DNSSEC

Domain Name System Security Extension

Referent:
Matthias Lohr <lohr@uni-trier.de>

DNS - Geschichte

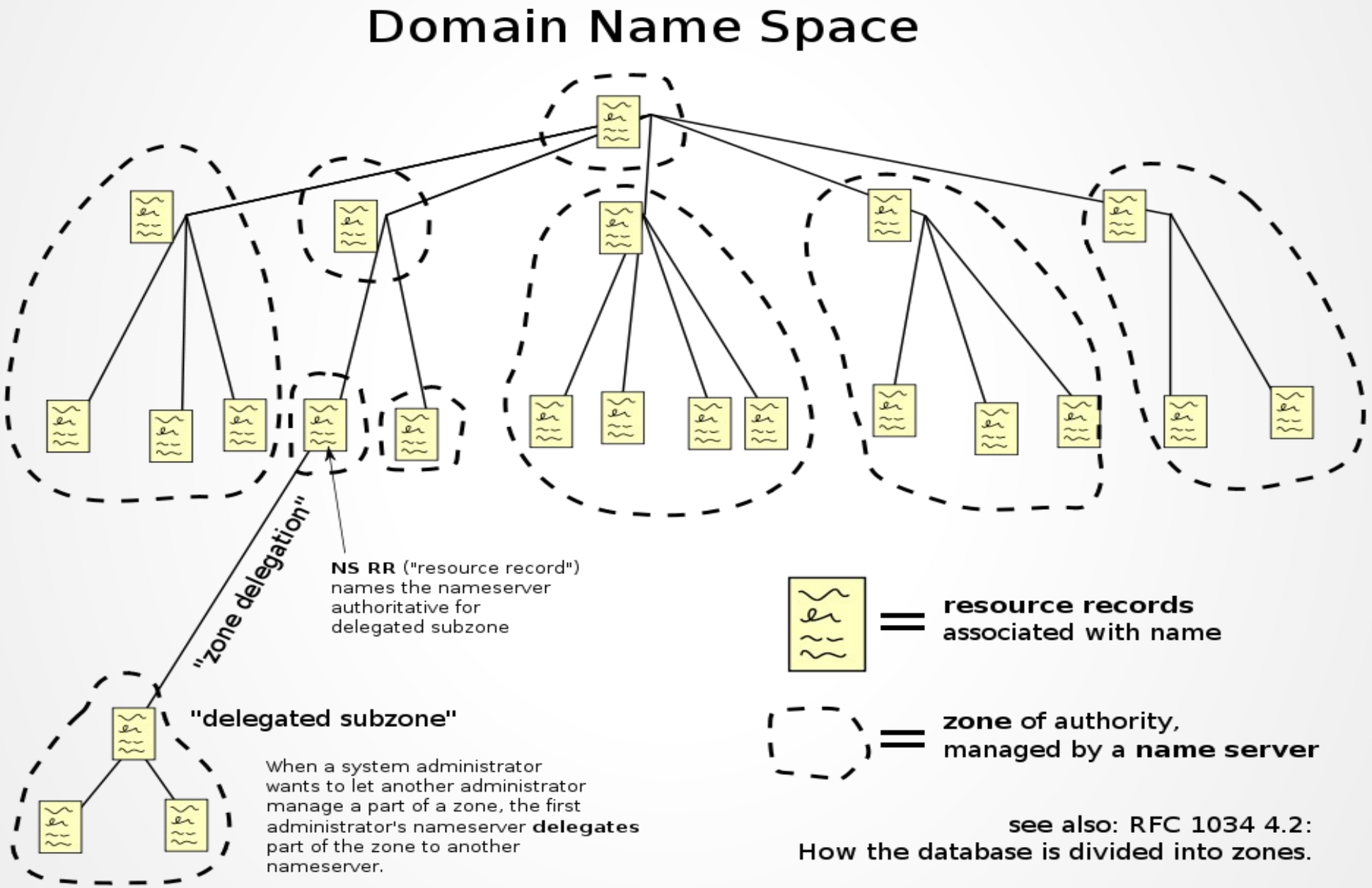
- Früher:
  - Master-Text-Datei
  - Abgleich über Download
- Jetzt:
  - Verteilte Datenbank
  - Abgleich über sog. Zonentransfers (AXFR)

DNS - Funktionsweise

- Aufteilung in Zonen

  de → uni-trier.de → syssoft.uni-trier.de
- Records speichern Informationen
  - Verschiedene Typen:
    - A: IPv4-Adresse
    - AAAA: IPv6-Adresse
    - MX: Zuständiger Mailserver
    - CNAME: Alias auf anderen Namen
    - …
- Zonen können an andere Nameserver delegiert werden (Zuständigkeit abgeben)

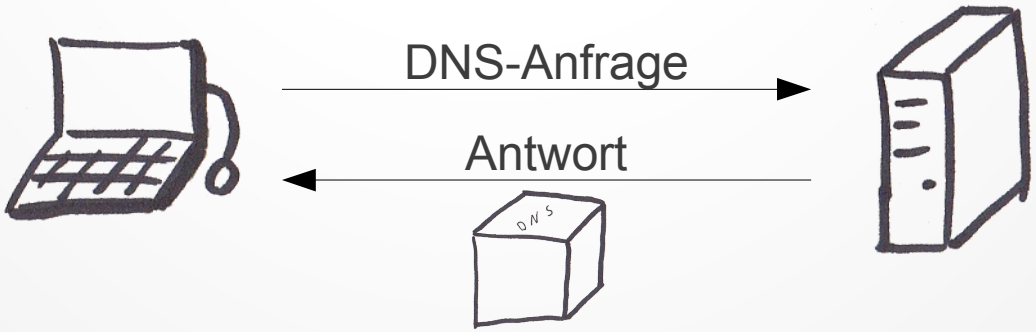
DNS - Funktionsweise



Quelle: http://en.wikipedia.org/wiki/File:Domain_name_space.svg

DNS - Sicherheit

- Keine Verschlüsselung
  - → Daten offen lesbar
- Keine Signierung
  - → Fälschungen möglich
- Bekannte Angriffsszenarien:
  - (D)DoS
  - DNS Rebinding
  - DNS Amplification Attack
  - Cache Poisoning (Fälschungen)

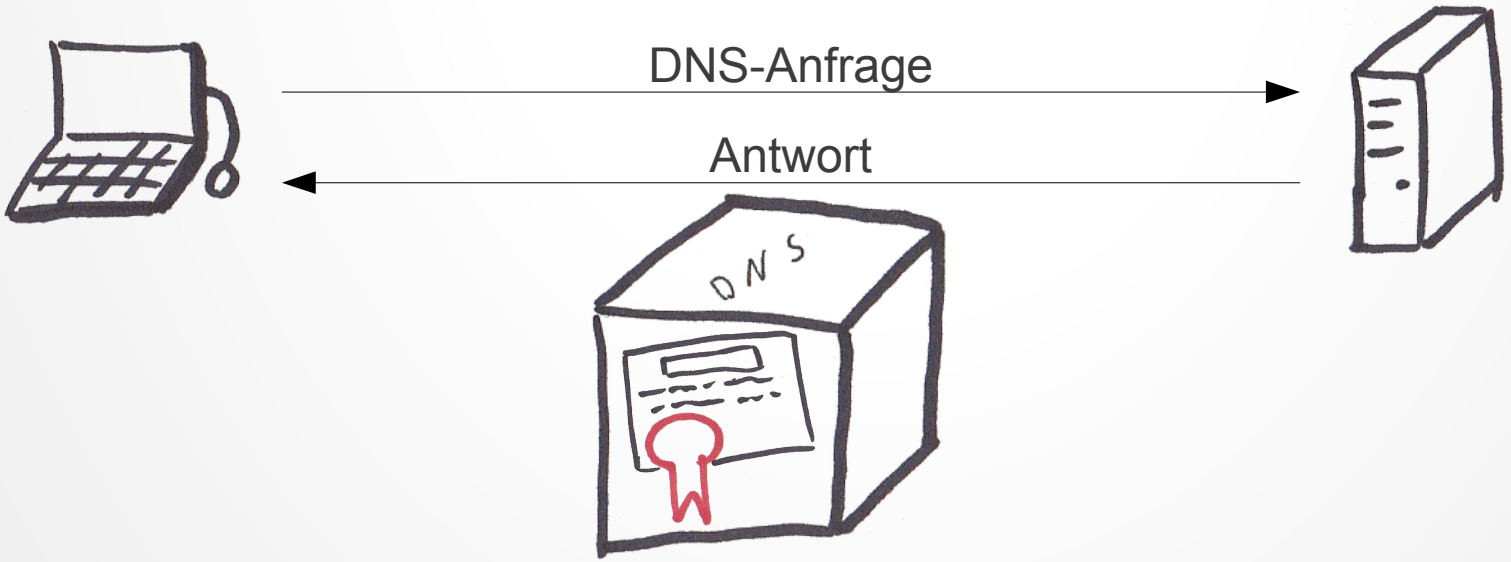


DNSSEC

- DNSSEC verhindert Fälschungen
  - Unterschrift der Daten mit digitaler Signatur
  - Automatische Überprüfung der Signatur

DNSSEC – Signatur

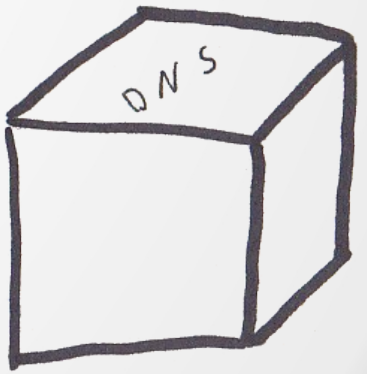
- Client schickt Anfrage
- Server antwortet mit angefordertem Record
- Server fügt RRSIG-Record hinzu



DNSSEC – Signatur – Beispiel

- ohne DNSSEC:

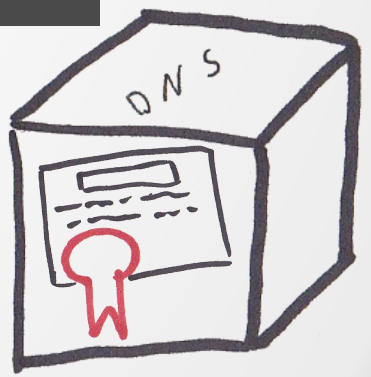
```
$ dig -t A www.bund.de

; <<>> DiG 9.8.1-P1 <<>> -t A www.bund.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19122
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bund.de.                  IN   A

;; ANSWER SECTION:
www.bund.de.     8653 IN   A    77.87.229.48
```



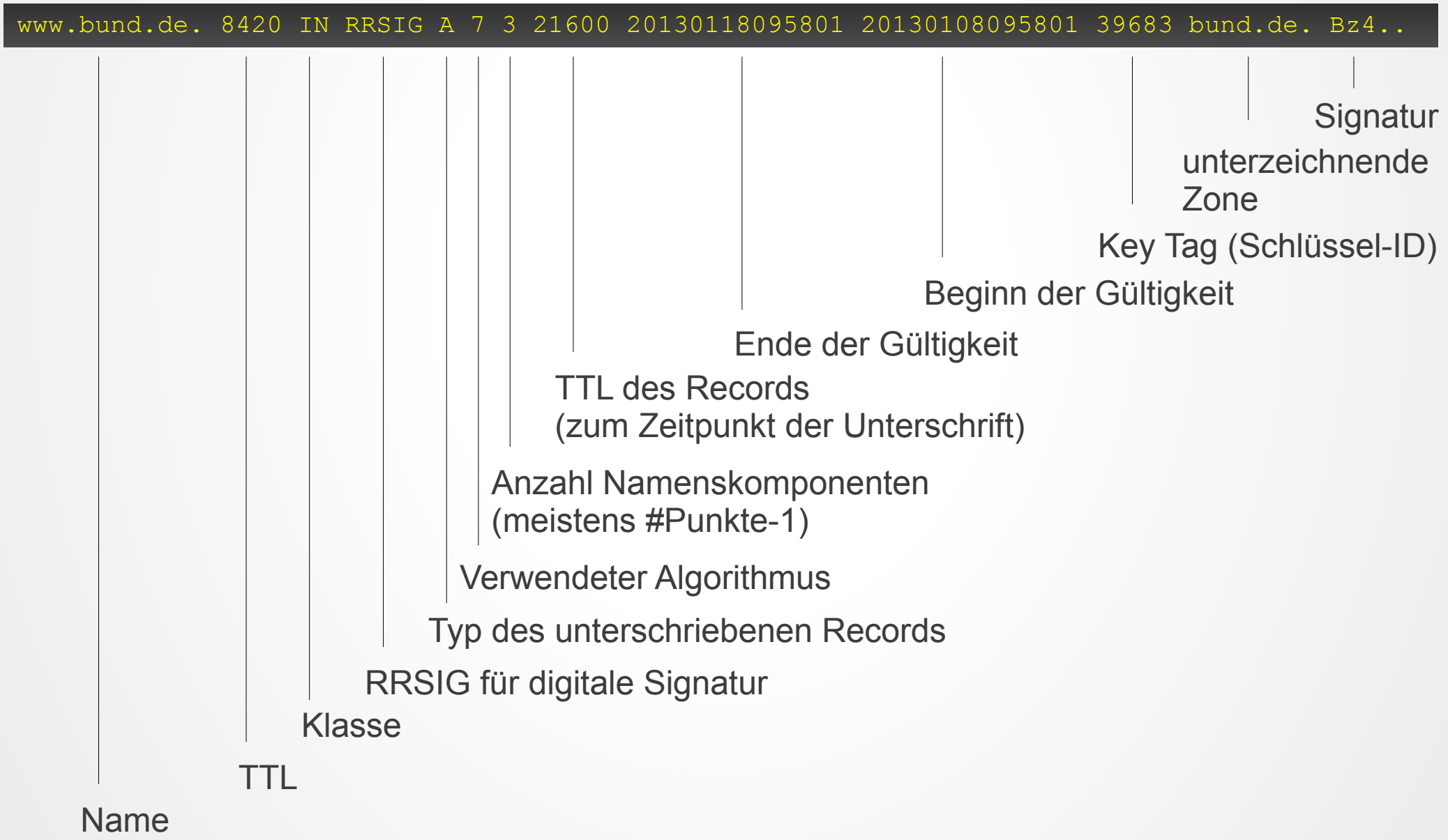
DNSSEC – Signatur – Beispiel

- mit DNSSEC:

```
$ dig +dnssec -t A www.bund.de

; <<>> DiG 9.8.1-P1 <<>> +dnssec -t A www.bund.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8866
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 7eba , udp: 1460
;; QUESTION SECTION:
;www.bund.de.                   IN   A

;; ANSWER SECTION:
www.bund.de.      8420 IN   A    77.87.229.48
www.bund.de.      8420 IN   RRSIG    A 7 3 21600 20130118095801
20130108095801 39683 bund.de.
Bz4M1BG2iO21Tu5vJX0i8K3oACOU0B/Zu9N69GQ/W7xhYFBsUAI/S9Mf
BDyFM3eZqKs/R8EQHDzB61TJzOk9Ow6TVKqOsg89V4F0oK0B1tHkTWSO
LHKwKMpGABofXtuRtemR1bhuKNuaOSxuZvk8JaF8fXfRJBiAFXKlsWVS LBk=
```



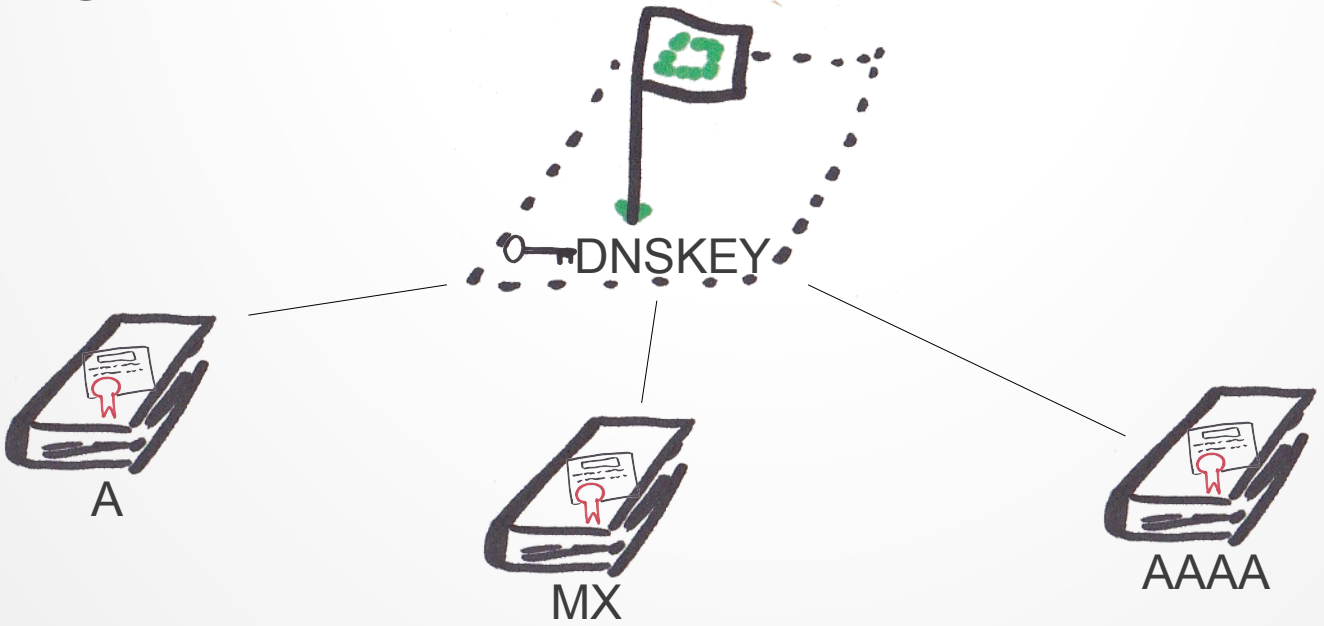
DNSSEC – Signatur – Aufbau



DNSSEC – Signatur – Validierung

- Signatur ist da – aber gültig?

- Signatur wird mit Schlüsselpaar erzeugt
  - Signatur mit öffentlichem Schlüssel überprüfen
- Schlüssel: DNSKEY-Record
  - liegt in „unterzeichnender Zone“

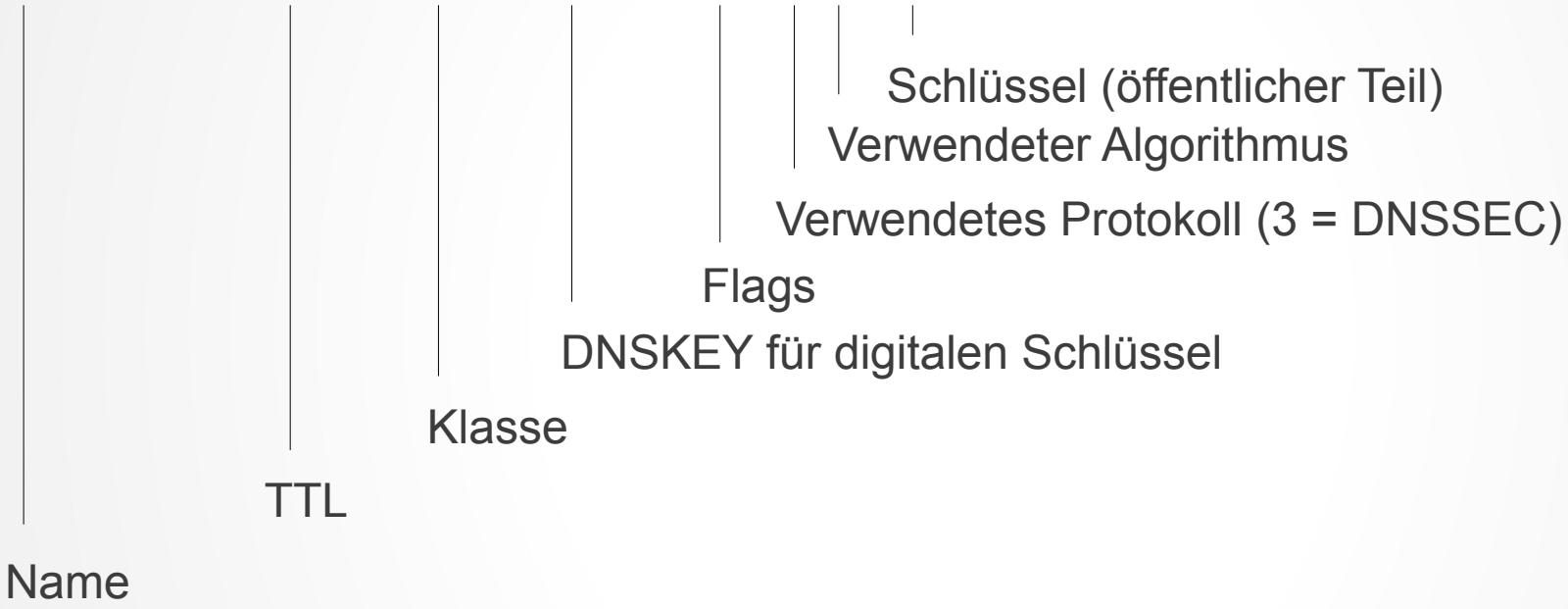


DNSSEC – Schlüssel – Beispiel

```
~$ dig +dnssec -t DNSKEY bund.de

;; ANSWER SECTION:
bund.de.     14372    IN   DNSKEY   257 3 7
AwEAAbHZMsmY/eWFaa+l4jM6C/j5QDQeNuG6lFpDuUjszxaeFSYckTyL
cmiGsSExC8movnKY9fc4X4GcM59bgSIX/ee+dgBBap5UCWmKTbO13rl1
nIm7jSSbo50MKSc00KX26shHaDUrMlF/wA4aJJEqZ0CVaL//JRNKEpuZ
a6UpveaDrzi0pL9qtgKbKmPsjYpHfljtJrSdcSzmmhqRBN2845cIUgBo
efBGfEuYNhLB8tGMXcq4uMwFH1qXcc5IUftf8c/wn0+9eo3Ga9N9eKKm
PUT4ERlkg7a9S0mJytEV8SoB4eTQexg4uYTY5FtjCPeMZKc8roFwPQQy zBmkRqH1Jrs=
bund.de.     14372    IN   DNSKEY   256 3 7
AwEAAcU/GIh0YzrxVLOglF48JX0lnXZEV/KVka4zZzjfT41+W/V8le6x
lyAfjzH4EA/tNbWD9ZSe6ugKefek+u2i5aSwcP4RaThOMvXPcB3VkO3n
a0XYMbki4kjSG12DbfZcSpI3RYiL9ZhTkxO5U5h+rgXbA/oPByKHU87/ Z64BhJhZ
bund.de.     14372    IN   RRSIG    DNSKEY 7 2 14400 20130120125001 20130110125001 5465
bund.de. MtCEcAa93W4lqe12TysfMMjs26Ej++LMJxAk6gFjnc7MG+PyXqtHBu2A
FxqM/5qDwcS+4df0XZQoMzLkcpQPLxKUfJwY4ymr7fKly7dBqHXTN0v5
u6QwSKD/sK6QrEwVuMkpxIttF9EYad/fYmX5NBqnzsOWv/hYKp4SBSht 9Rw=
bund.de.     14372    IN   RRSIG    DNSKEY 7 2 14400 20130120125001 20130110125001 28608
bund.de. rHwsga+lo3EvALUIdR974jcy8ThNx1fEFow5Ksx2jaxPTaTyb+QRwG9J
8eYFhzzON5/rEHATkIWVYZpStbg7sirhfcLEE6kTnnGSfywANjVF9rg+
ksvszGV0f8/zi42gzcegA0XfO695jmfSY3J3m2dCA6k9FuylCznPl4IH
WL37XgYoui2GYltzvtXIOt7bjG6aFaTX/bvGuiBH+QrKt0gDZDk6wcvb
T/TAgIaC/bwXNl+sHNyBOzKdDVuUXA8CwyEqjhGV4a+q6tkyfbroFMM5
Qvw5Rqtz9DtDNFyB0P0az9cock+zxlceNPm9xDniQTFM7m/ZZH6A6ZIN tMPLFw==
```

DNSSEC – Schlüssel – Aufbau

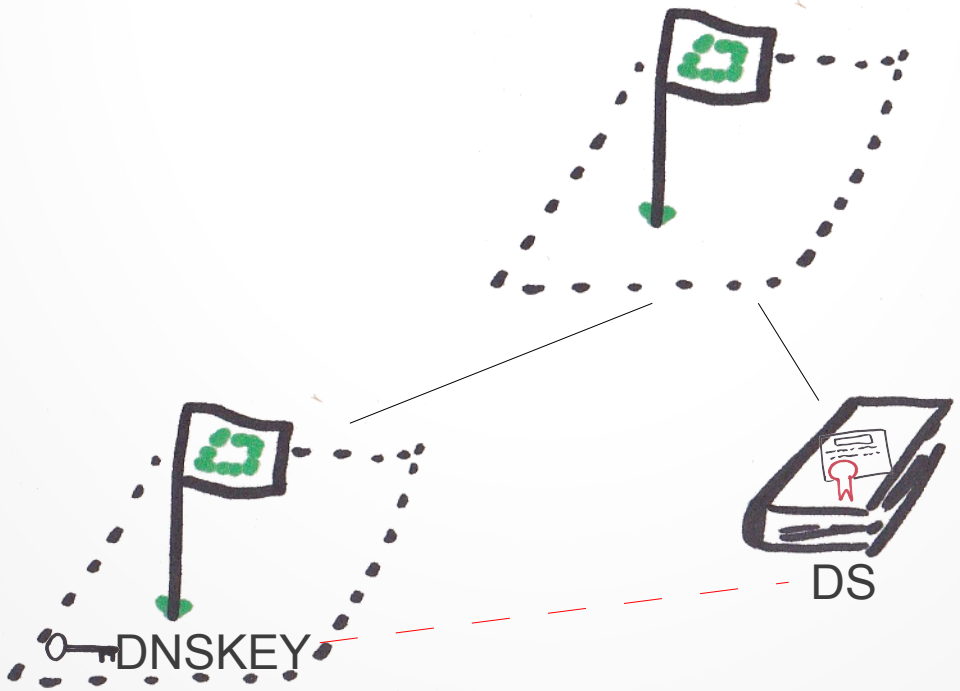
```
bund.de.     14372    IN   DNSKEY   257 3 7 AwE...
```



DNSSEC – Echtheit des Schlüssels

- Schlüssel bekannt, Signatur kann validiert werden
- Aber: Ist der Schlüssel überhaupt korrekt?

- Schlüssel-Authentifizierung
  - Übergeordnete Zone stellt Hash des Schlüssels bereit (DS-Record)

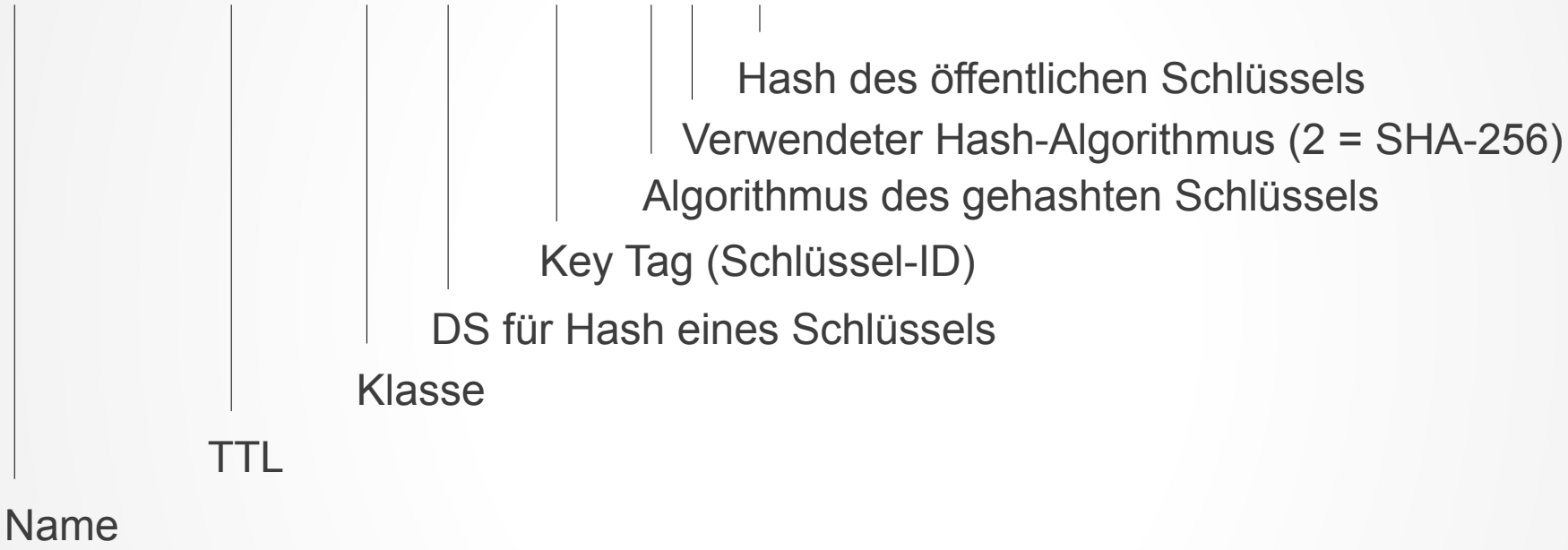


DNSSEC – Hash – Beispiel

```
$ dig +dnssec -t DS bund.de

;; ANSWER SECTION:
bund.de.     43144    IN   DS   28608 7 2
5880A557096B6AA01BD37CDEA8CCC85FC966845A75A78ED63A4CBB64 9BF9BF68
bund.de.     43144    IN   DS   10923 7 2
9C621225960D5837BB1CFE49F421CF341422AB206414E454245F055F 5581C75D
bund.de.     43144    IN   RRSIG    DS 8 2 86400 20130123070000 20130116070000 1540 de.
v7Ki/IZVdId/fcvlDISUGgPW2rNJj6fI87vriSwDDcUNFzZQMGtOpwqj
xlw4VHt+gJn+NFKvWLGcKR7UgKn/IrDalV18HQgg5OeIOmez58vR5krH
xE2KBt8JRonuX5Fjn3u2NntAvKmT/RBuBd4e99OgqFdp5l8nDbp4UnNY H10=
```

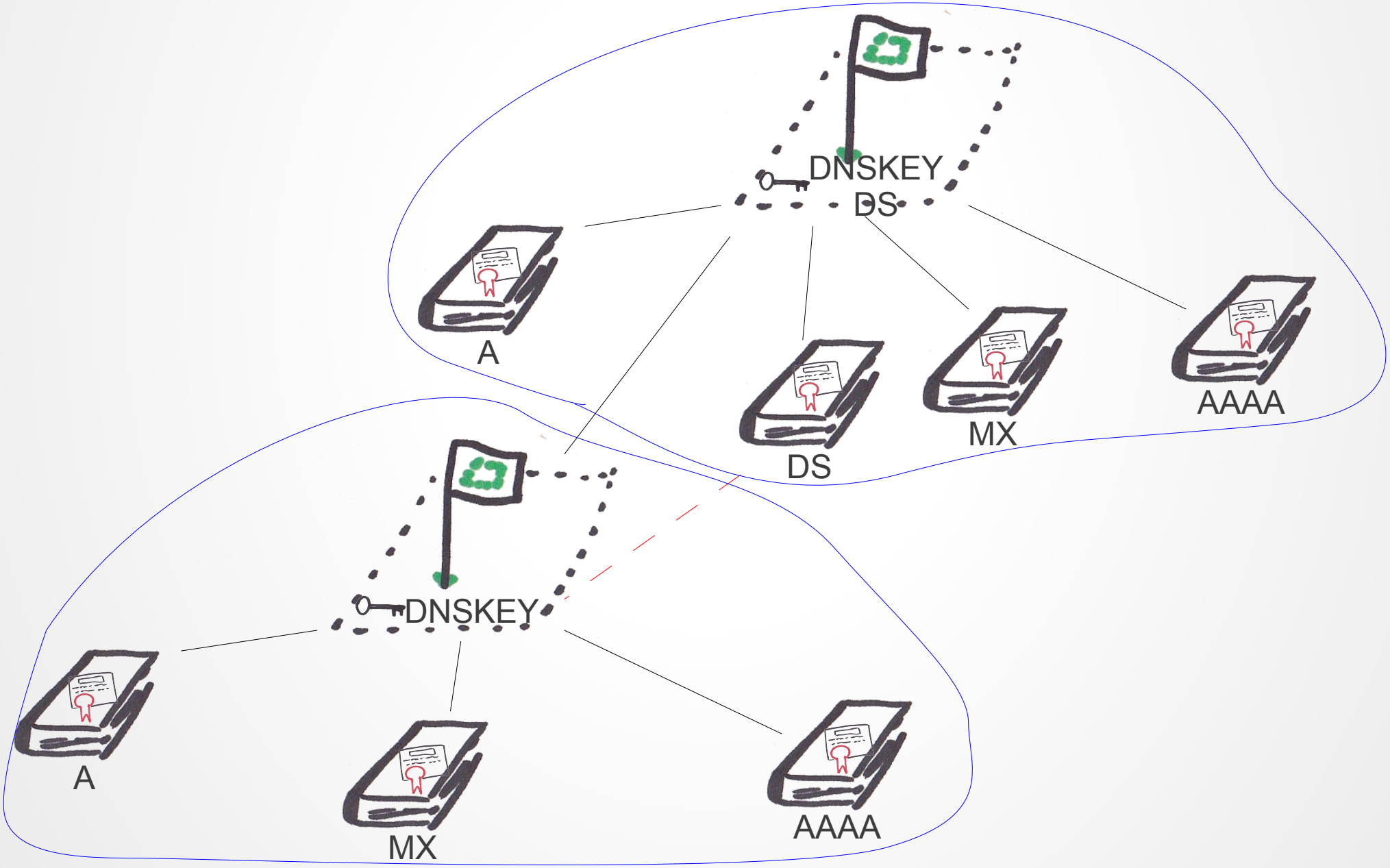
DNSSEC – Hash – Aufbau

```
bund.de.     43144    IN   DS   28608 7 2 588...
```



DNSSEC – Key Chain

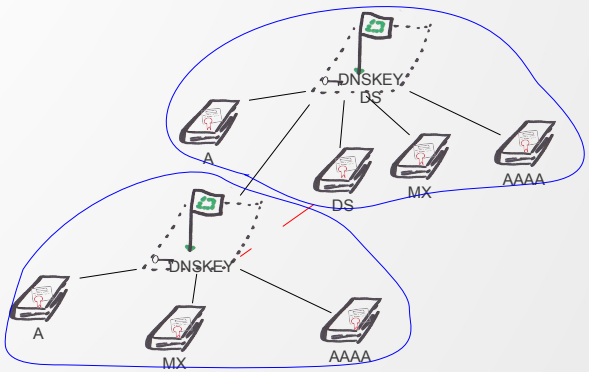
- Key Chain komplett



DNSSEC – Key Chain

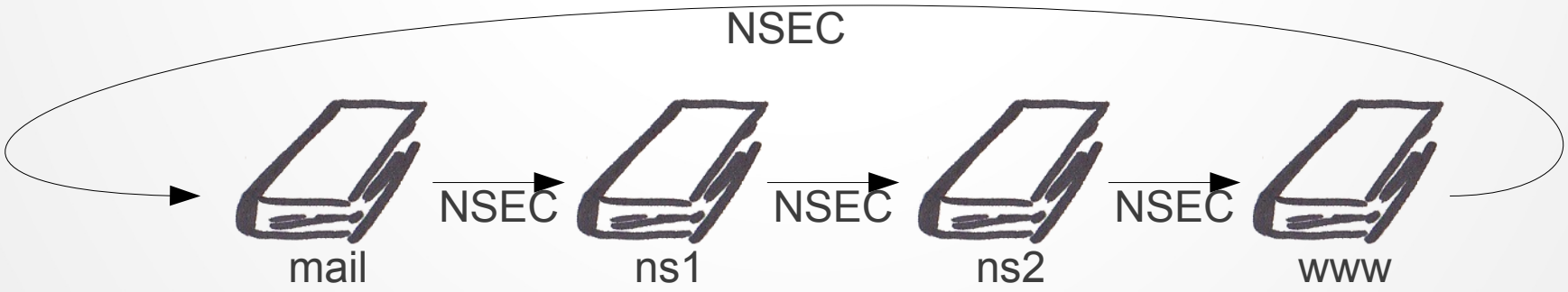
- Key Chain beliebig tief verschachtelt
- Validierung rekursiv bis zur obersten Ebene
- Schlüssel/Hashes der Root-Zone bekannt
  - Vom Betriebssystem mit ausgeliefert (wie die Liste der Root-Nameserver)

- Überprüfung möglich ✓



DNSSEC – Nichtexistente Records

- Problem: Was, wenn ein Record nicht existiert?
  - Angreifer könnte einfach Pakete droppen und durch leere Antworten ersetzen
  - Leere Pakete haben keine Signatur
- Lösung: Namens-Ketten mit NSEC-Records
  - Alphabetische Sortierung

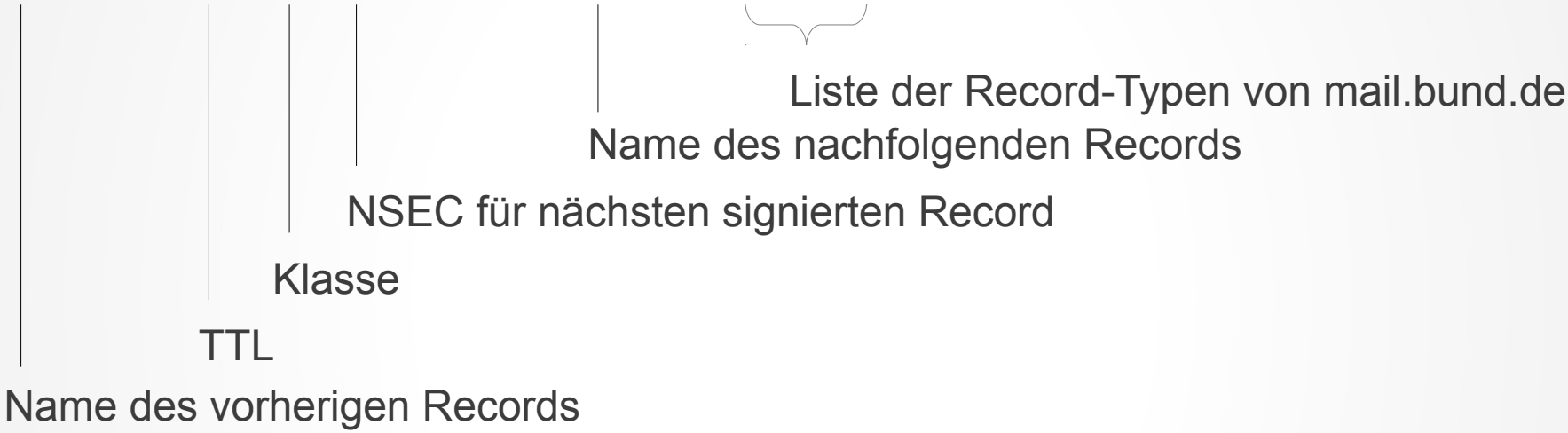


DNSSEC – NSEC – Beispiel

```
$ dig +dnssec -t A test.bund.de

;; AUTHORITY SECTION:
bund.de.     2924 IN  SOA radium.bund.de. uhd.bund.de. 2013011002 10800 3600 604800 14400
bund.de.     2924 IN  RRSIG   SOA 7 2 21600 20130120125001 20130110125001 5465 bund.de.
JJQ2GcZrrRSVc6LswX34ufy2uHKYFTo4oCe7L4mZ3TciDdui+Q635pPT
qq3dBz4zCGV4Ry4uNm8iQNzK7IkBuzrIbLANUcP//CLJ4leNhgocRokQ
vKFLDCWjtBQ52NOx1xE6fdRUMy6OWYWjHqiYouv2lrj0VMPLK+18VTSV p9M=
mail.bund.de. 2924 IN RRSIG   NSEC 7 3 14400 20130120125001 20130110125001 5465 bund.de.
MNR1xwJhdpBG8+cDapgYpcwV9szf+w4ou15aqArcYwjGPR1R6rXBFbAd
4k2zcxTDtNY6Y+E7beDh0597r3NHIAfdMeB9IkMImaUcCKMMafciMrmh
Q1HNwHZlgUiIAdIVdZRYOjxZcwxy93FOnSI3+cI+waNzgZjPq03uRiMz uFY=
mail.bund.de. 2924 IN NSEC    www.bund.de. A RRSIG
```

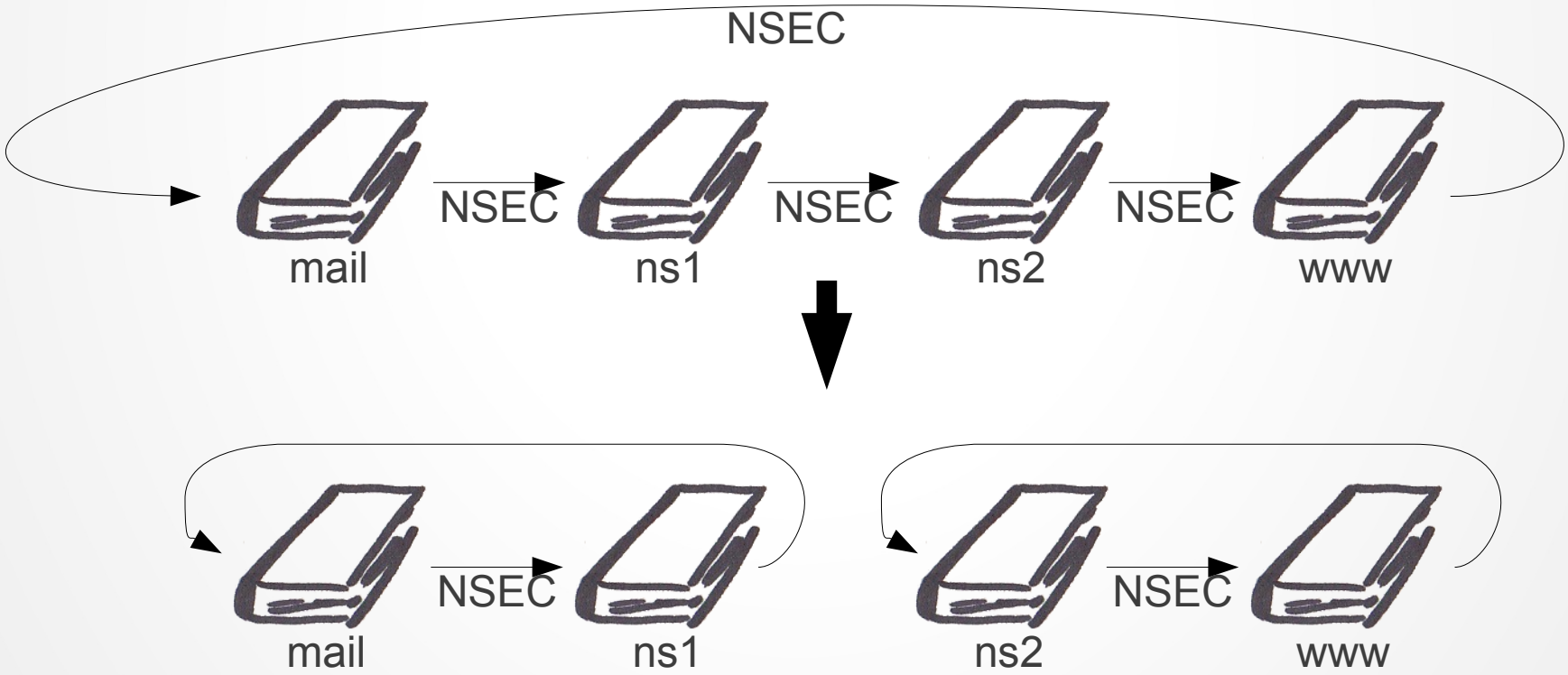
DNSSEC – NSEC – Aufbau

```
mail.bund.de. 2924 IN NSEC    www.bund.de. MX RRSIG
```



DNSSEC – NSEC

- Nachteil: Iterationen möglich (zone walking)
  - Alle (auch möglicherweise interne) Records auflistbar
- Verbesserung:
  - Erste Idee: Mehrere NSEC-„Kreise“



DNSSEC – NSEC

- Problem gelöst?
  - Zone Walking schwieriger
  - nicht unmöglich
- Neue Idee
  - Hashes statt lesbarer Domain-Namen

DNSSEC – NSEC3 – Beispiel

```
$ dig +dnssec -t A test.bund.de

;; AUTHORITY SECTION:
bund.de.     1800 IN   SOA  radium.bund.de. uhd.bund.de. 2013011002 10800 3600 604800 14400
bund.de.     14400    IN   RRSIG    SOA 7 2 21600 20130120125001 20130110125001 5465 bund.de.
JJQ2GcZrrRSVc6LswX34ufy2uHKYFTo4oCe7L4mZ3TciDdui+Q635pPT
qq3dBz4zCGV4Ry4uNm8iQNzK7IkBuzrIbLANUcP//CLJ4leNhgocRokQ
vKFLDCWjtBQ52NOx1xE6fdRUMy6OWYWjHqiYouv2lrj0VMPLK+18VTSV p9M=
J97P86RAL50L5TPDPPTN84O5EJ4D90VQ.bund.de. 14400    IN NSEC3 1 0 10 3D0CB9
JC4KJO7B5E378QHM2997P7BQPR71E6F0 A NS SOA MX RRSIG DNSKEY NSEC3PARAM
J97P86RAL50L5TPDPPTN84O5EJ4D90VQ.bund.de. 14400    IN RRSIG NSEC3 7 3 14400 20130120125001
20130110125001 5465 bund.de. MiepYCz9cK3uF0S8DN1HXYZdobv94yKpQkw9HwvrCrjF9xjwfoJIjVA2
Ms1TuzSW+zjND0YugL5LYdZmCkHA0iaIAY8efVj+VuEvZiql8iQL+2Sx T5AUISiYYbvL/
+JEBTUOZpnPiEx+S7o5hYoeVqjY2XU9VJYJMyuQ5c6m HPo=
81S3BC64ANM495CJ1QVSD0O44U0CFPLJ.bund.de. 14400    IN NSEC3 1 0 10 3D0CB9
866Q4IHC1L5Q0QREE8TSKKCHUDN0TKBE MX RRSIG
81S3BC64ANM495CJ1QVSD0O44U0CFPLJ.bund.de. 14400    IN RRSIG NSEC3 7 3 14400 20130120125001
20130110125001 5465 bund.de. VwdV+5ls9JrDZl3noG3wBJhkiAbRXO9KQgpB9YzBuB5L2/TbUCdTdqTP
M+Cvnd2y0S0WFsLJqS5reEej6eXZiLZoFe9+dJFvlhfDP9vmbHQUw9hY
oEIgzrM68M9a8giTVOZUrx9x6Vpus8aBDi3rZ2b0sMNqoY7ORV+6pxU+ geo=
2KIMSAR1Q5HUGJBN4UJEDBURHD7DI4DM.bund.de. 14400    IN NSEC3 1 0 10 3D0CB9
2L9KGADPISA77B7S2P1HVND15IAL7UO5 MX RRSIG
2KIMSAR1Q5HUGJBN4UJEDBURHD7DI4DM.bund.de. 14400    IN RRSIG NSEC3 7 3 14400 20130120125001
20130110125001 5465 bund.de. MNR1xwJhdpBG8+cDapgYpcwV9szf+w4ou15aqArcYwjGPR1R6rXBFbAd
4k2zcxTDtNY6Y+E7beDh0597r3NHIAfdMeB9IkMImaUcCKMMafciMrmh
Q1HNwHZlgUiIAdIVdZRYOjxZcwxy93FOnSI3+cI+waNzgZjPq03uRiMz uFY=
```

DNSSEC – NSEC3 – Aufbau

```
J97...0VQ.bund.de. 14400 IN NSEC3 1 0 10 3D0CB9 JC4...6F0 A ... RRSIG DNSKEY NSEC3PARAM
```

Liste der Record-Typen

Hash des nachfolgenden Record-Namens

Salt (für Hash)

Anzahl Iterationen

Flags

Hash-Algorithmus

NSEC3

Klasse

TTL

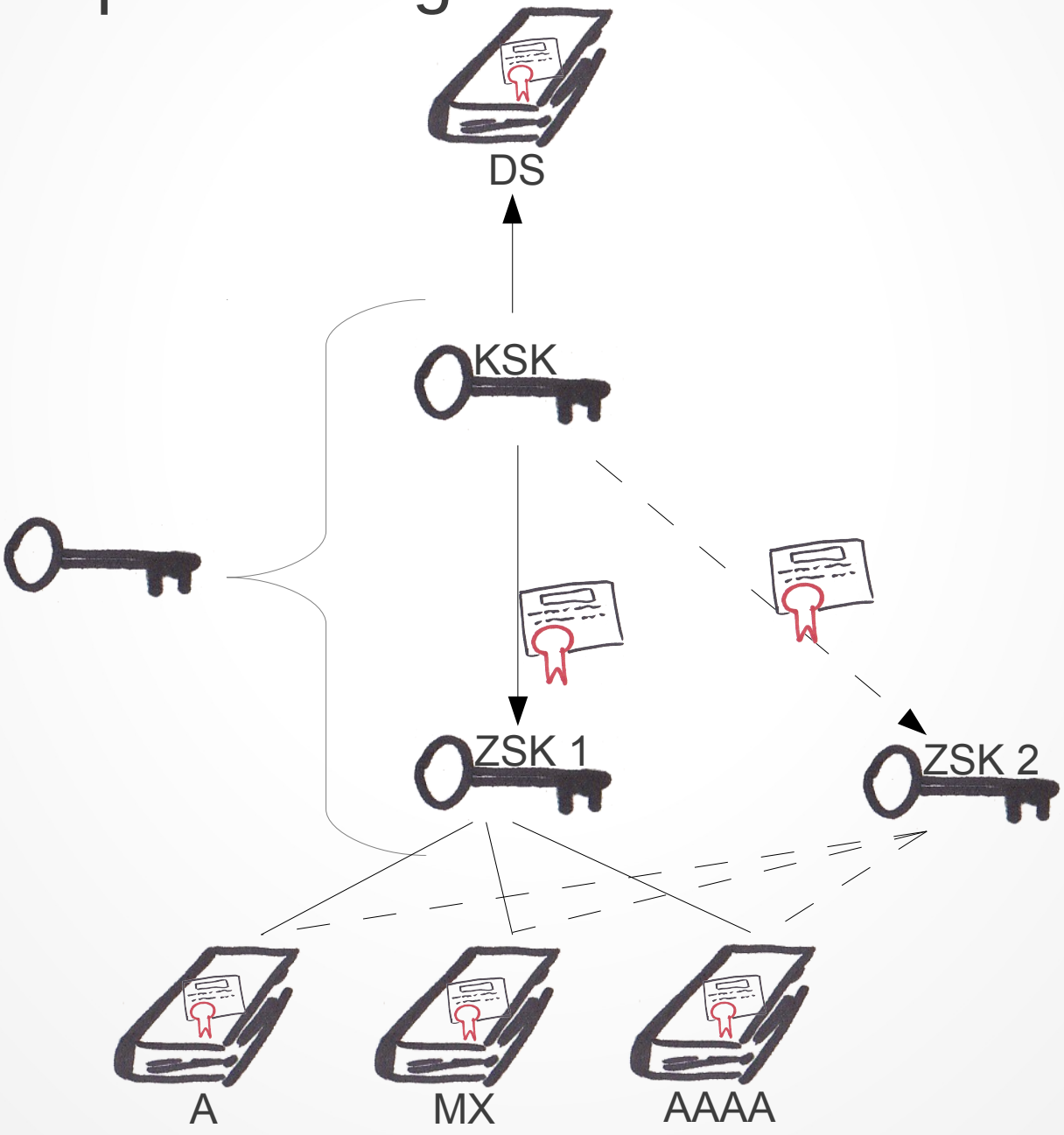
Hash des vorherigen Record-Namens

DNSSEC – Schlüsseltausch

- Schlüssel sind mit Ablaufdatum versehen
  - Je „höher“ in der Hierarchie desto länger die Gültigkeit
- Teilweise können mehrere Schlüssel parallel existieren
- Unterteilung in KSK und ZSK (Key Signing Key und Zone Signing Key)

DNSSEC – KSK und ZSK

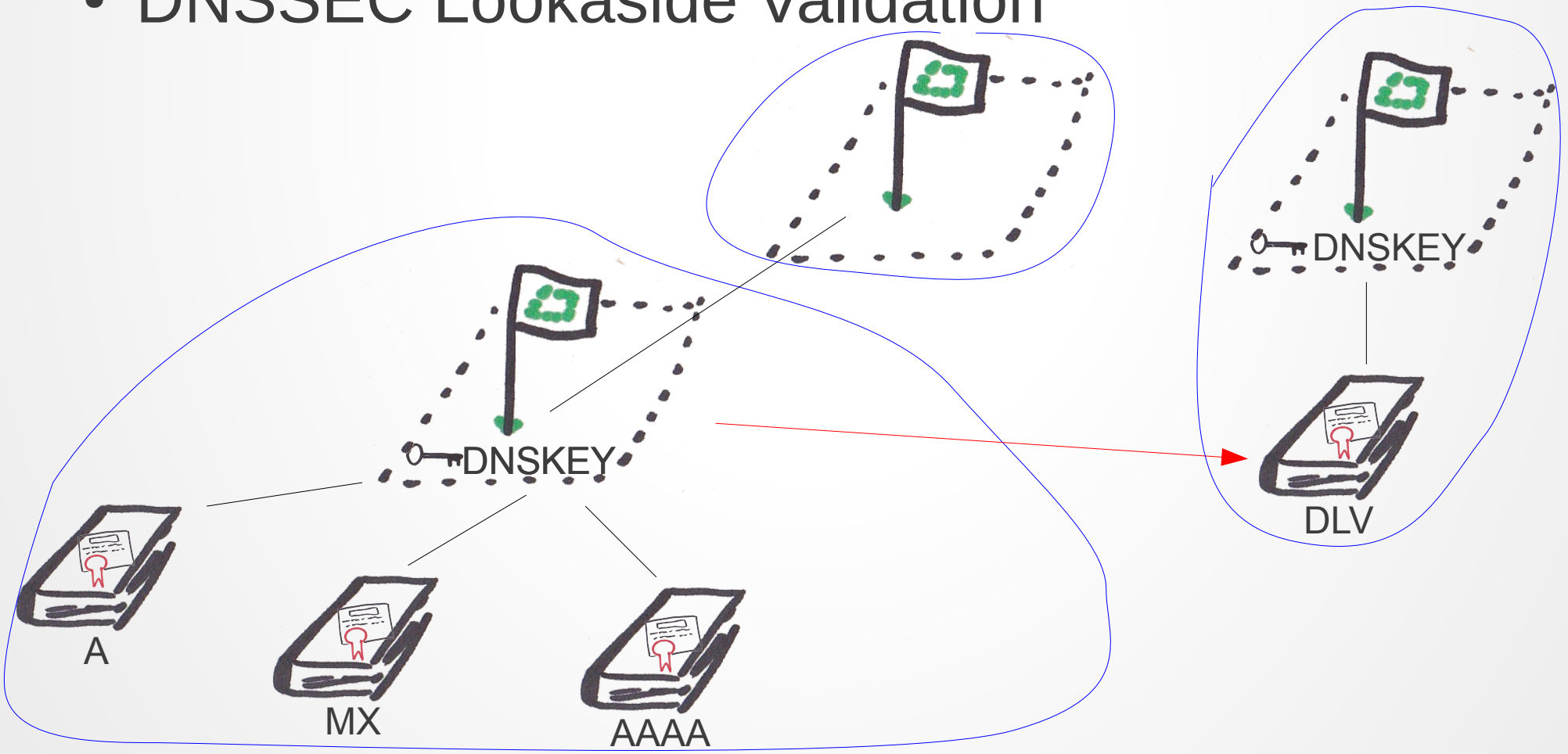
- Schlüsselpaare aufgeteilt in KSK und ZSK:



DNSSEC – nicht unterstützt?

- Was tun, wenn die übergeordnete Zone DNSSEC nicht unterstützt?

- DNSSEC Lookaside Validation



DNSSEC – DLV

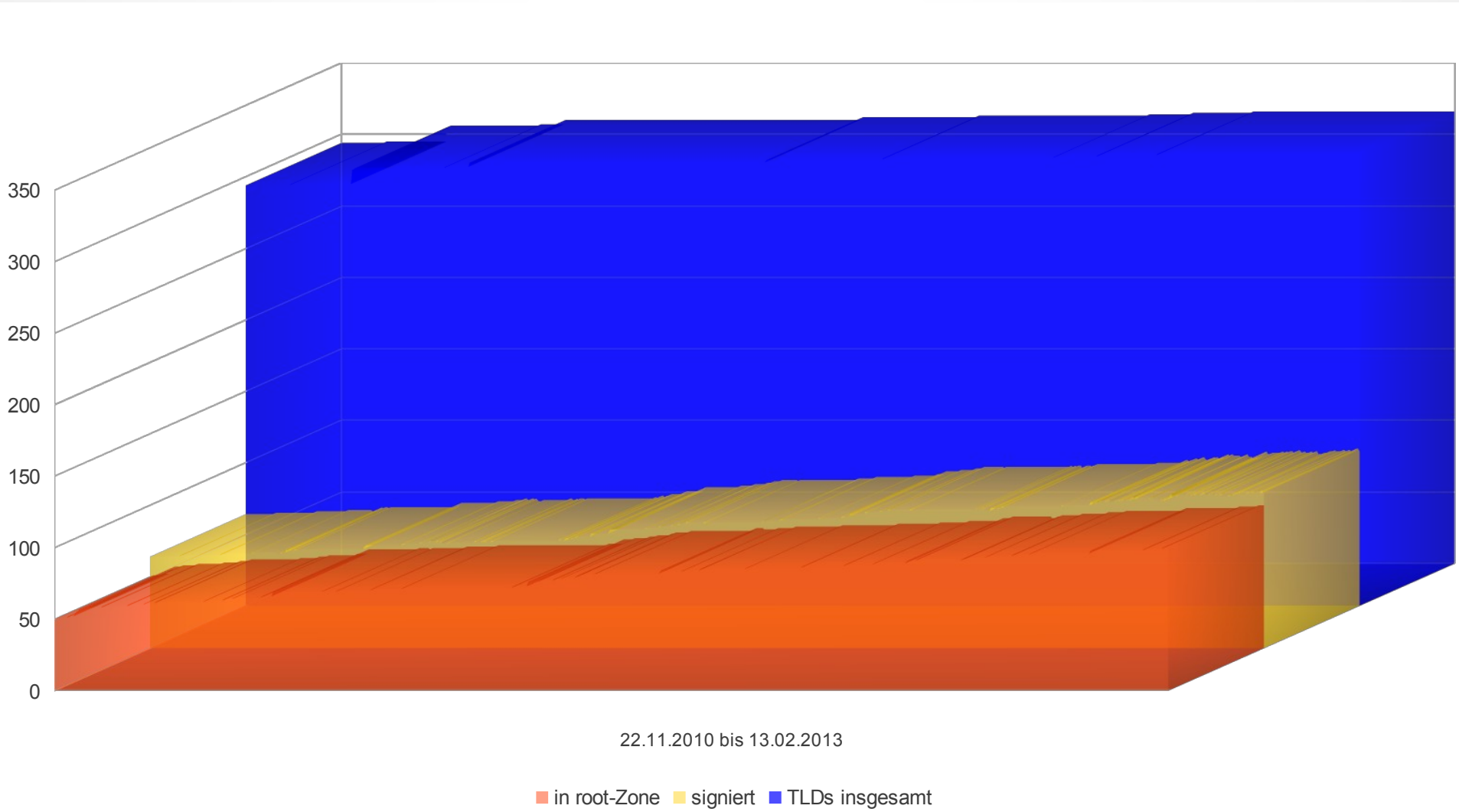
- Gleiche Felder wie DS
- Schlüssel-Hash in beliebiger Zone statt parent zone
- Konfiguration eines sog. „trust anchor“ im Resolver, zeigt auf Zone mit DLV-Records
- DLV-Dienst: https://dlv.isc.org/

DNSSEC – Verbreitung

- Verbreitung steigt langsam, Gründe dafür sind
  - höhere Auslastung der Server
  - mehr Wartungsarbeiten
- Standardverhalten bei fehlender/ungültiger Signatur: Trotzdem akzeptieren.
  - Problematik ähnlich wie bei SSL-Zertifikaten

DNSSEC – Verbreitung

- Zeitlicher Verlauf vom 22.11.2010 bis 13.02.2013



Daten Stand 13.02.2013, Quelle: http://stats.research.icann.org/dns/tld_report/

DNSSEC – Verbreitung

- Aktueller Stand
  (Stand 13.02.2013, Quelle: http://stats.research.icann.org/dns/tld_report/)
  - 316 TLDs in der root-Zone
  - 108 TLDs sind signiert
  - 100 TLDs veröffentlichen DS-Record in der root-Zone

- Top Level Domains mit DNSSEC:

ac, ag, am, arpa, asia, at, be, bg, biz, br, bz, ca, cat, cc, ch, cl, co, com, cr, cz, de, dk, edu, eu, fi, fo, fr, gi, gl, gov, gr, hn, in, info, io, jp, kg, kr, la, lb, lc, li, lk, lu, lv, me, mil, mm, mn, museum, my, na, nc, net, nl, nu, nz, org, pl, pm, post, pr, pt, pw, re, ru, sc, se, sh, si, su, sx, tf, th, tm, tt, tw, tz, ua, ug, uk, us, wf, xn--0zwm56d.   测试 , xn--11b5bs3a9aj6g.   परीक्षा, xn--3e0b707e.   한국 , xn--80akhbyknj4f.   испытание, xn--9t4b11yi5a.   테스트 , xn--deba0ad.   ᵾᵴᵴᵾ, xn--g6w251d.   測試 , xn--hgbk6aj7f53bba.   آزمایشی, xn--hlcj6aya9esc7a.   பரிட்சை, xn--jxalpdlp.   δοκιμή, xn--kgbechtv.   إختبار, xn--kprw13d.   台湾 , xn--kpry57d.   台灣 , xn--mgbx4cd0ab.   مليسيا, xn--p1ai.   рф, xn--zckzah.   テスト , yt

DNSSEC

Vielen Dank

für

Ihre Aufmerksamkeit!

DNSSEC – Software

- BIND
  - Daten liegen in Textdateien
  - Signatur wird über CLI-Tool erzeug
  - https://www.isc.org/software/bind
- PowerDNS
  - Daten liegen in SQL-Datenbank
  - Signierung und Schlüsselwechsel automatisiert
    - Ausnahme: KSK, DS muss manuell abgefragt werden
  - http://www.powerdns.com/

DNSSEC – Anbieter

- Hostway Deutschland
  - Nur für Unternehmenskunden
  - DNSSEC per API steuerbar
  - Beta-Betrieb
  - http://www.hostway.de/webhosting/domains/s-dns/index.php
- InterNetworx
  - Privat- und Unternehmenskunden
  - DS-Eintrag über Support
  - https://www.inwx.de/

DNSSEC

Domain Name System Security Extension

Referent:
Matthias Lohr <lohr@uni-trier.de>