DNS 2

DNSSEC – Hintergründe

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Agenda

TECHNISCHE UNIVERSITÄT DARMSTADT

1. Wie es war
2. Wie es ist
3. Was sich daraus ergibt
4. TTL
5. DNSSEC
6. KSK Rollover
7. Fragen

1. Wie es war

TECHNISCHE UNIVERSITÄT DARMSTADT

Autoritativ

Ist für eine Domain zuständig

Resolving

Gibt Antworten auf Anfragen und geht nötigenfalls selber suchen

3 Nameservern mit jeweils beiden Diensten

HRZ Hochschulrechenzentrum

1.1. Nameserver an der TU

TECHNISCHE UNIVERSITÄT DARMSTADT

Hostname	IPv4	IPv6
ns1.hrz.tu-darmstadt.de	130.83.22.63	2001:41b8:83f:22::60
ns2.hrz.tu-darmstadt.de	130.83.22.60	2001:41b8:83f:22::63
ns3.hrz.tu-darmstadt.de	130.83.56.60	2001:41b8:83f:56::60

3 Nameservern mit jeweils beiden Diensten

2. Wie es ist

TECHNISCHE UNIVERSITÄT DARMSTADT

Autoritativ

Ist für eine Domain zuständig

Resolving

Gibt Antworten auf Anfragen und geht nötigenfalls selber suchen

2 (neue) Nameserver als Autoritative Nameserver

3 (alte) Nameserver als Resolving Nameserver (aka Resolver)

2.1. Autoritative Nameserver an der TU

TECHNISCHE UNIVERSITÄT DARMSTADT

Hostname	IPv4	IPv6
ans1.net.hrz.tu-darmstadt.de	130.83.22.61	2001:41b8:83f:22::61
ans2.net.hrz.tu-darmstadt.de	130.83.56.61	2001:41b8:83f:56::61

2 (neue) Nameserver als Autoritative Nameserver

2.2. Resolving Nameserver an der TU

TECHNISCHE UNIVERSITÄT DARMSTADT

Hostname	IPv4	IPv6
ns1.hrz.tu-darmstadt.de	130.83.22.63	2001:41b8:83f:22::60
ns2.hrz.tu-darmstadt.de	130.83.22.60	2001:41b8:83f:22::63
ns3.hrz.tu-darmstadt.de	130.83.56.60	2001:41b8:83f:56::60

3 (alte) Nameserver als Resolving Nameserver (aka Resolver)

3. Was sich daraus ergibt

TECHNISCHE UNIVERSITÄT DARMSTADT

- Keine Änderungen für normale Namensauflösung
- Änderungen falls man einen eigenen Nameserver betreibt
  - Zonen liegen jetzt auf der ans1 und ans2
  - Forwarders bleiben auf der ns1, ns2 und ns3
- Negatives Caching 15min (900s) anstatt 3h (10800s)
- Änderungen greifen nicht mehr zu einer bestimmten Zeit (Stichwort TTL)
- DNSSEC

4. TTL

TECHNISCHE UNIVERSITÄT DARMSTADT

TTL (Time to live)

Im DNS wird eine TTL in Sekunden dargestellt und von einem Startwert aus nach unten gezählt. Bei 0 gilt der Eintrag als veraltet und wird verworfen.

1 Tag => 24 Stunden

1 Stunde => 60 Minuten * 60 Sekunden => 3600 Sekunden

24 Stunden * 3600 Sekunden => 86400 Sekunden

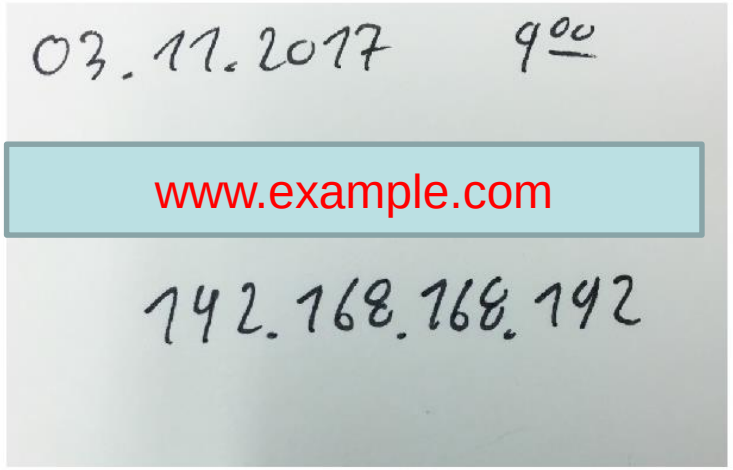
4.1. Warum wir die TTL senken

03.11.2017 9⁰⁰

www.example.com

142.168.168.142

4.2. Warum wir die TTL senken



4.3. Warum wir die TTL senken

TECHNISCHE UNIVERSITÄT DARMSTADT

Der Unterschied zwischen den beiden Bildern ist eigentlich nur das wir uns in zweiten Bild wie alle anderen verhalten.

5. DNSSEC

TECHNISCHE UNIVERSITÄT DARMSTADT

Welche Vorteile ergeben sich durch DNSSEC?

Chain-of-Trust (Kette des Vertrauens)

DANE (DNS-based Authentication of Named Entities),

DKIM (DomainKeys Identified Mail),

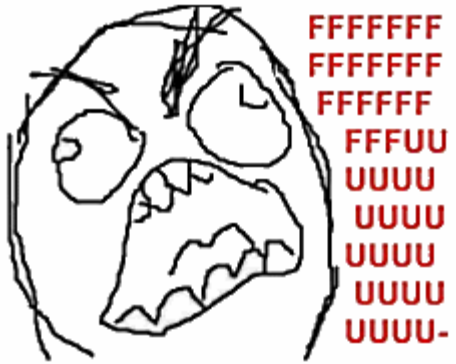
SPF (Sender Policy Framework) usw.

waren schon vorher möglich!

MIT DNSSEC kann man den Daten aber vertrauen.

5.1. DNSSEC

TECHNISCHE UNIVERSITÄT DARMSTADT



Auf http://dnssec.vs.uni-due.de kann man überprüfen ob der eigene Resolver DNSSEC unterstützt.

Wer eduroam nutzt verwendet als Resolver ns1, ns2 und ns3 und bekommt damit DNSSEC Validierung.

5.2. DNSSEC

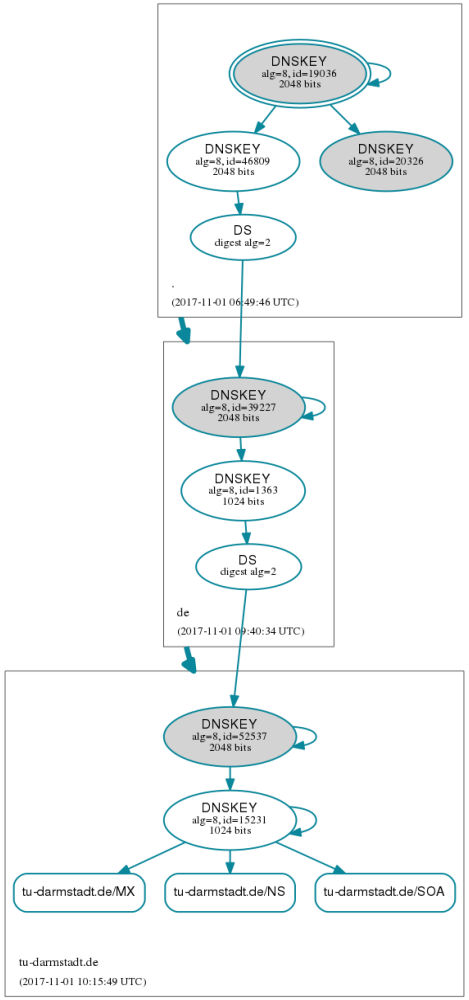
Auf https://www.dnssec-validator.cz findet man ein Plugin mit dem man DNSSEC (und TSLA (Transport Layer Security Association)) überprüfen kann.

Das Plugin wird ab Firefox 57 und wird deswegen aktuell nicht gepflegt.

5.3. DNSSEC

Für Domains (bzw. Sub Domains) kann man http://dnsviz.net verwenden. (Allerdings hat die Seite aktuell wohl Probleme.)

5.4. DNSSEC



http://dnsviz.net/

Asymmetrische Keys

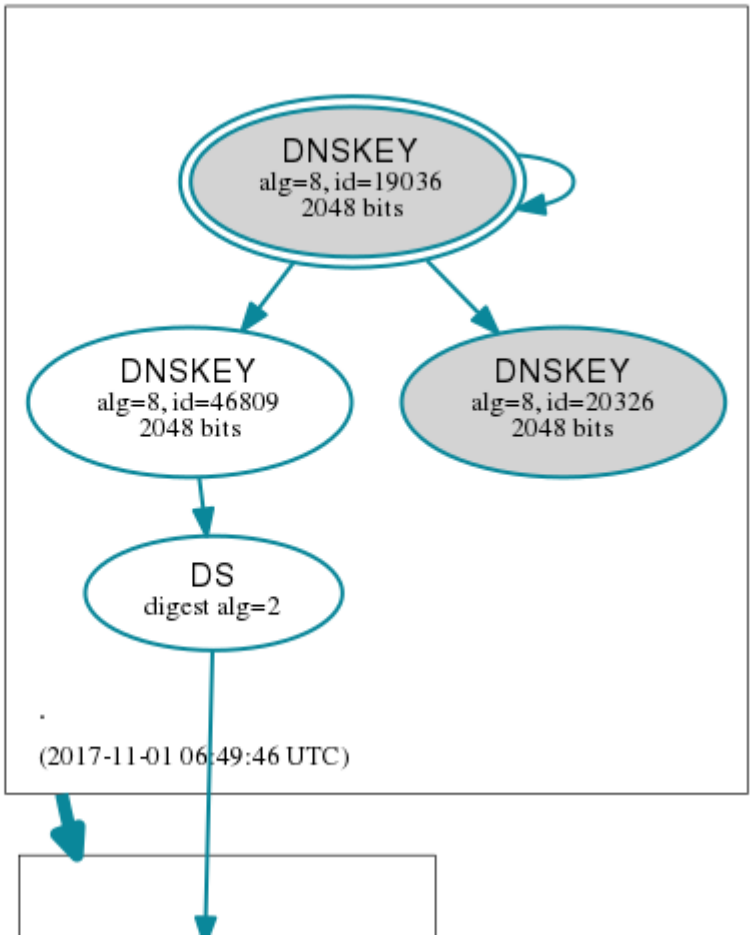
Private Key > Signieren

Public Key > Überprüfen

KSK (Key Signing Key)

ZSK (Zone Signing Key)

5.5. DNSSEC



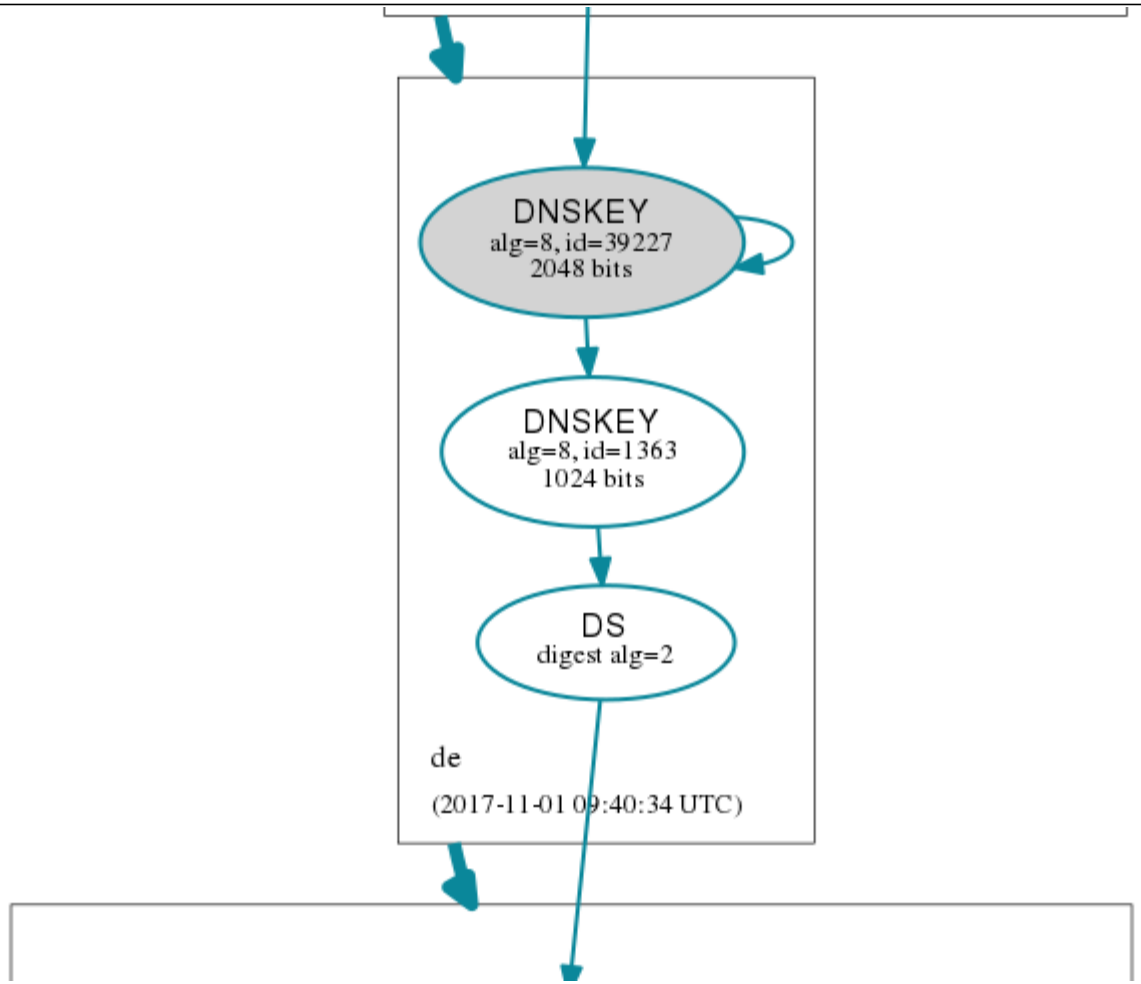
„.“ Zone (Root Zone)

alg 8 => RSASHA256

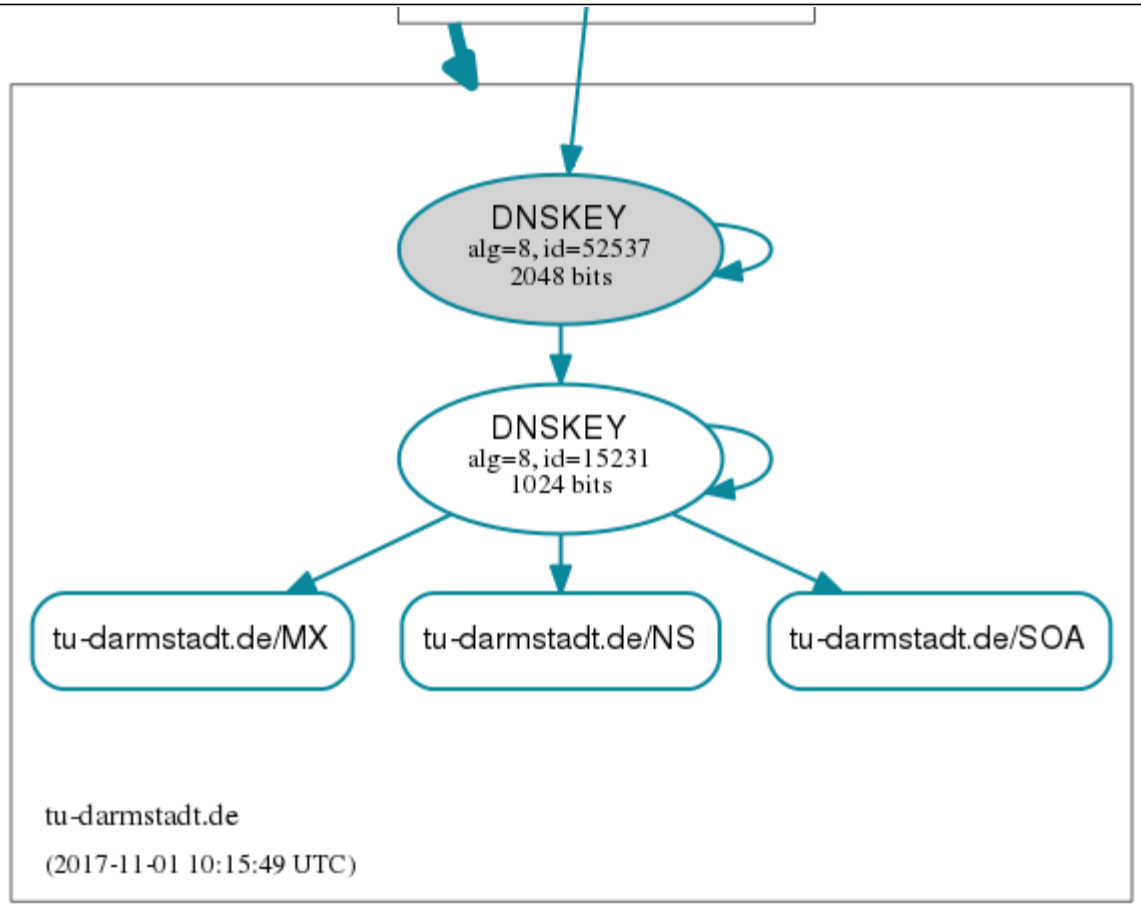
DS => Delegation Signer

5.6. DNSSEC

„de.“ Zone



5.7. DNSSEC



„tu-darmstadt.de“ Zone

6. KSK Rollover

TECHNISCHE UNIVERSITÄT DARMSTADT

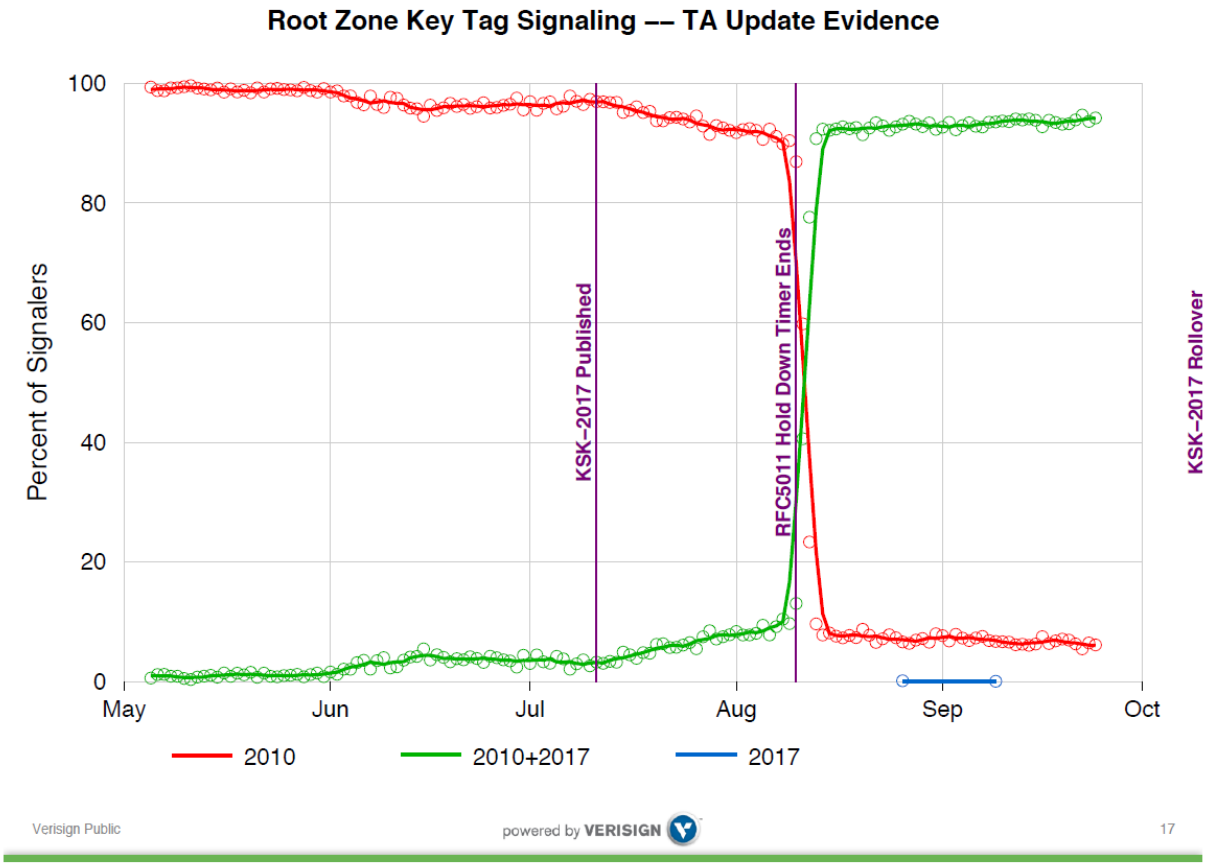
Der KSK Rollover war für den 11. Oktober geplant

Am 27. September hat das ICANN den KSK Rollover verschoben

KSK2010 => KSK der Root Zone mit der ID 19036

KSK2017 => KSK der Root Zone mit der ID 20326

6.1. KSK Rollover



6.2. KSK Rollover

TECHNISCHE UNIVERSITÄT DARMSTADT

Further analysis by OCTO Research

- ICANN OCTO Research did an analysis similar to Duane's
  - Analyzed query data from B, D, F and L
  - Combined with Verisign's A & J data
  - For 1 September 2017 through 25 September 2017
- Results:
  - Total number of unique addresses reporting key tag data: **11,692**
  - Total number that only ever reports KSK-2010: **577**
  - **4.93% of reporting validators are not ready for the KSK roll on 11 October 2017**
- Analysis is complicated
  - Dynamic IPs make the situation look worse by inflating true number of sources
  - Forwarders make the situation look better if they obscure multiple validators behind the forwarder
  - BIND reports trust anchors even if not validating

ICANN

| 2

7. Fragen

TECHNISCHE UNIVERSITÄT DARMSTADT

?

HRZ Hochschulrechenzentrum

Quellen

TECHNISCHE UNIVERSITÄT DARMSTADT

5.3. Grafik siehe https://dnsreactions.tumblr.com/post/166776837752/dnsviz-in-october

6.1. Grafik siehe Duane Wessels, VeriSign, Slides

6.2. Grafik siehe Matt Larson, ICANN, Slides

Der komplette Vortrag findet sich unter den weiterführenden Links auf der Seite https://heise.de/-3855063

0. Daten

TECHNISCHE UNIVERSITÄT DARMSTADT

- Im Juli und August 2017 wurden die Domains und Sub Domains auf ans1 und ans2 umdelegiert.
- Seit dem 28. August ist die Domain tu-darmstadt.de mit DNSSEC signiert.
- Ende August 2017 wurden auch die Ipv4 und IPv6 Reverse Mappings auf ans1 und ans2 umdelegiert.
- Seit dem 11. September sind (fast) alle ca. 280 Sub Domains der Domain tu-darmstadt.de mit DNSSEC signiert.
- Seit dem 23. Oktober wird die TTL gesenkt (24h/86400s, 12h/43200s, 6h/21600s, 3h/10800s und 1h/3600s)

2.3. Autoritative Nameserver

TECHNISCHE UNIVERSITÄT DARMSTADT

dig @8.8.8.8 th-darmstadt.de ns

ans1.net.hrz.tu-darmstadt.de.

ans2.net.hrz.tu-darmstadt.de.

dig @ans1 th-darmstadt.de soa

;; flags: qr aa rd;

th-darmstadt.de. 21600 IN SOA ans1.net.hrz.tu-darmstadt.de. netz.hrz.tu-darmstadt.de. 1111710221

2.4. Resolving Nameserver

TECHNISCHE UNIVERSITÄT DARMSTADT

Hostname zu IP => forward lookup

IP zu Hostname => reverse lookup

```
dig @ns1 adminday.th-darmstadt.de
;; flags: qr rd ra ad;
adminday.th-darmstadt.de. 21600 IN      A       130.83.42.98

dig @ns1 -x 130.83.42.98
98.42.83.130.in-addr.arpa. 21600 IN PTR adminday.th-darmstadt.de.
```