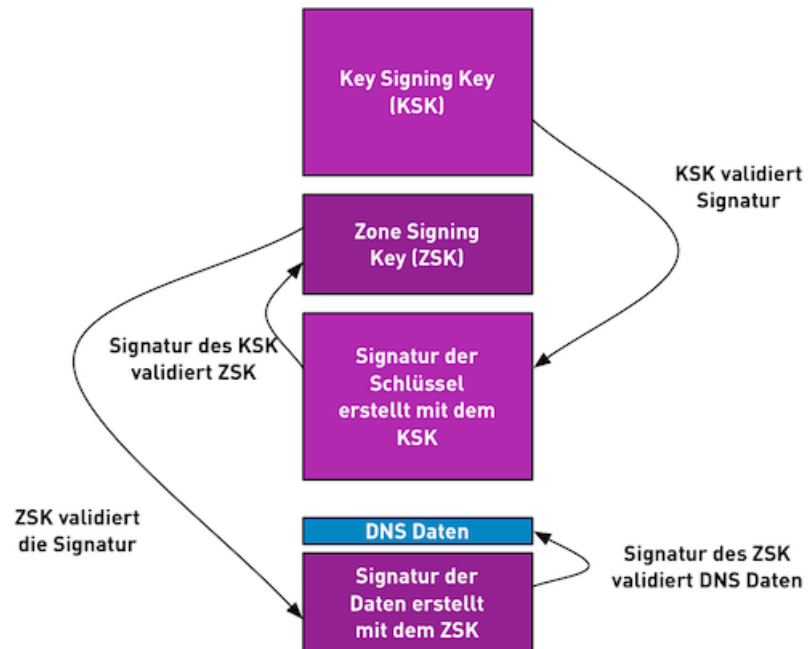


Zone "de"

Hash des
sys4.de KSK

Signatur des DS-
Record erstellt
mit dem ZSK der
DE Zone

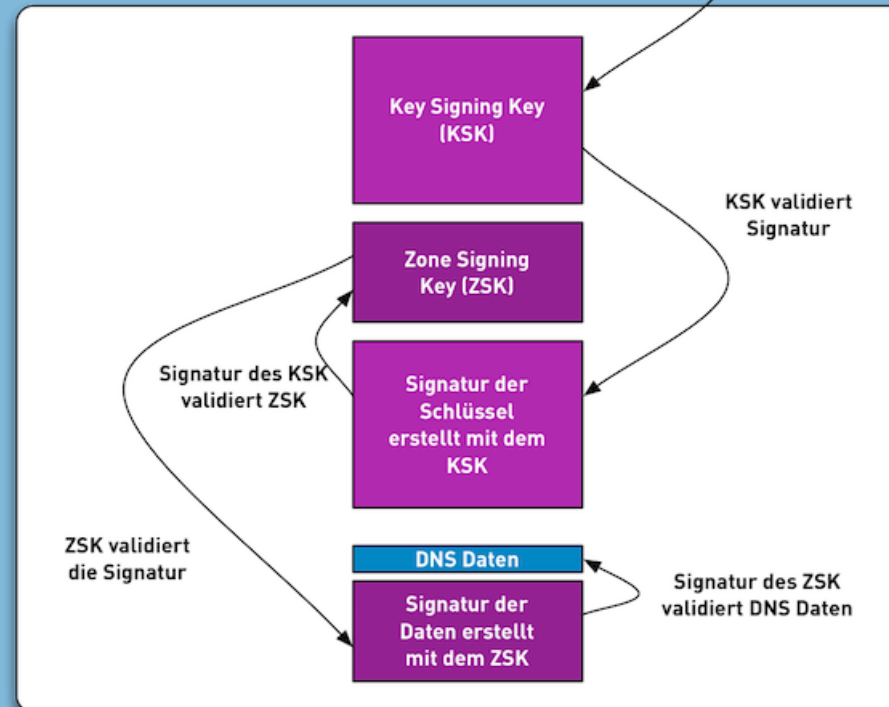
Zone "sys4.de"



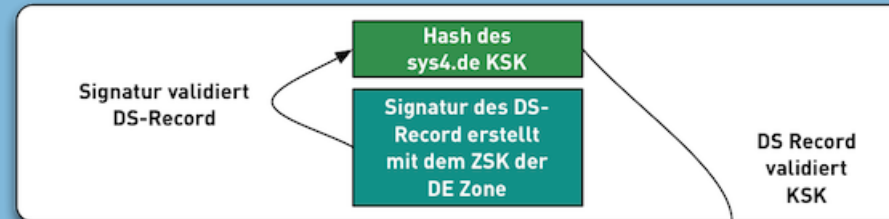
Zone "de"



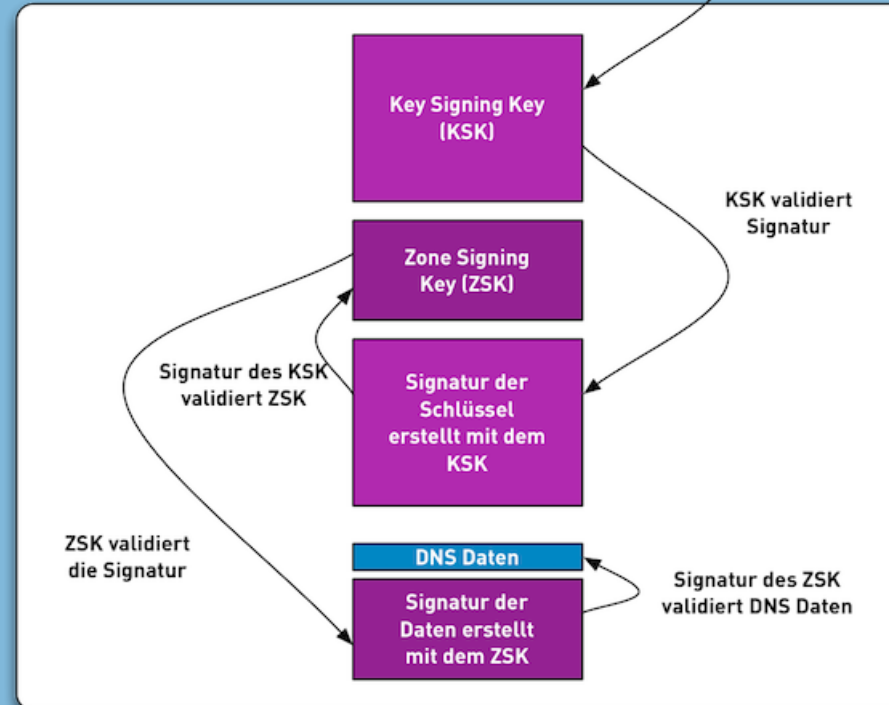
Zone "sys4.de"



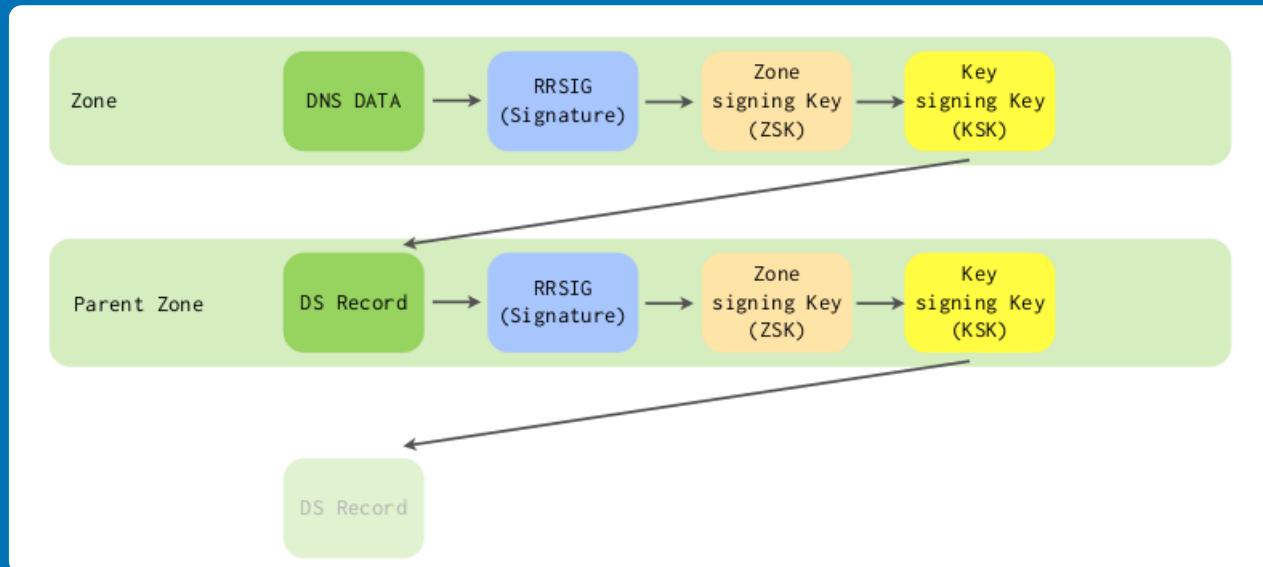
Zone "de"



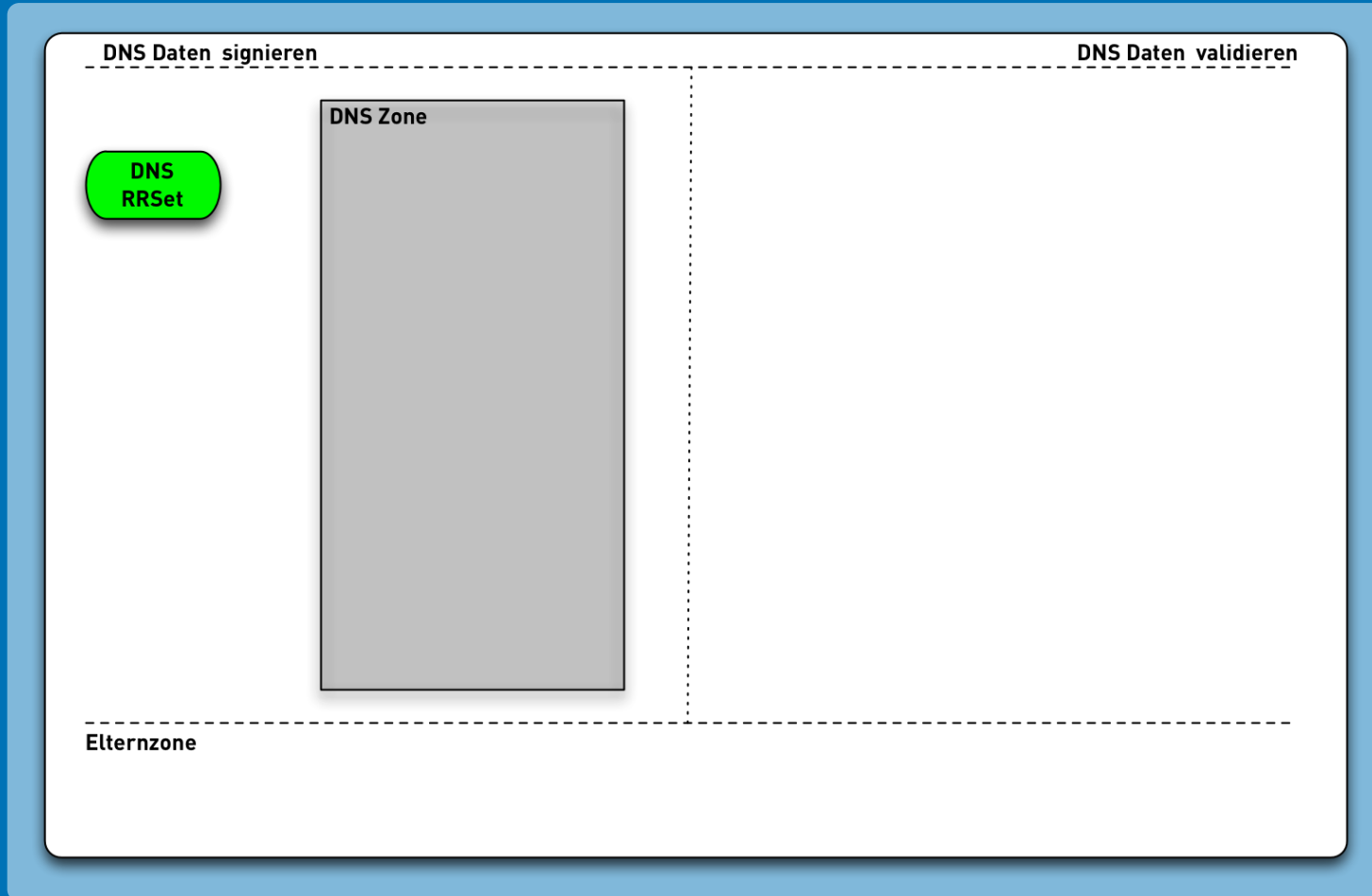
Zone "sys4.de"



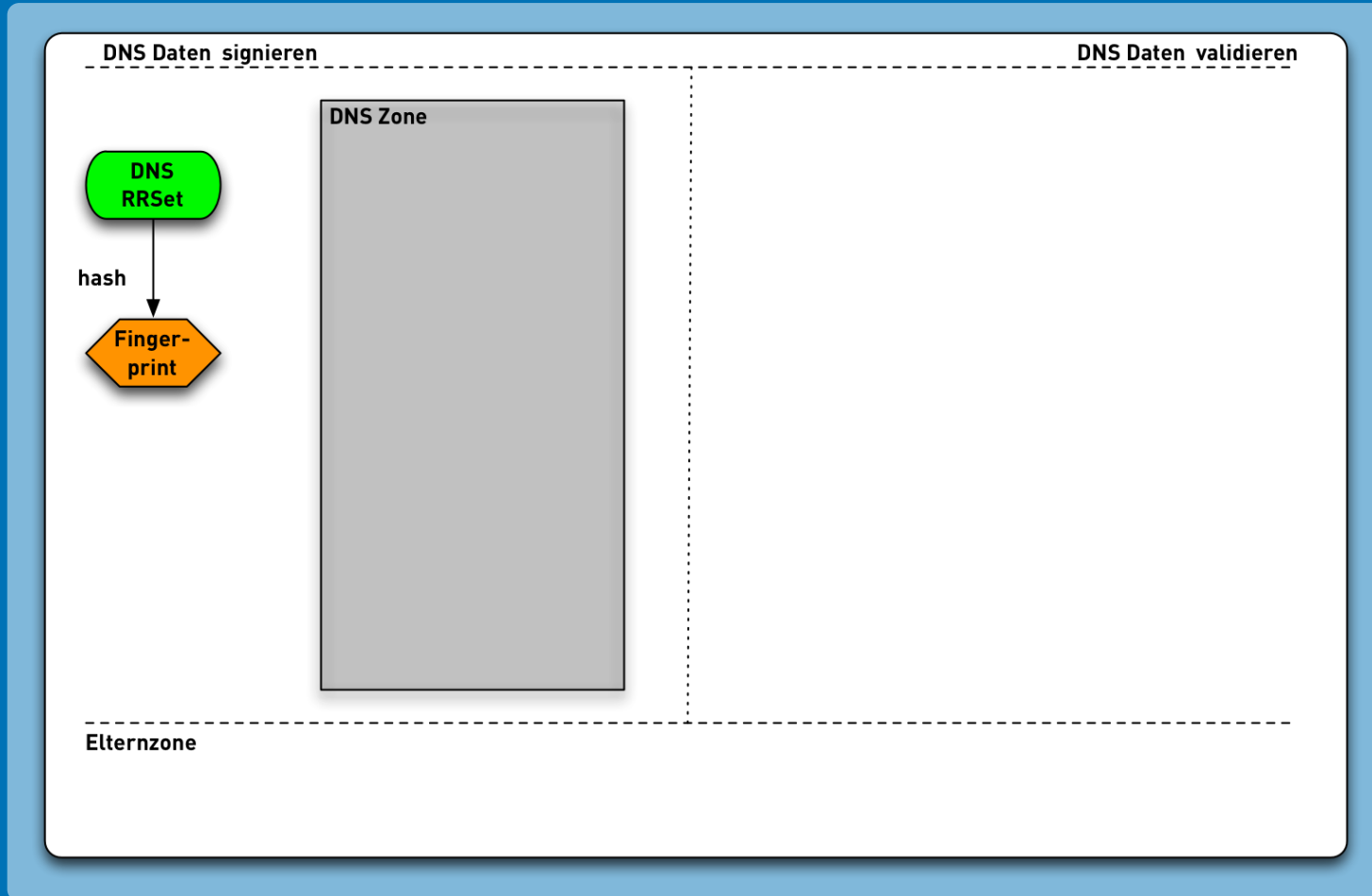
DNSSEC Validierung



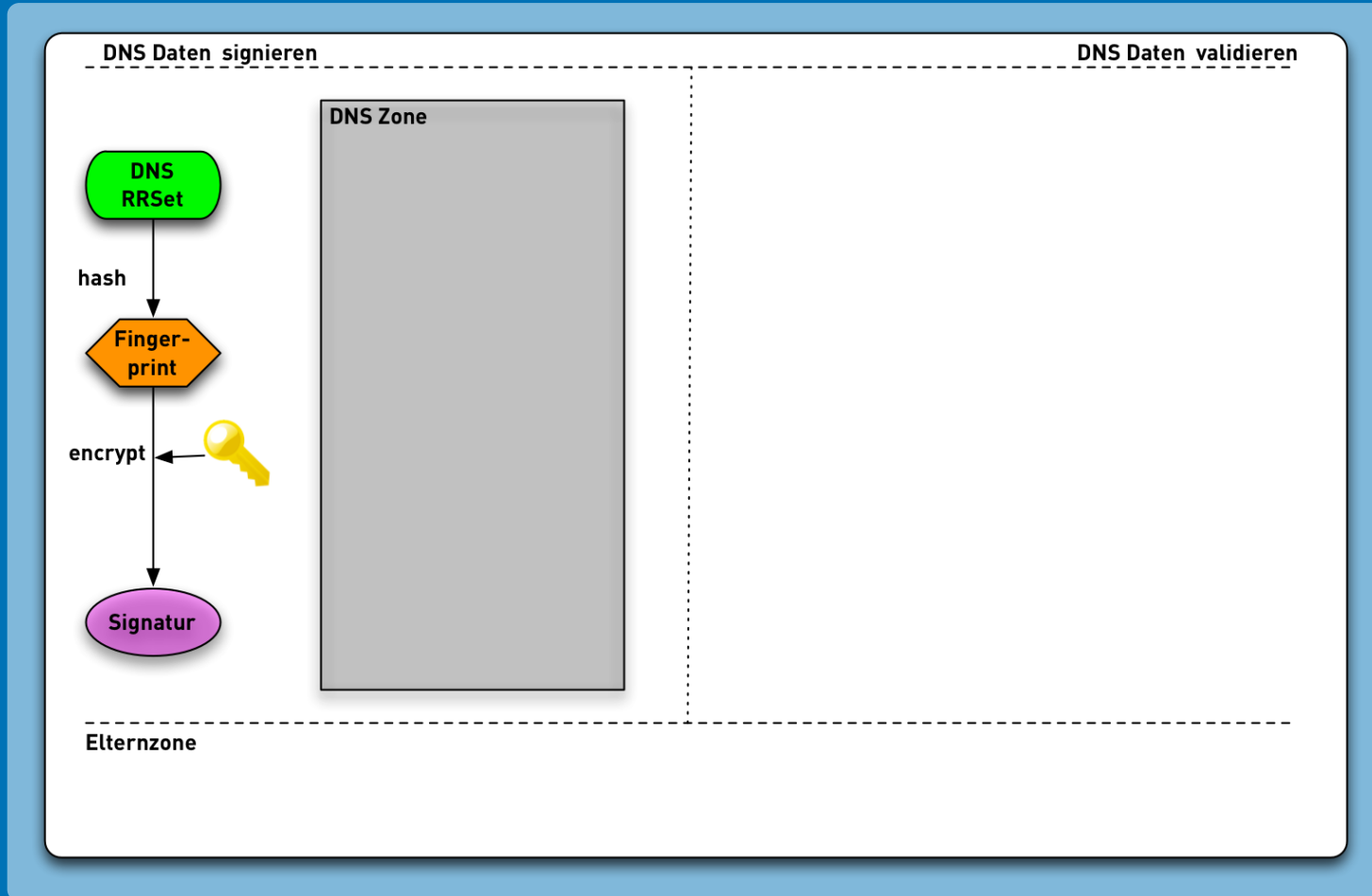
DNSSEC Validierung



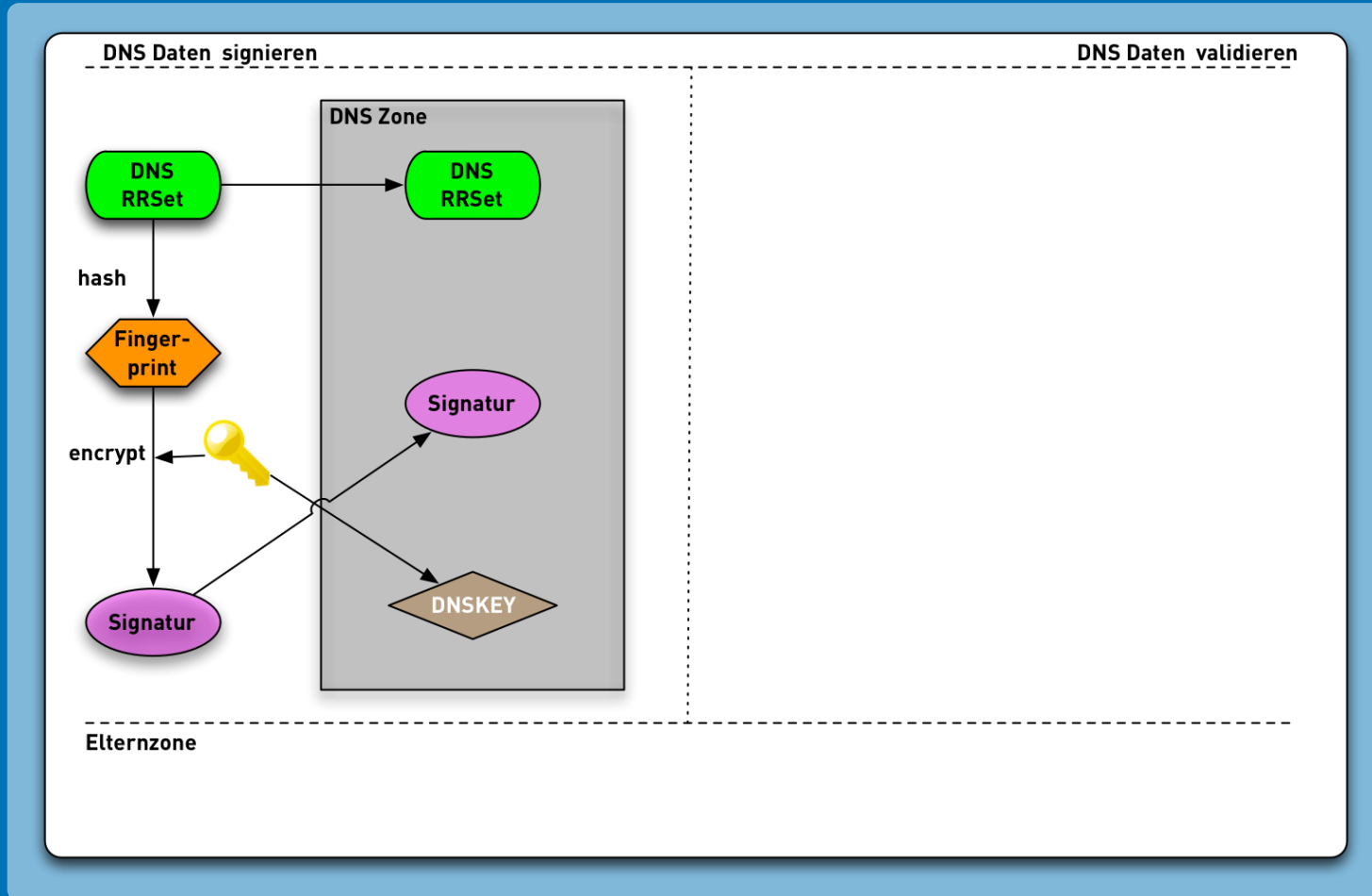
DNSSEC Validierung



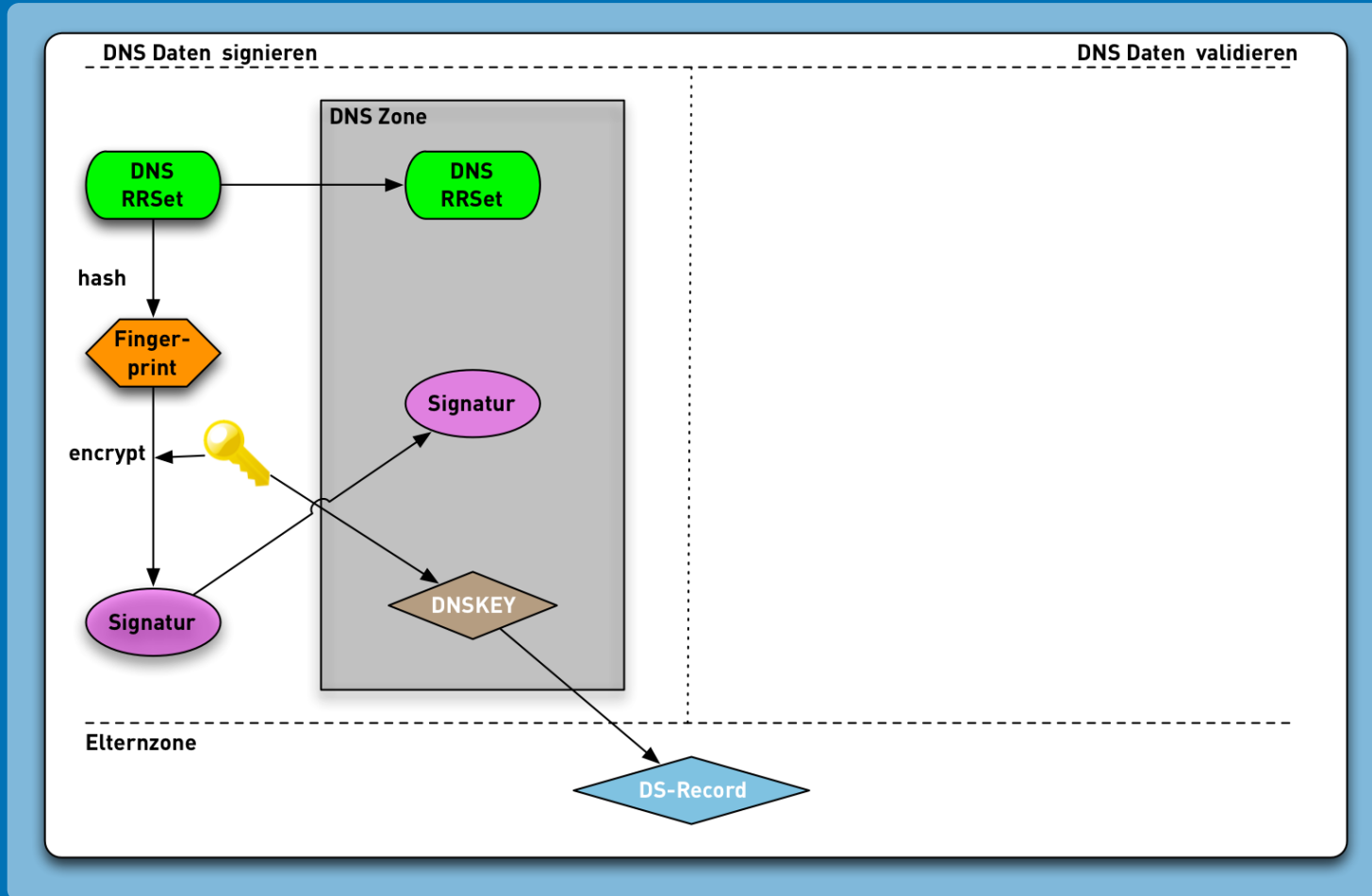
DNSSEC Validierung



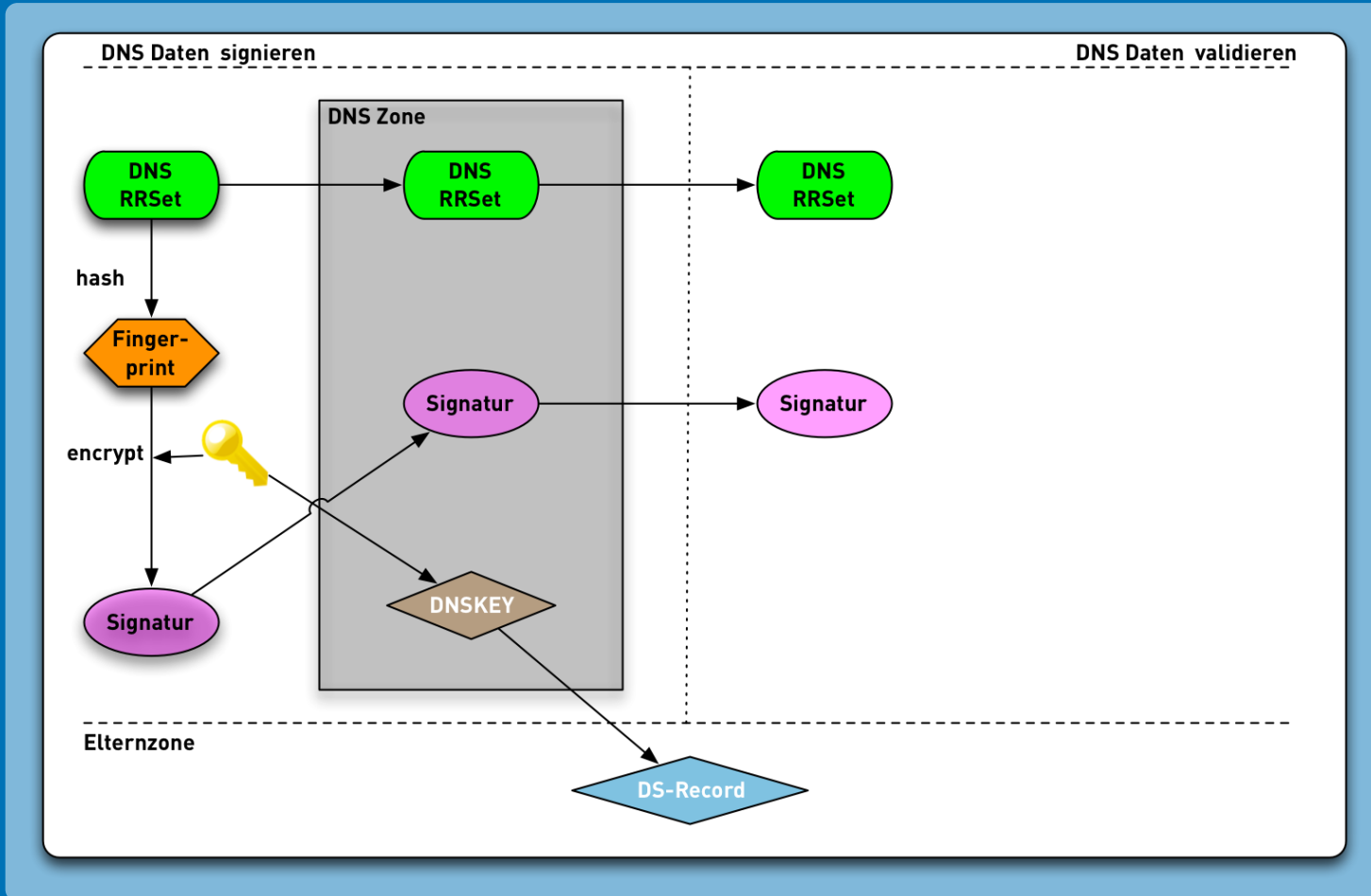
DNSSEC Validierung



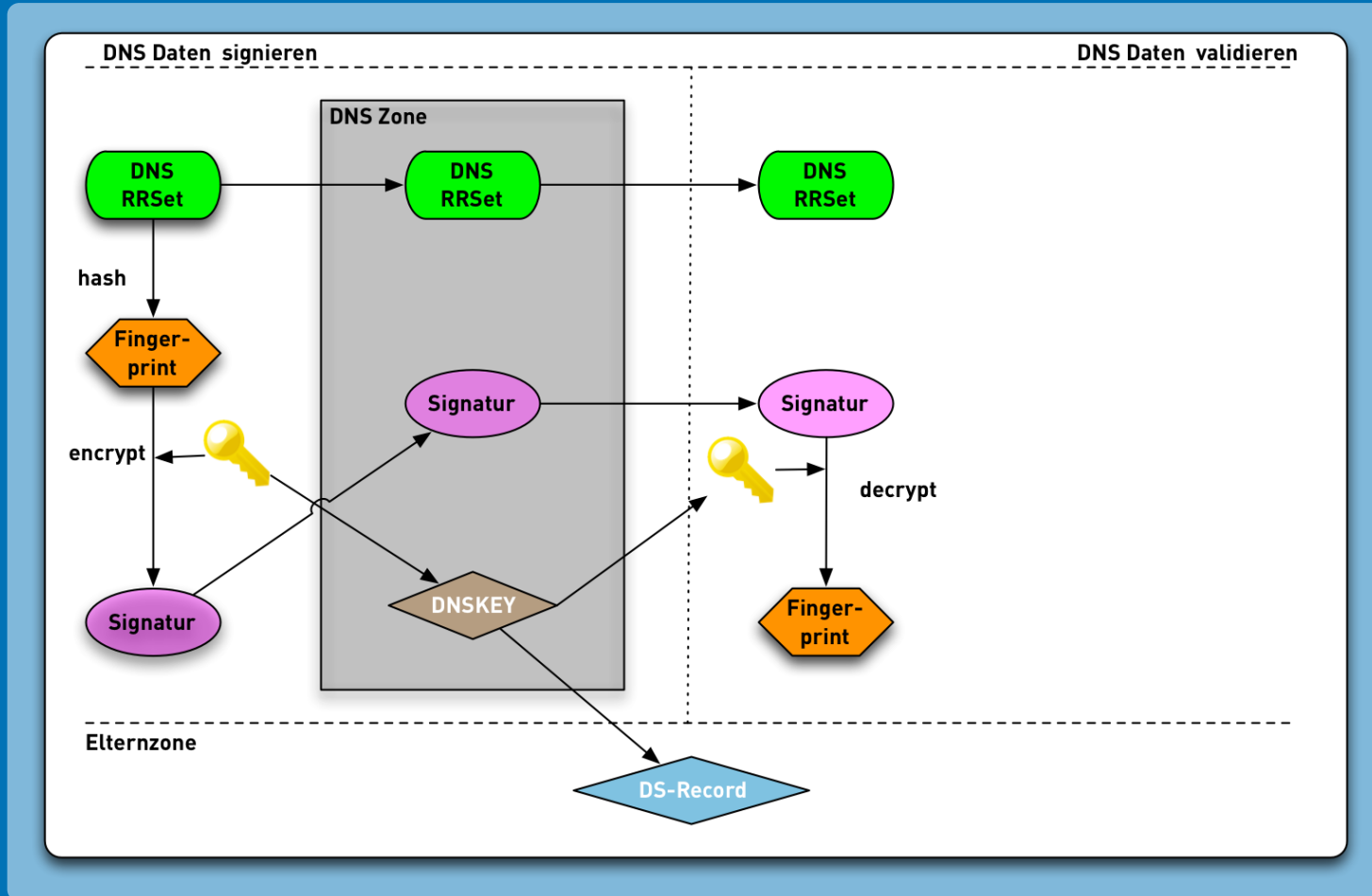
DNSSEC Validierung



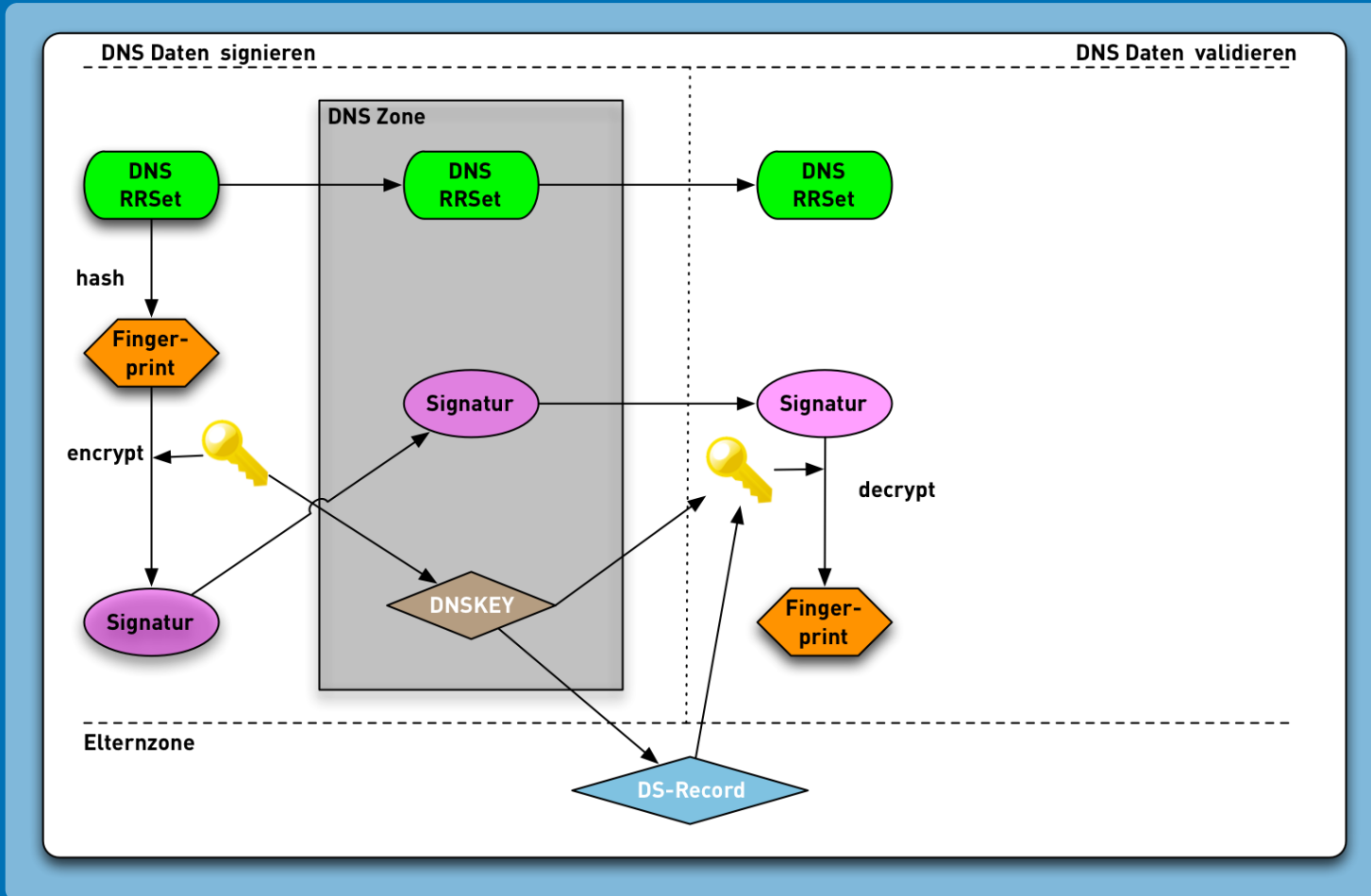
DNSSEC Validierung



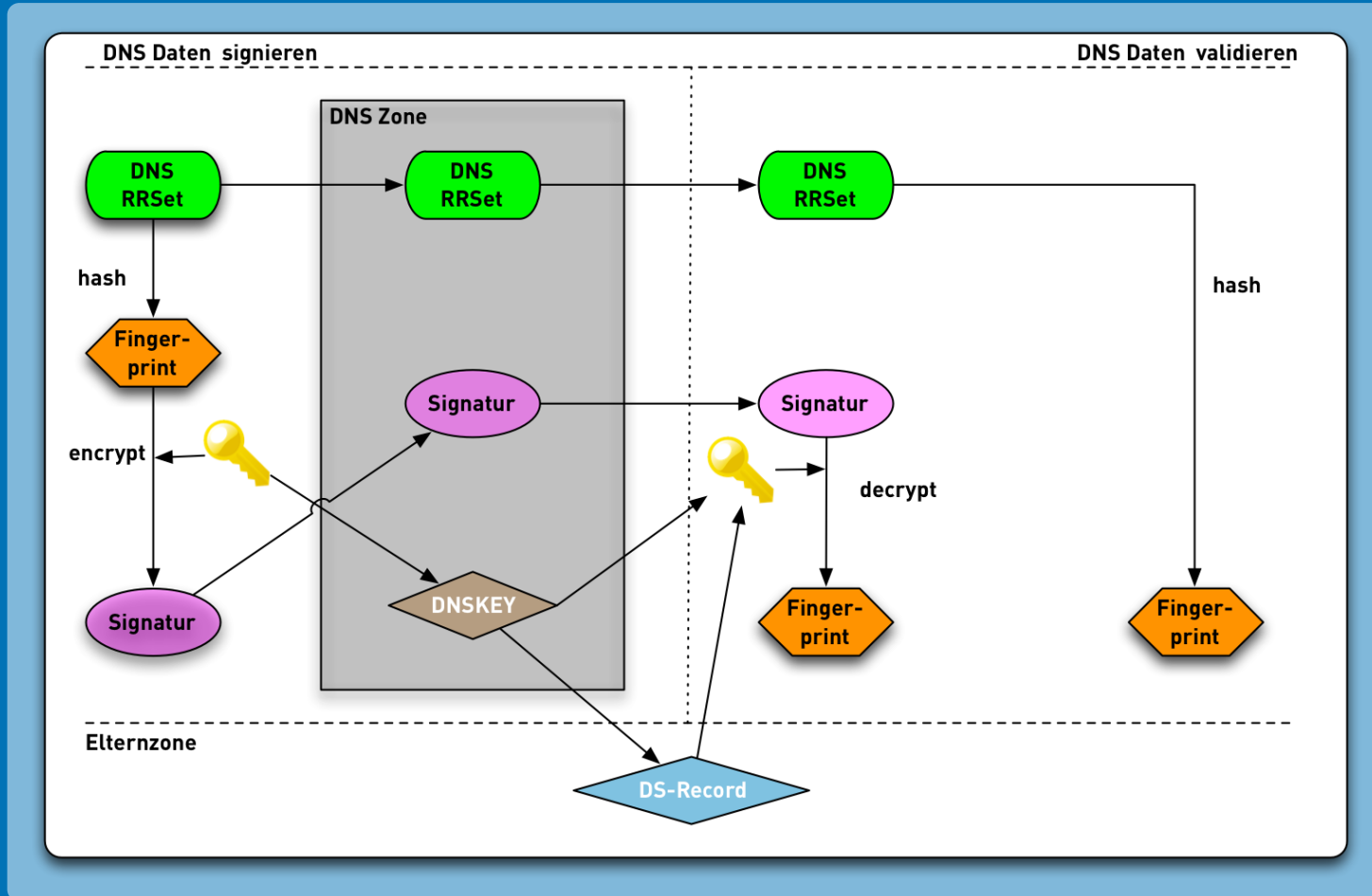
DNSSEC Validierung



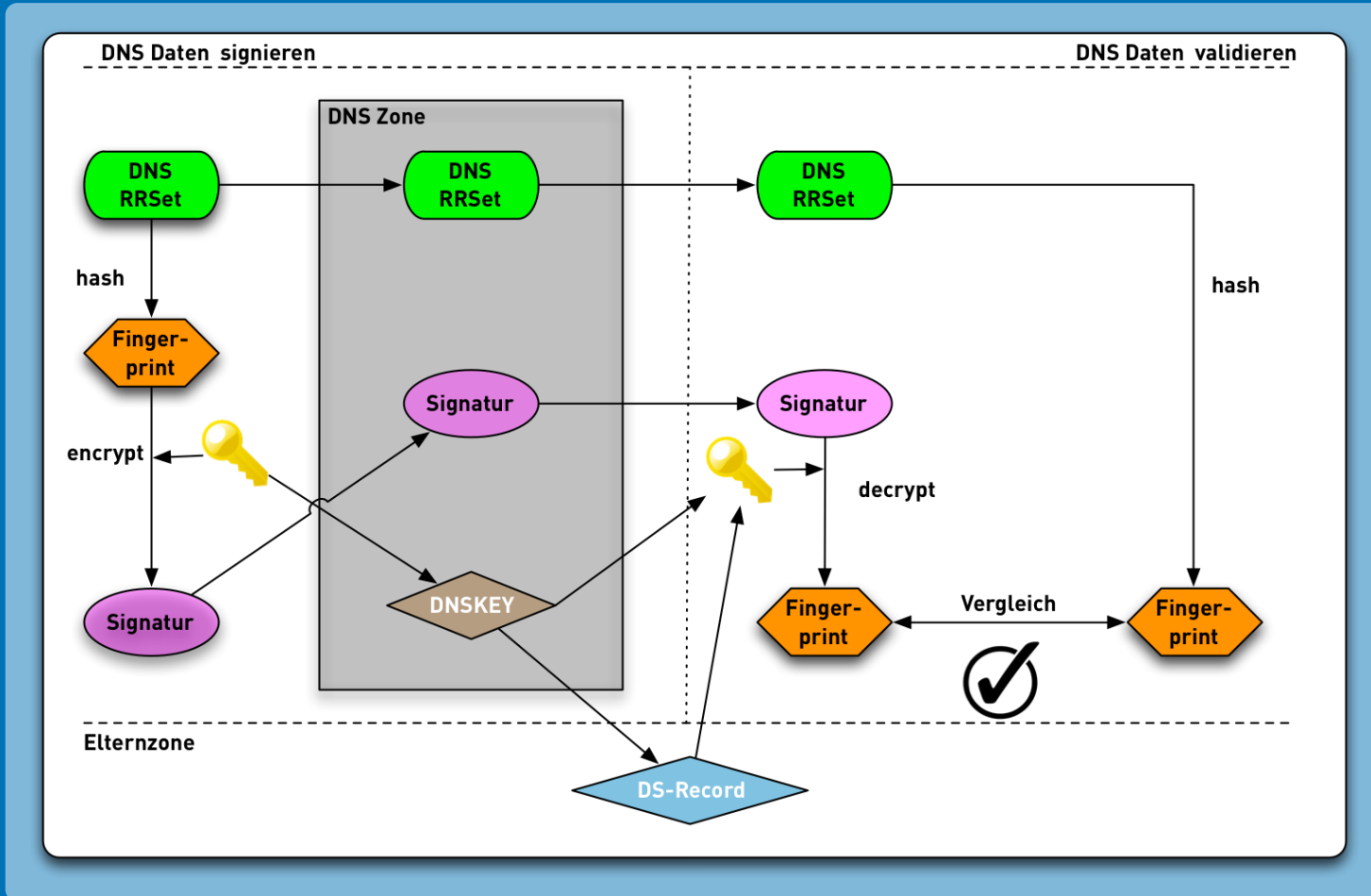
DNSSEC Validierung



DNSSEC Validierung



DNSSEC Validierung




DNSSEC Records

RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```




A blue callout box with a black border and rounded corners contains the text "Signierter RRSig Type". Two black arrows originate from the right side of this box and point to the "RRSIG" and "A" fields of the second DNS record in the list above.

**Signierter
RRSig Type**

RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```



RRSIG - Resource Record Signature

RRSIG-Record

Anzahl Label im
Domain Namen

```
www.sys4.de. 3600 IN A 194.126.152.154
www.sys4.de. 3600 IN RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```

RRSIG - Resource Record Signature

RRSIG-Record

Original
TimeToLive (TTL)

```
www.sys4.de.    3600 IN  A 194.126.158.174
www.sys4.de.    3600 IN  RRSIG A 8 3 3600 20151009061215 (
                20151002141517 57438 sys4.de.
                NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
                P5E58zluFwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
                QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
                H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```

RRSIG - Resource Record Signature

RRSIG-Record

www.sys4.de. 3600 IN A 194.126.158.154
www.sys4.de. 3600 IN RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY=)


Gültigkeitsende
der Signatur



RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEaM4M1ut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```




A blue rounded rectangle with the text "Gültigkeitsstart der Signatur" has an arrow pointing to the date "20151002141517" in the RRSIG record above.

**Gültigkeitsstart
der Signatur**

RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
20151002141517 57438 sys4.de.
NEAm4MIut1YZe2W5V6+QPO/JkQ1TIpqW9k421nw9rXey
P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```



A blue callout box with a black border contains the text "Key-ID/Key-Tag des Schlüssels". An arrow points from this box to the number "57438" in the RRSIG record, which is highlighted in green.

RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
                    20151002141517 57438 sys4.de.
                    NEaM4M1ut1YZe2W5V6+QP0kQ1TIpqW9k421nw9rXey
                    P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
                    QUtK3GhXh5R+RtfhkPPJR87cvRy60026p1/R8Bm5QX6P
                    H/Fn9EgueVnhJDn0bnyWzQv/YgdNVBf9vNoGidY= )
```

**Domain-Name
des öffentlichen
Schlüssels**

RRSIG - Resource Record Signature

RRSIG-Record

```
www.sys4.de.      3600 IN  A 194.126.158.154
www.sys4.de.      3600 IN  RRSIG A 8 3 3600 20151009061215 (
                    20151002141517 57438 sys4.de.
                    NEaM4M1ut1YZe2W5V6+QP0/JkQ1TIpqW9k421nw9rXey
                    P5E58zlufwS/+0iCR8IPx872023heK0fhk0B9gmH95FQ
                    QUtK3GhXh5R+RtfhkPP0R87cvRy60026p1/R8Bm5QX6P
                    H/Fn9EgueVnhJDn0bmyWzQv/YgdNVBf9vNoGidY= )
```



**Signatur
(Base64)**

DNSKEY - DNSSEC Schlüssel

DNSKEY-Record

sys4.de. 3600 IN DNSKEY 256 3 8 (
AwEAAAdZFu5qBo0tXH2VNlsxjKyrp+lsc/wyyw2Cn7guV
7RMe4D1X/vU/dvF4Zy2yyv98ZHscBwqBRMbspr33fu28
n27dEZrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg
ThYt2Y54H607wuUP2ulhJjz2aQfmTbENLNL18gt8zIOP
) ; key id = 57438

Flags
256 = ZSK
257 = KSK

DNSKEY - DNSSEC Schlüssel

DNSKEY-Record

sys4.de. 3600 IN DNSKEY 256 3 8 (
AwEAAAdZFu5qBo0tXH2VNlsxjKyrp+lsc/wyyw2Cn7guV
/RMe4D1X/vU/dvF4Zy2yyv98ZHscBwqBRMbspr33fu28
n27dEZrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg
ThYt2Y54H607wuUP2ulhJjz2aQfmTbENLNL18gt8zIOP
) ; key id = 57438

**Protokoll
3 = DNSSEC**

DNSKEY - DNSSEC Schlüssel

DNSKEY-Record

sys4.de. 3600 IN DNSKEY 256 3 8 (
AwEAAAdZFu5qBoOtXH2VNlsxjKyrp+lsc/wyyw2Cn7guV
7RMe4D1X/vU/dvF4Zy2yyv98ZHscBwqBRMbspr33fu28
n27dEZrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg
ThYt2Y54H607wuUP2ulhJjz2aQfmTbENLNL18gt8zIOP
) ; key id = 57438

**Schlüssel
Algorithmus**

DNSKEY - DNSSEC Schlüssel

DNSKEY-Record

```
sys4.de.      3600 IN  DNSKEY 256 3 8 (  
  AwEAdZFu5qBo0tXH2VNlsxjKyrp+lsc/wyyw2Cn7guV  
  7RMe4D1X/vU/dvF4Zy2yyv98ZHscBwqBRMbspr33fu28  
  n27dEZrFBHHAVCRE3BzrsL8o/L/eU57xDF9q6avRxGmg  
  ThYt2Y54H607wuUP2ulhJjz2aQfmTbENLNL18gt8zIOP  
  ) ; key id = 57438
```

**Schlüssel
(Base 64)**



DS - Delegation Signer Record

DS-Record

sys4.de. 86400 IN DS 47579 8 2 (
47D772EA1CE9CFBFB1A38BE335372F44C28878C93BF0
70E2855F7659DA935887)

**KSK Key-ID in
der delegierten
Zone**

A blue rounded rectangular callout box with a black border contains the text 'KSK Key-ID in der delegierten Zone'. A black arrow originates from the top-right corner of this box and points to the green-highlighted number '47579' in the DS record text above.

DS - Delegation Signer Record

DS-Record

sys4.de. 86400 IN DS 47579 8 2 (
47D7722A1CE9CFBFB1A38BE335372F44C28878C93BF0
70E2855F7659DA935887)

Algorithmus des
KSK Schlüssel

A blue rounded rectangular callout box with a black border contains the text "Algorithmus des KSK Schlüssel". Two black lines extend from the top-right corner of the box, converging into an arrow that points directly at the green-highlighted number "8" in the DS record text above.

DS - Delegation Signer Record

DS-Record

sys4.de. 86400 IN DS 47579 8 2 (47D772EA1CE90FBFB1A38BE335372F44C28878C93BF0 70E2855F7659DA935887)

Hashing-
Algorithmus
(2= SHA256)

DS - Delegation Signer Record

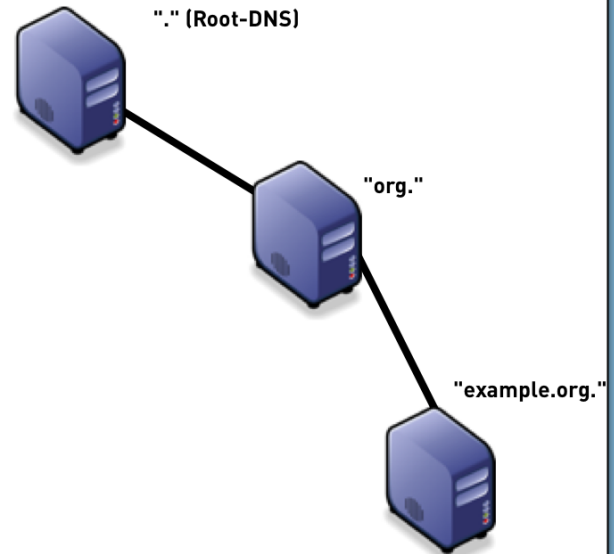
DS-Record

sys4.de. 86400 IN DS 47579 8 2 (47D772EA1CE9CFBFB1A38BE335372F44C28878C93BF0 70E2855F7659DA935887)

Hash des KSK
der delegierten
Zone

A blue rounded rectangular box with a black border contains the text 'Hash des KSK der delegierten Zone'. A black arrow points from the top of this box to the green highlighted hash portion of the DS record text above it.

DNSSEC Validierung (vereinfacht)

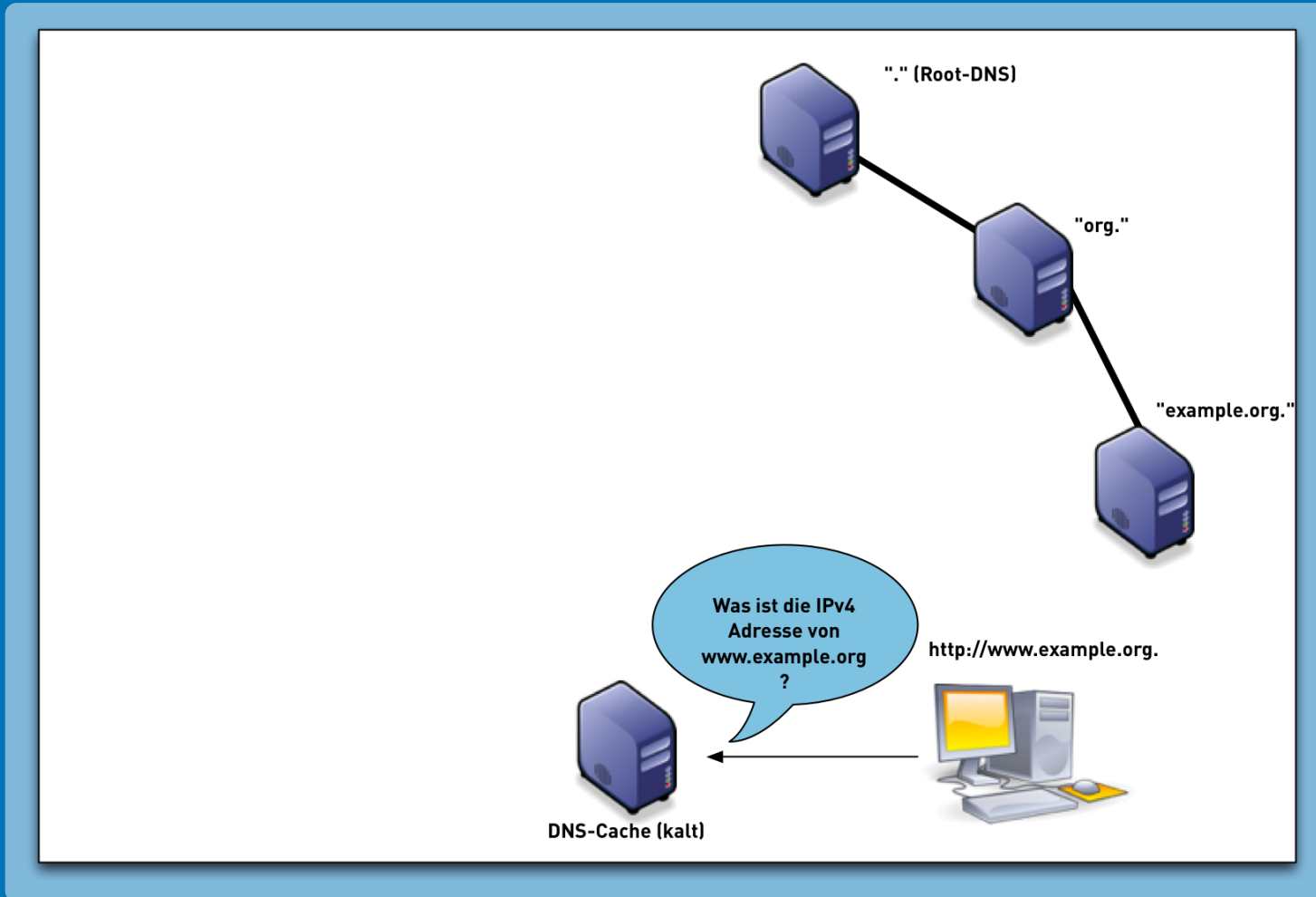


DNS-Cache (kalt)

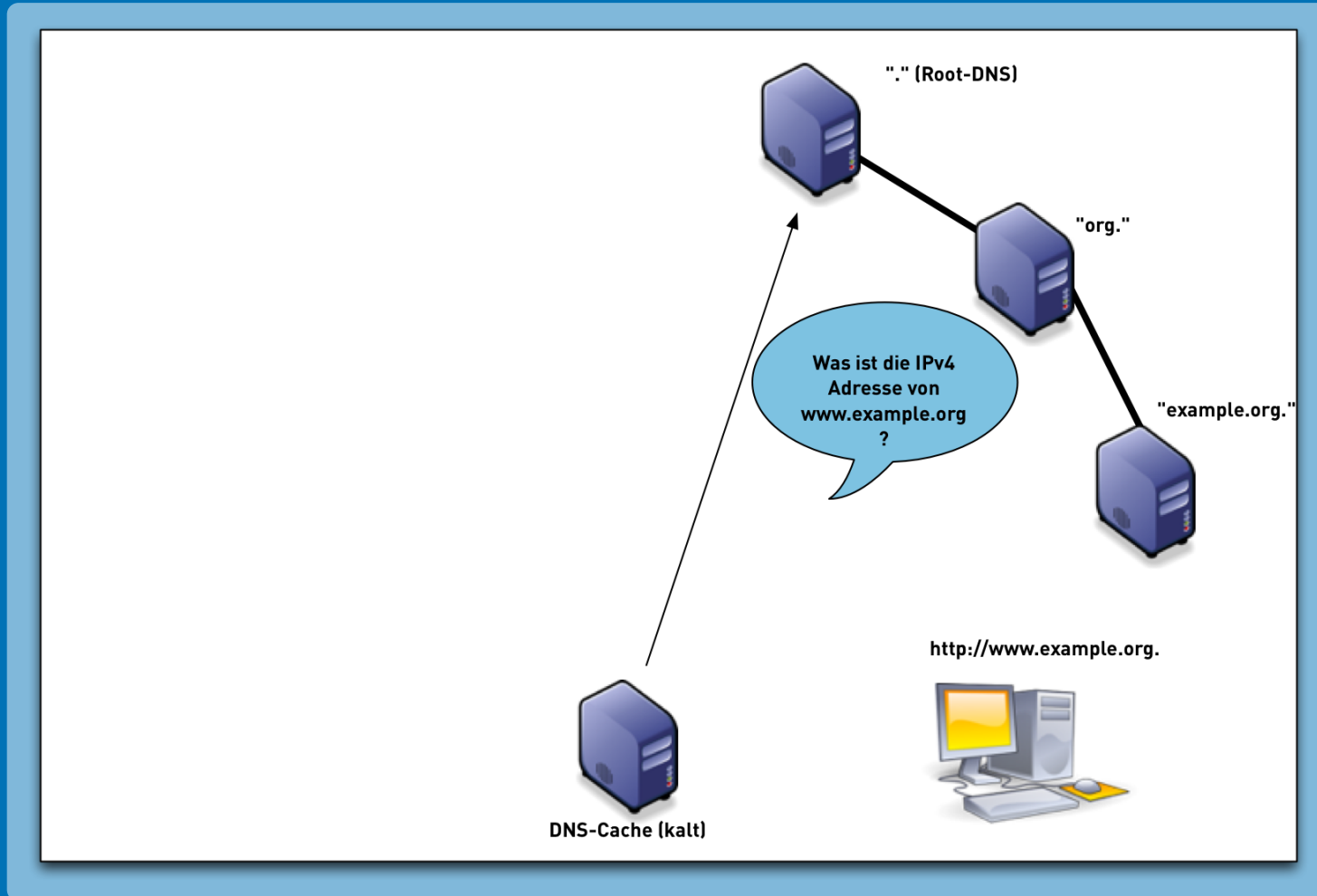
<http://www.example.org>.



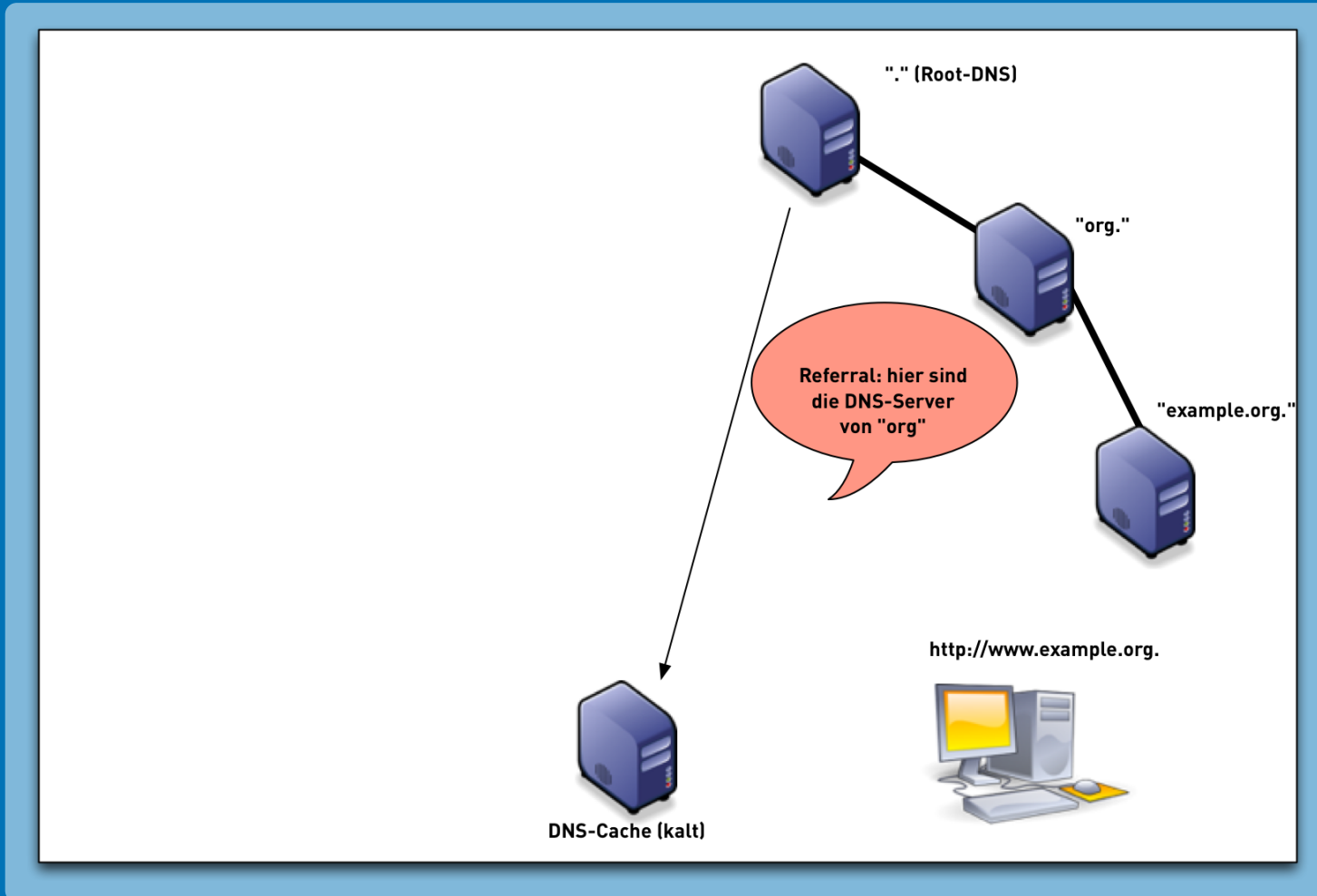
DNSSEC-Validierung (vereinfacht)



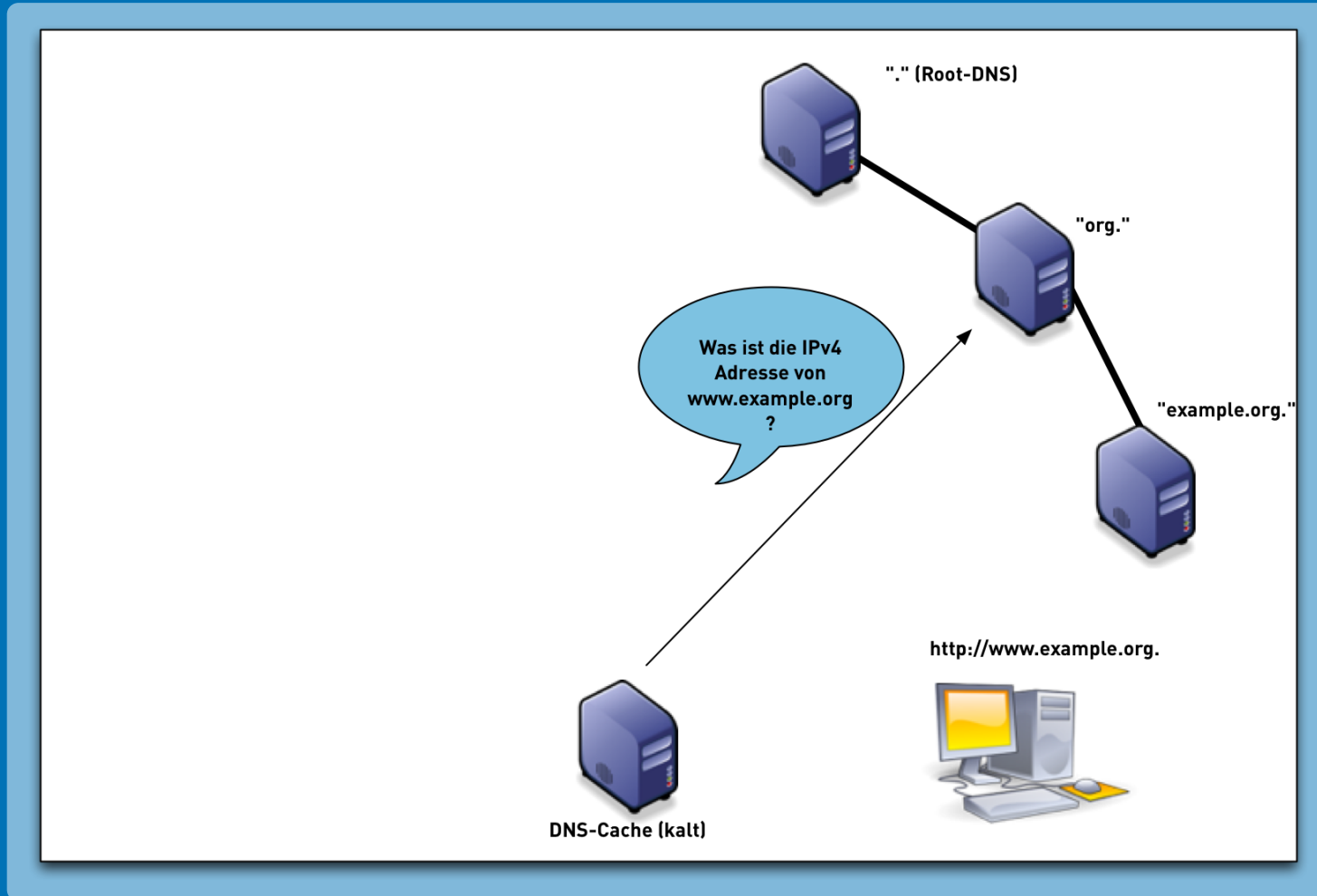
DNSSEC-Validierung (vereinfacht)



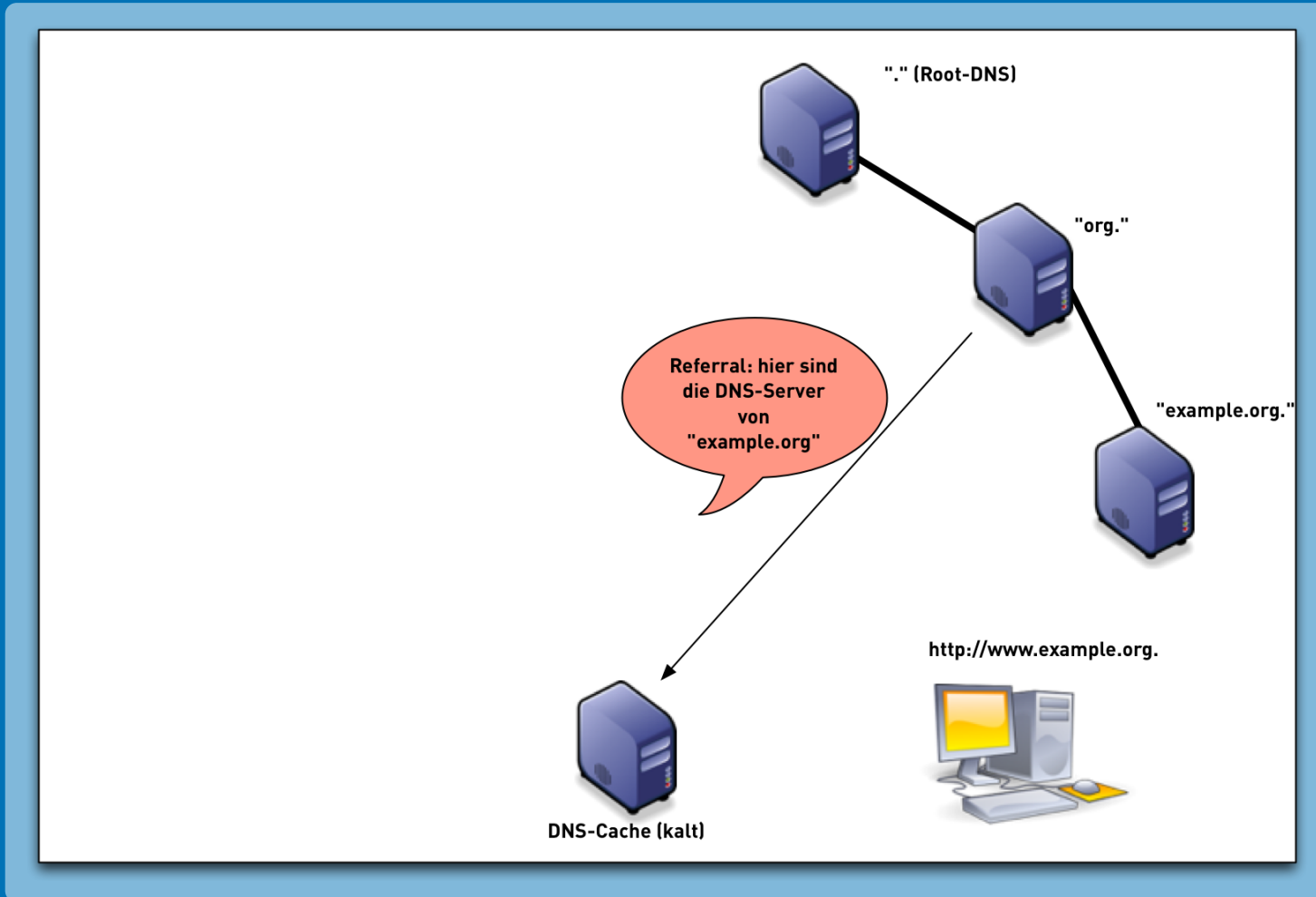
DNSSEC-Validierung (vereinfacht)



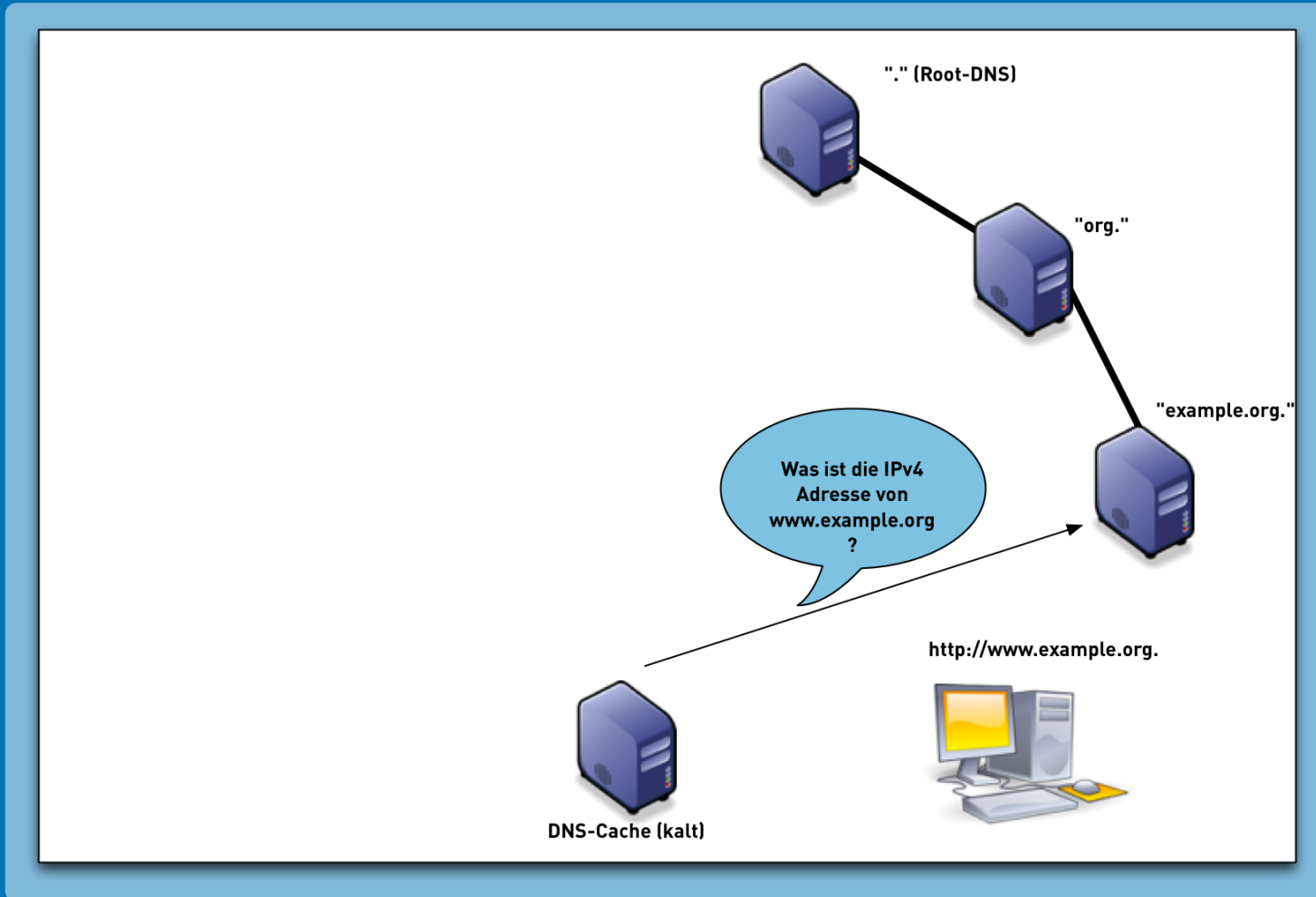
DNSSEC-Validierung (vereinfacht)



DNSSEC-Validierung (vereinfacht)

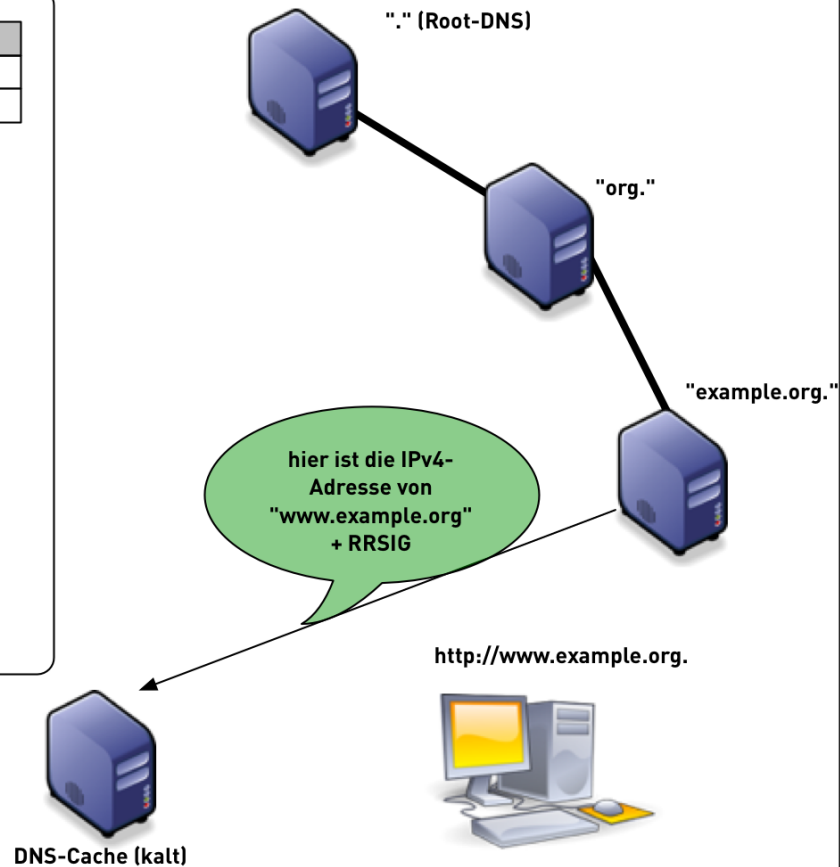


DNSSEC-Validierung (vereinfacht)



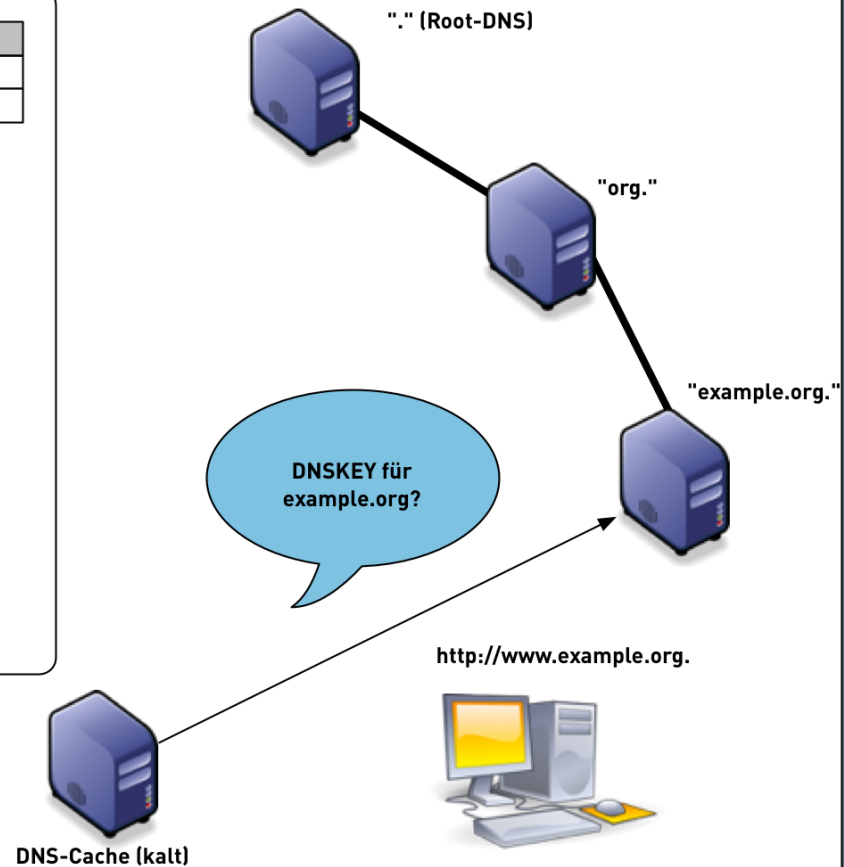
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑



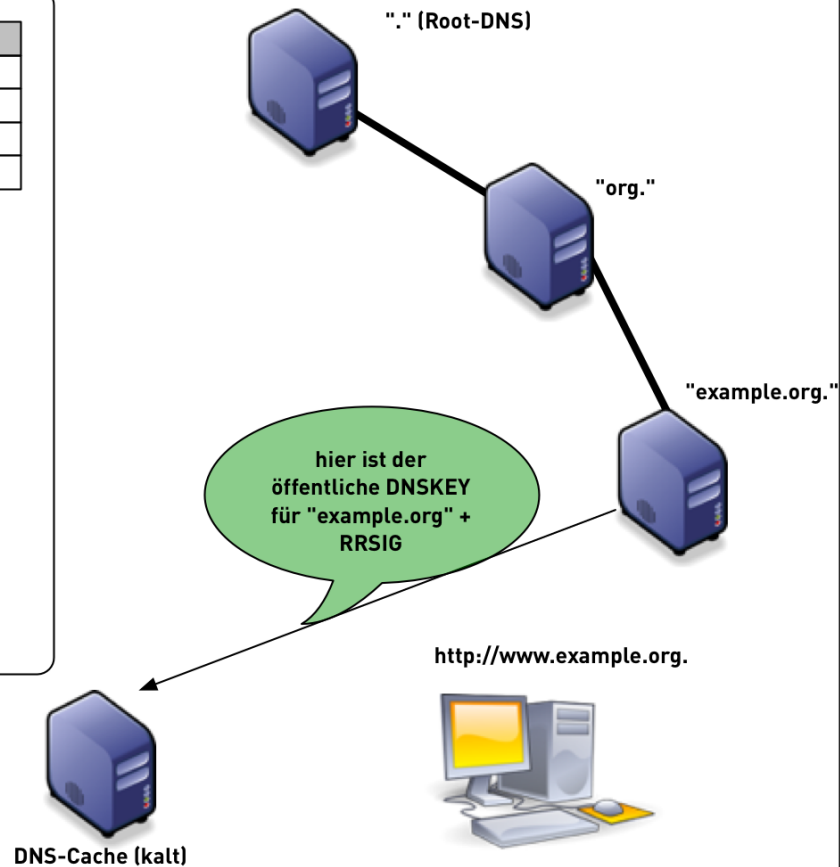
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑



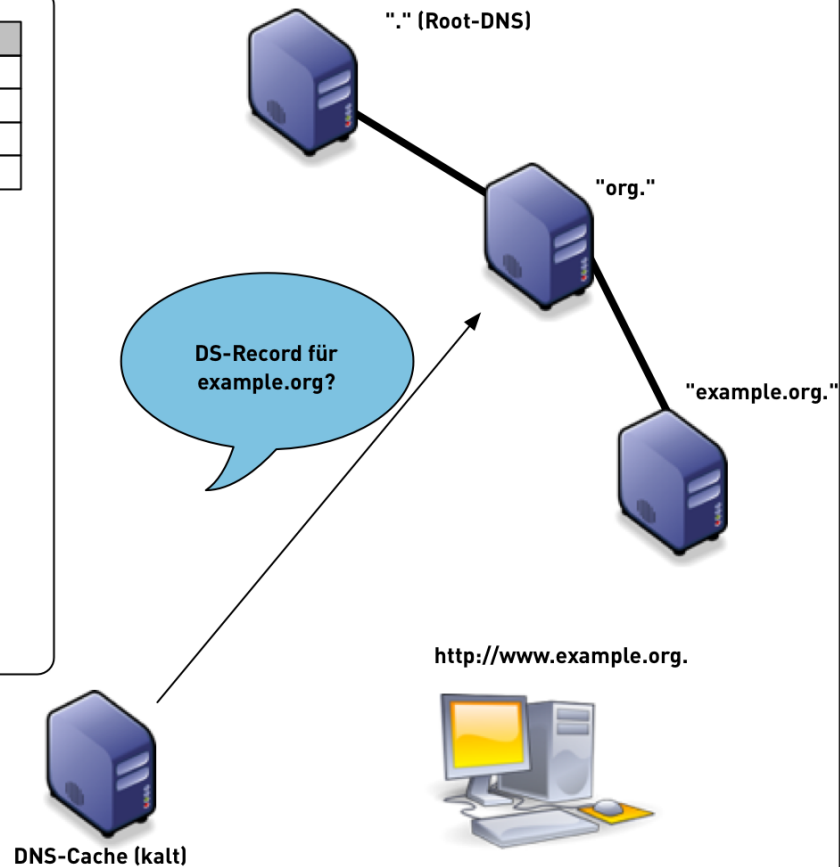
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑



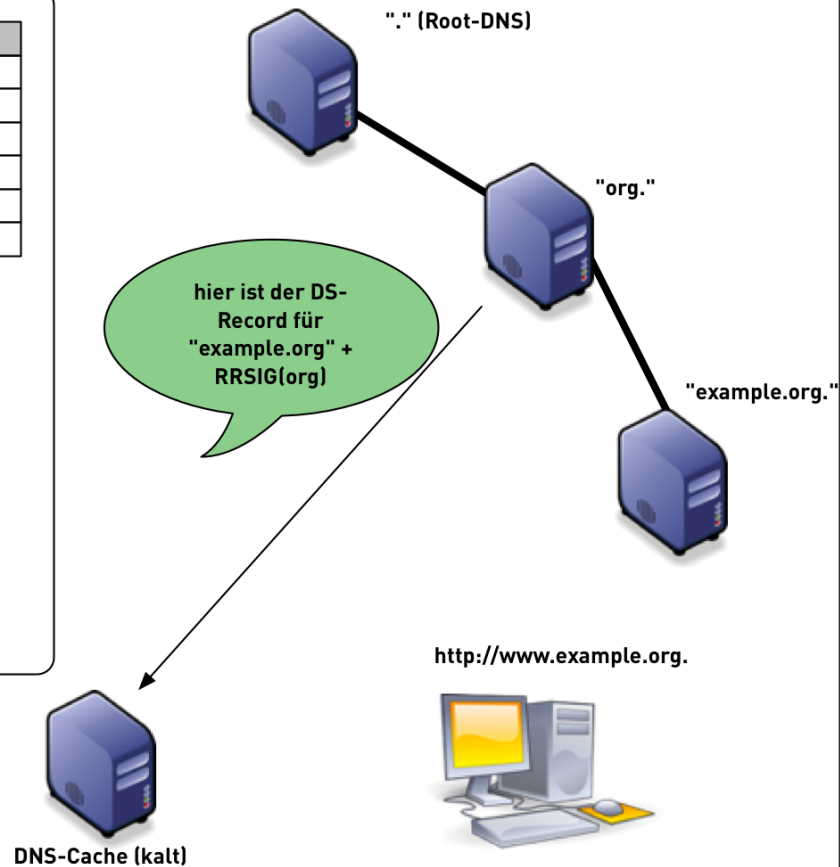
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑



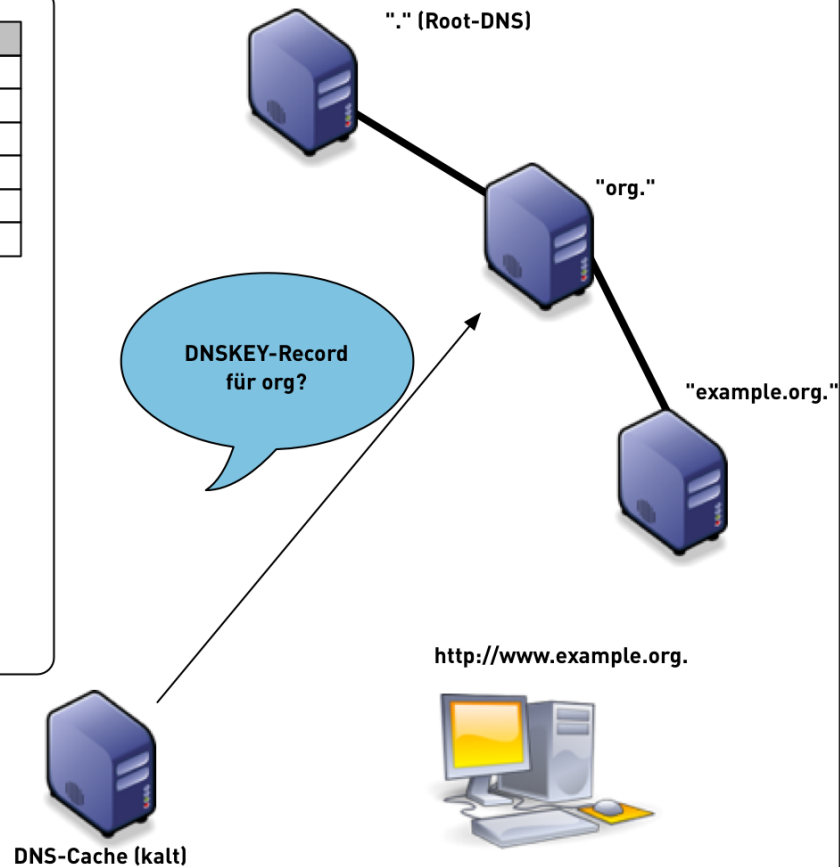
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑



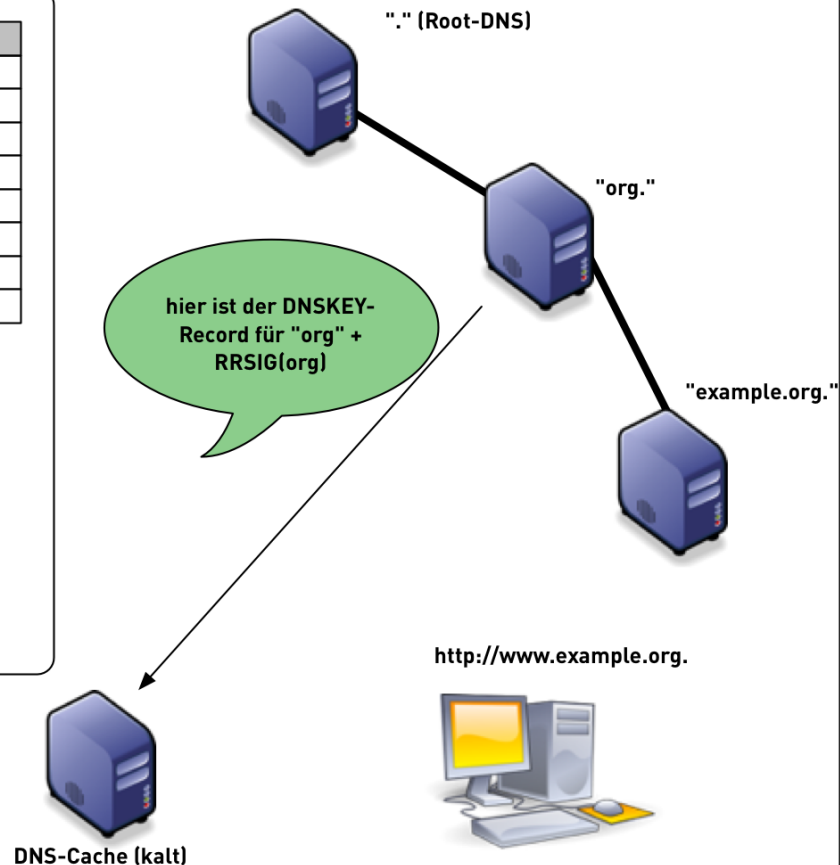
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑



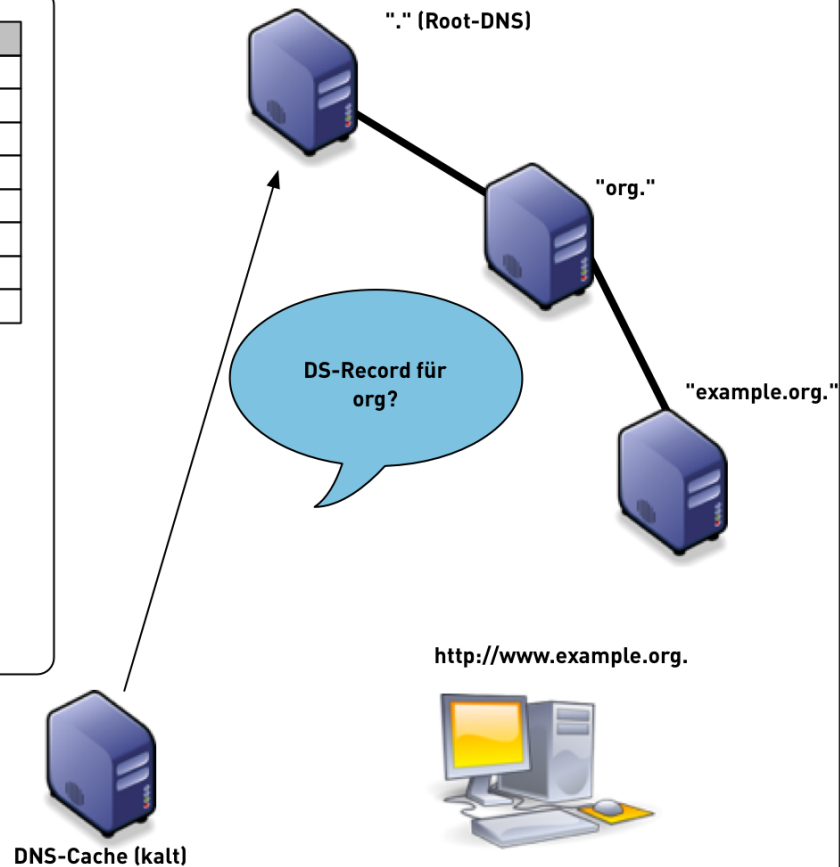
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑



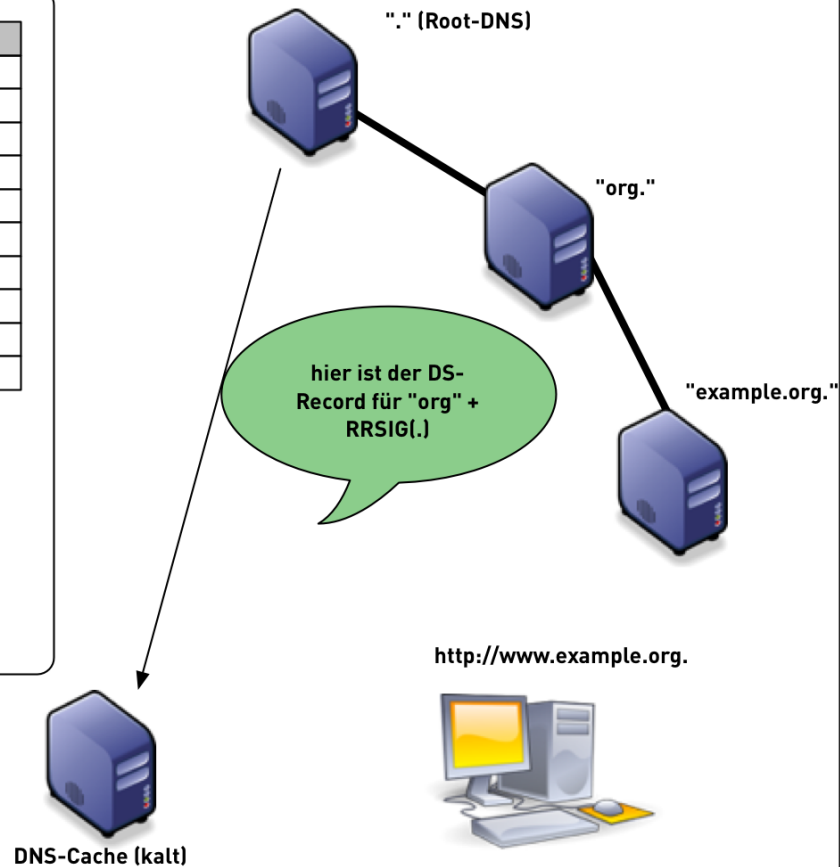
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑



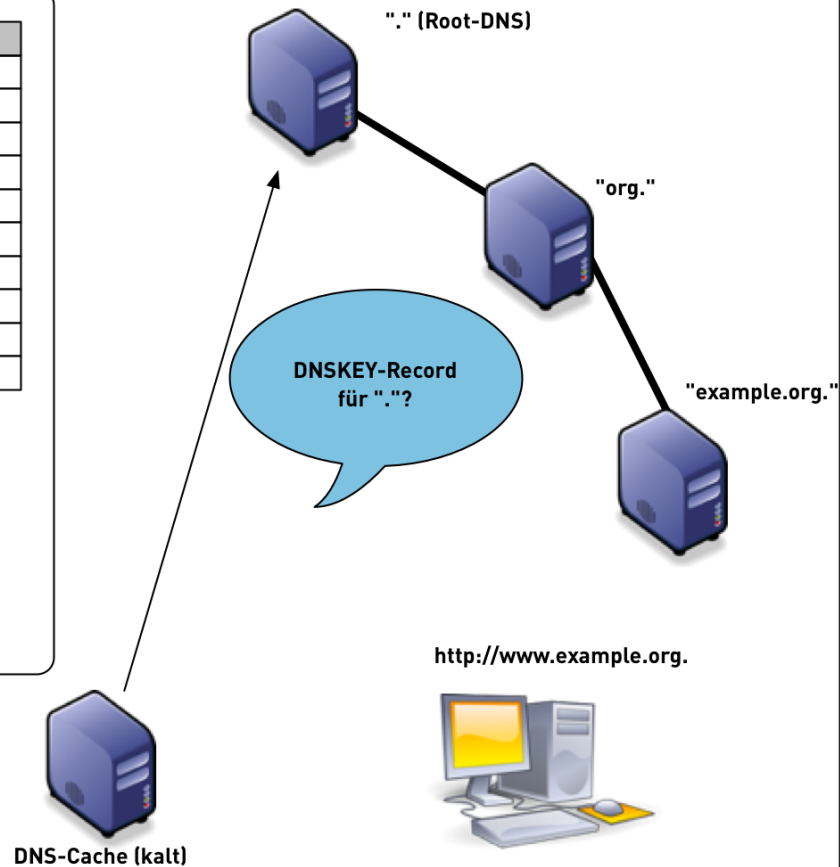
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑
org DS	Hash des KSK
. RRSIG	Signatur ↑



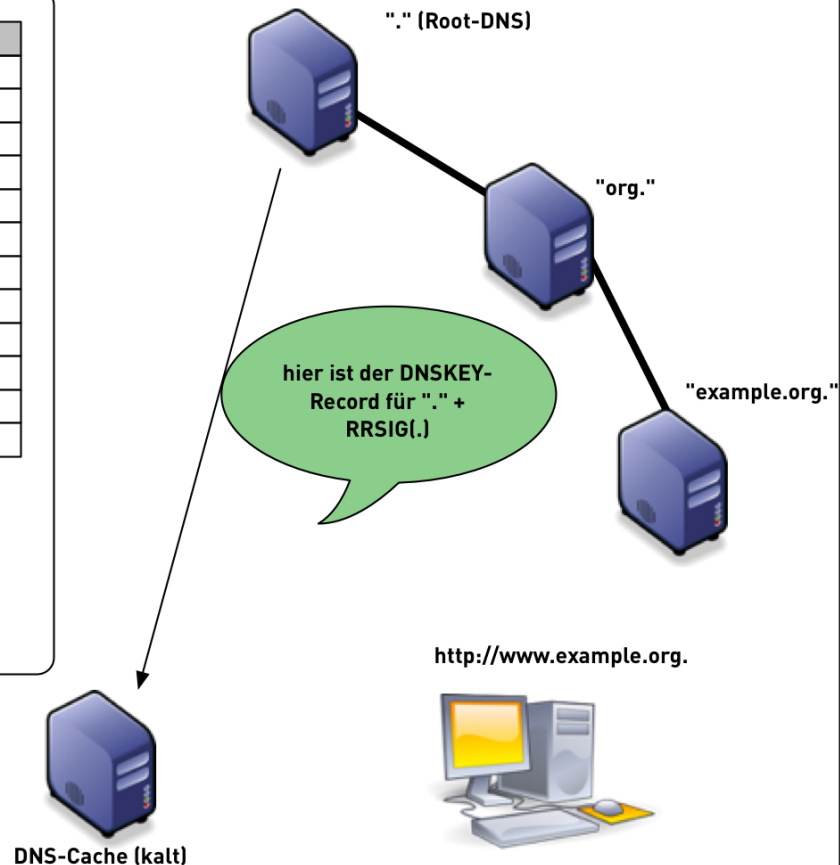
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑
org DS	Hash des KSK
. RRSIG	Signatur ↑



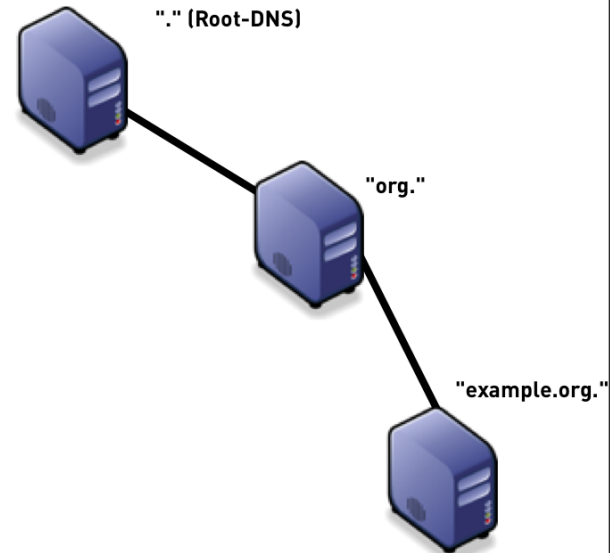
DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑
org DS	Hash des KSK
. RRSIG	Signatur ↑
. DNSKEY	öffentlicher Schlüssel
. RRSIG	Signatur ↑

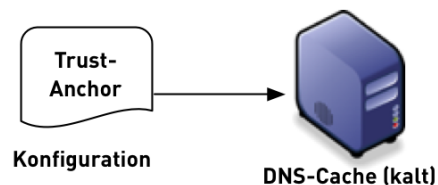


DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑
org DS	Hash des KSK
. RRSIG	Signatur ↑
. DNSKEY	öffentlicher Schlüssel
. RRSIG	Signatur ↑
Trust-Anchor for "."	(Hash of) Public-Key

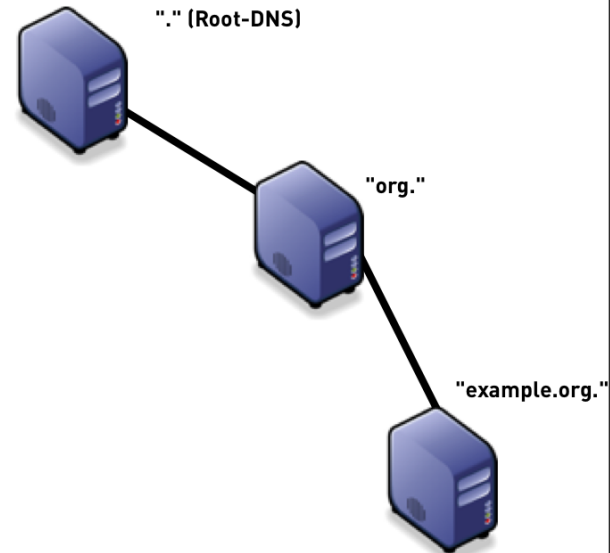


<http://www.example.org>.



DNSSEC-Validierung (vereinfacht)

Record	Funktion	
www.example.org A	IPv4-Adresse	✓
www.example.org RRSIG	Signatur ↑	✓
example.org DNSKEY	öffentlicher Schlüssel	✓
example.org RRSIG	Signatur ↑	✓
example.org DS	Hash des KSK	✓
org RRSIG	Signatur ↑	✓
org DNSKEY	öffentlicher Schlüssel	✓
org RRSIG	Signatur ↑	✓
org DS	Hash des KSK	✓
. RRSIG	Signatur ↑	✓
. DNSKEY	öffentlicher Schlüssel	✓
. RRSIG	Signatur ↑	✓
Trust-Anchor for "."	(Hash of) Public-Key	✓



<http://www.example.org>.

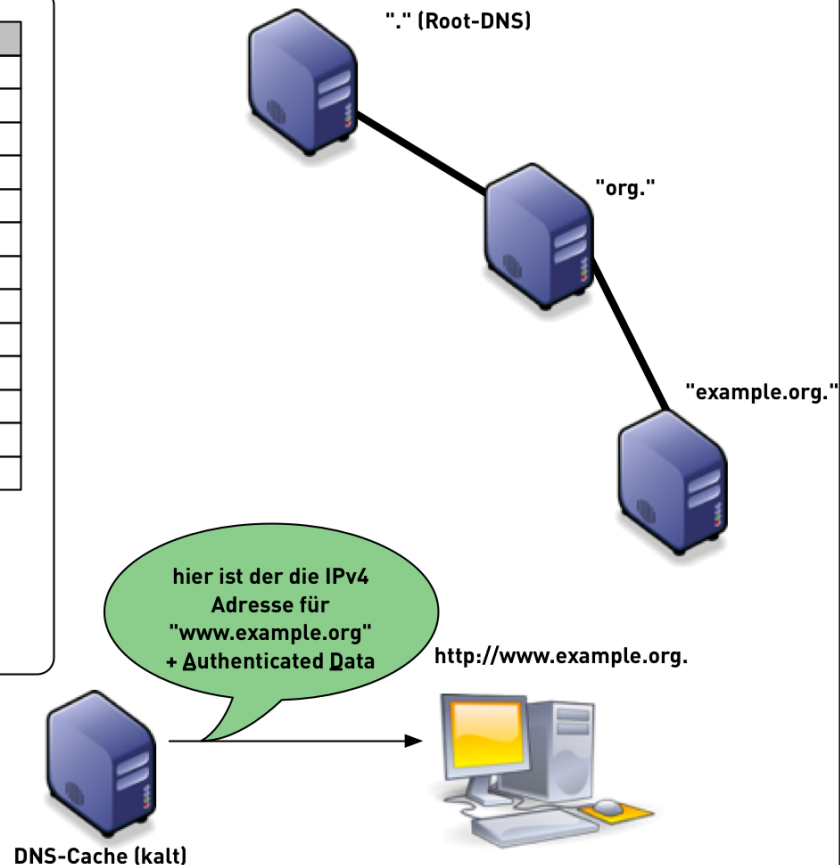


DNS-Cache (kalt)



DNSSEC-Validierung (vereinfacht)

Record	Funktion
www.example.org A	IPv4-Adresse
www.example.org RRSIG	Signatur ↑
example.org DNSKEY	öffentlicher Schlüssel
example.org RRSIG	Signatur ↑
example.org DS	Hash des KSK
org RRSIG	Signatur ↑
org DNSKEY	öffentlicher Schlüssel
org RRSIG	Signatur ↑
org DS	Hash des KSK
. RRSIG	Signatur ↑
. DNSKEY	öffentlicher Schlüssel
. RRSIG	Signatur ↑
Trust-Anchor for "."	(Hash of) Public-Key



Fragen?
