DNSSEC automatisieren mit Knot & Child DS

s3lph

s3lph@s3lph.me

@s3lph@chaos.social

@s3lph:kabelsalat.ch

CoSin 2023

June 17, 2023

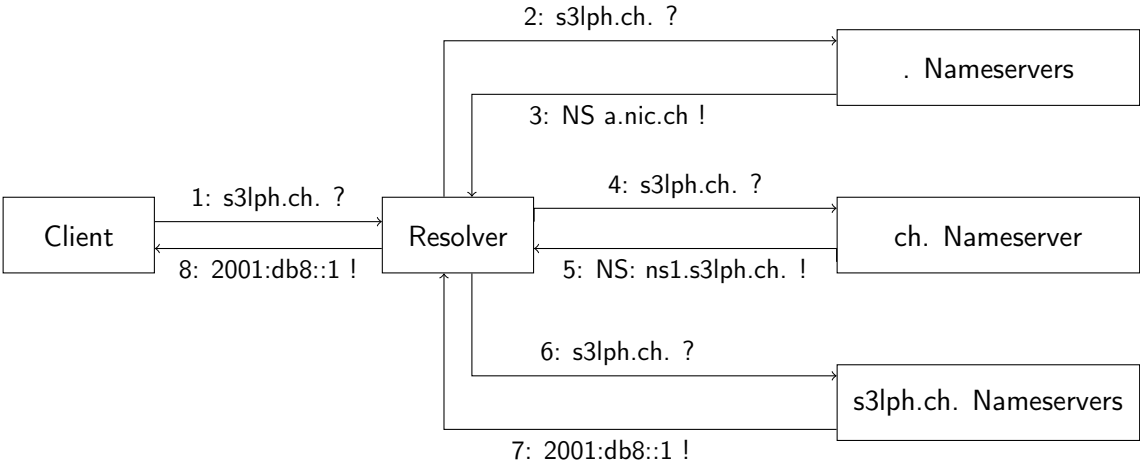
Über mich

- s3lph (he/him)
- Linux Systems Engineer
- Macht `$dinge` im CCC Basel
  - Ansible
  - Python
  - E-Mail
- www.s3lph.me

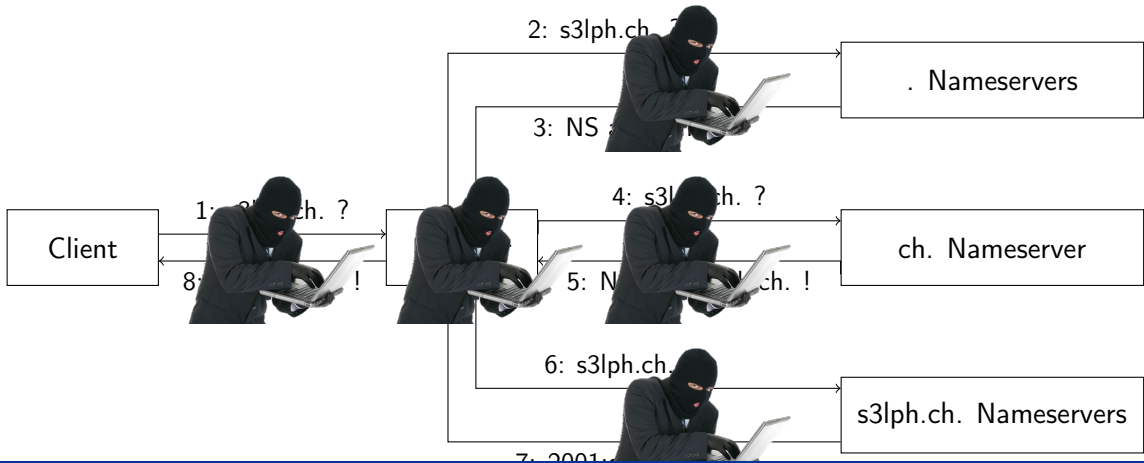
DNS Refresher

- **Domain Name System**
- Namensauflösung im Internet
  - `s3lph.ch` → `2a01:4f8:1c1c:1ae7::1`
- Dezentrale, hierarchisch strukturierte, weltweit verteilte «Datenbank»
- Unauthentifiziert, unverschlüsselt
  - Anfällig für Angriffe & Zensur

DNS Refresher



DNS Refresher



Was ist DNSSEC?

- Kryptografisch signierte DNS-Records
- Chain of Trust zwischen Zonen
- Integritätsprüfung von DNS Responses
- Authentifizierte Nicht-Existenz von Records
- RFC 4035

Was macht DNSSEC nicht?

- Transportverschlüsselung
  - DoH, DoT
- Verfügbarkeit

DNSSEC RRTypes

RRSIG	Signatur eines DNS-Records
DNSKEY	Zur Signatur verwendeter Public Key
	› ZSK, KSK oder CSK
DS	Chain of Trust zwischen Zonen
NSEC	
NSEC3	
NSEC3PARAM	Authentifizierte Nicht-Existenz

RRSIG

```
s3lph.ch.  300  IN  AAAA  2a01:4f8:1c1c:1ae7::1

s3lph.ch.  300  IN  RRSIG
    AAAA              ; RRType
    15                ; Signaturalgorithmus (15 = ed25519)
    2                 ; Hash-Algorithmus (2 = SHA256)
    300               ; TTL des Records
    20230624103205    ; Gültig bis
    20230610090205    ; Gültig von
    59883             ; Key Tag
    s3lph.ch.         ; Name der Zone
                      ; Signatur
    ho6PyVeNNzgtoYj7hkAsYJgnpTHVdsav4AI1XuoiA0QGaUfgCiZz60Sx
    r/ENfiD6p1Lv5kcLCHY852kquS5QCQ==
```

DNSKEY

```
s3lph.ch.  300  IN  DNSKEY
    256    ; Flags (256 = ZSK)
    3      ; Verwendungszweck (3 = DNSSEC)
    15     ; Signaturalgorithmus (15 = ed25519)
           ; Public Key, key tag = 52246
    zrxtj9TPFU8YkFz38Yr6Xgzw4UAiRbLqt1mLXciljOI=

s3lph.ch.  300  IN  DNSKEY
    257    ; Flags (257 = KSK)
    3
    15
           ; Public Key, key tag = 54673
    sYNO9/+iIpczl91XO418Pb4mlQn5tzWSve8ZKsbJLXQ=
```

DNSKEY

- KSK signiert das DNSKEY RRSet
- ZSK signiert den Rest der Zone
- CSK: KSK & ZSK in einem

DS

```
s3lph.ch.  86400  IN  DS
    54673     ; key tag
    15        ; Signaturalgorithmus  (15 = ed25519)
    2         ; Hash-Algorithmus (2 = SHA256)
              ; Hash des Public Keys
    6CBD333B39EA252B82E4E31AE7D9D6BA302BC62EE7BDBC92BE6768B7
    B71E1006
```

- DS-Records werden in der Parent-Zone (`ch.`) angelegt.

NSEC

```
$ dig gibt-es-nicht.s3lph.ch
gibt-es.s3lph.ch.  300  IN  NSEC
    www.s3lph.ch.     ; Nächster existierende Record
                      ; RRTypes des nächsten Records
    A SOA MX TXT AAAA RRSIG DNSKEY
```

- **Authoritative** Nicht-Existenz-Antwort
  - «Zwischen `gibt-es` und `www` sind keine weiteren Records»
  - Lexikalisch sortiert
- Ermöglicht Zone Walking
  - Lösung: NSEC3

NSEC3

```
s3lph.ch.  300  IN  NSEC3PARAM
    1                ; Hash-Algorithmus (1 = SHA1)
    0                ; Flags (0 = keine)
    0                ; Anzahl Hash-Iterationen (+1)
    8E8E43B46029F294  ; Salt

                     ; Vorangehender Hash
j9gkjdta2gissdi90m4tduc1mbu4t4u0.s3lph.ch.  300  IN  NSEC3
    1  0  0  8E8E43B46029F294           ; NSEC3PARAM-Werte
    JF5722VC39KFI6K0LU1ON3E55CN2NS7C    ; Nachfolgender Hash
                     ; Existierende RRTypes
    A SOA MX TXT AAAA RRSIG DNSKEY NSEC3PARAM
```

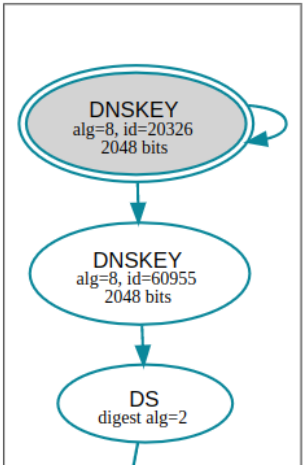
- Lexikalische Sortierung der **Hashes**
- Keine* Rückschlüsse auf tatsächliche Namen

Chain of Trust

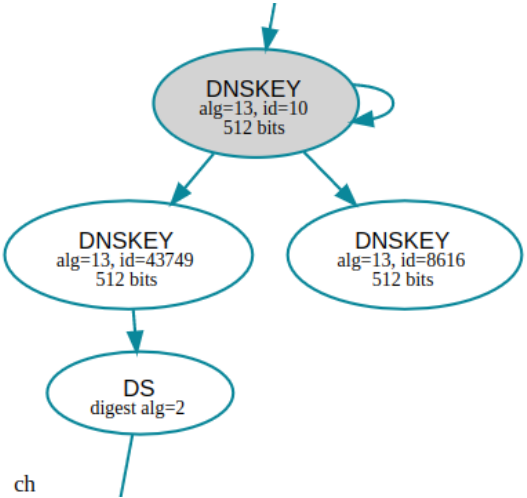
- «Und wie passt das alles jetzt zusammen?»
- Trust Anchor: ICANN Root KSK

```
.  172800  IN  DNSKEY  257 3 8 (
    AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
    iW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN
    7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5
    LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8
    efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7
    pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY
    A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws
    9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
) ; KSK; alg = RSASHA256 ; key id = 20326
```

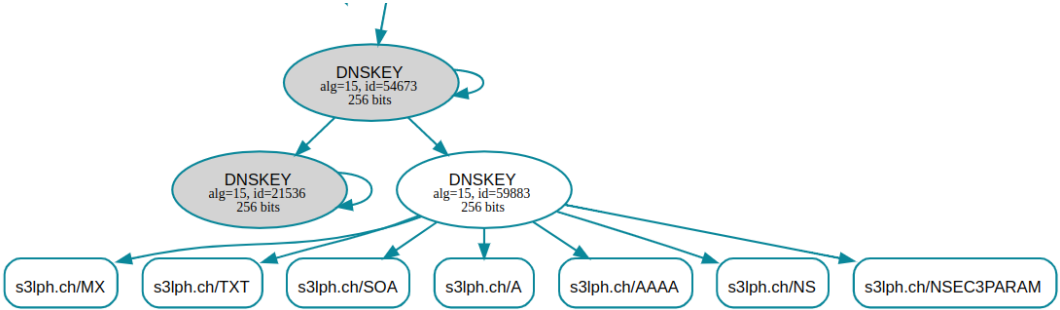
Chain of Trust



Chain of Trust



Chain of Trust



s3lph.ch

Signaturprüfung durch Resolver

Chain of Trust OK:

```
; <<>> DiG 9.18.3 <<>> sigok.verteiltesysteme.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54008
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

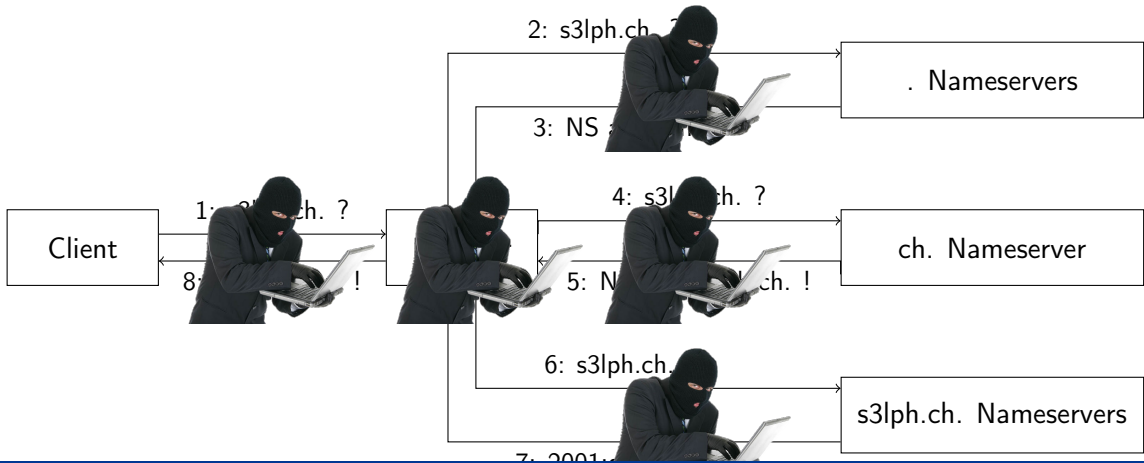
Signaturprüfung durch Resolver

Chain of Trust ungültig:

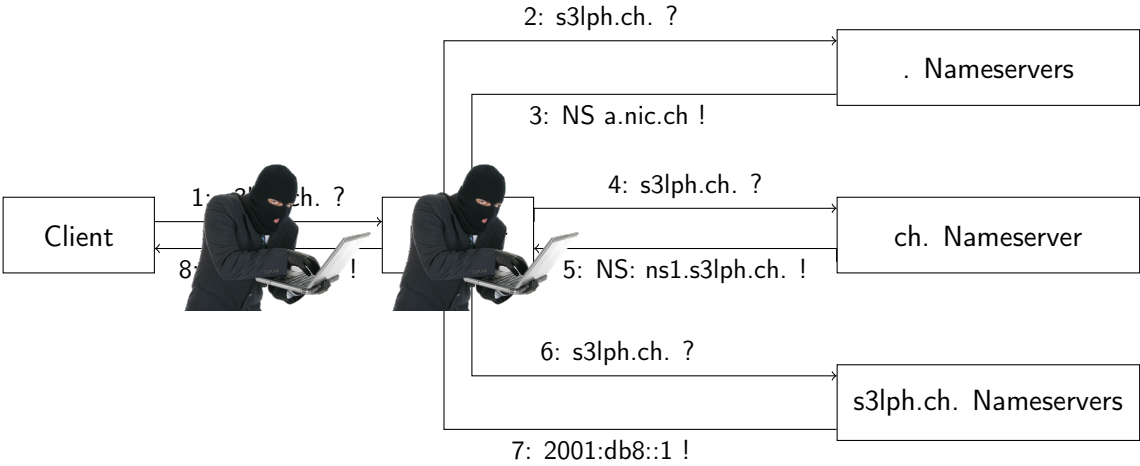
```
; <<>> DiG 9.18.3 <<>> sigfail.verteiltesysteme.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 51176
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

- **Achtung**: Dem Resolver wird blind vertraut!

Angriffsszenario ohne DNSSEC



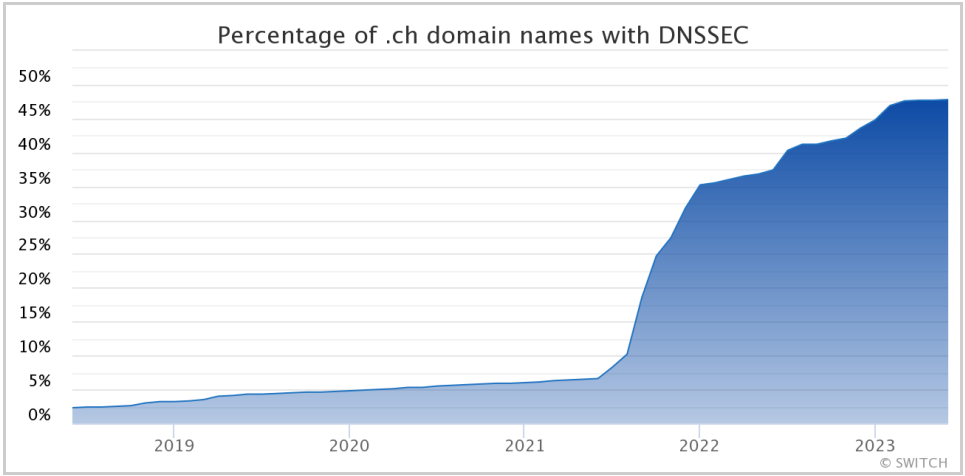
Angriffsszenario mit DNSSEC



State of the DNSSEC: Signierung

- 92% der TLDs signiert
  - `https://stats.research.icann.org/dns/tld_report/`
- Anteil .ch/.li-Domains mit DNSSEC Delegation
  - Juni 2020: 6%
  - Juni 2023: 48%
  - https://www.nic.ch/statistics/dnssec/
- BAKOM / SWITCH DNS Resilience Program
  - https://www.nic.ch/security/resilience/
  - Registrare ohne DNSSEC zahlen mehr

State of the DNSSEC: Signierung



State of the DNSSEC: Validierung

- $\sim 65 - 70\%$ Queries via CH-ISP-Resolver validiert
  - 2019 hat Swisscom auf ihren Resolvern Validierung aktiviert
  - Seitdem ziemlich stagnant
  - https://stats.labs.apnic.net/dnssec/CH
- Die «üblichen Verdächtigen» validieren
  - 1.1.1.1, 8.8.8.8, 9.9.9.9

State of the DNSSEC: KSK Rollover

- 2018: Erster Rollover des ICANN Root KSK

Review of the 2018 DNSSEC KSK Rollover

Some resolver operators do not understand what their resolvers do. [...] They could not determine if they were using automatic updates of the KSK or even if they were using DNSSEC validation.

- https://www.icann.org/review-2018-dnssec-ksk-rollover.pdf

Setup: «Ich will einen validierenden Resolver»

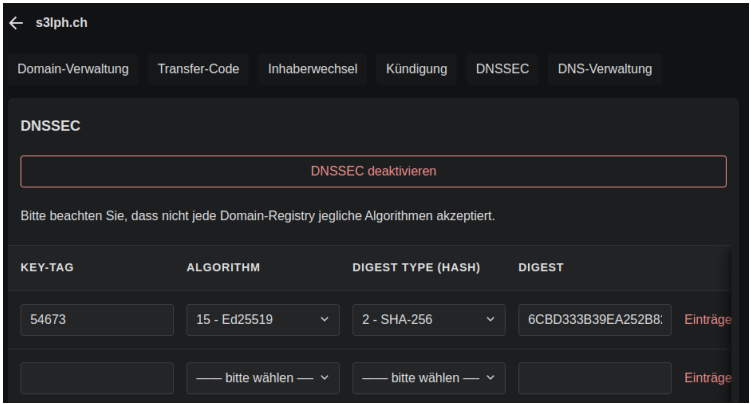
- Existierenden Resolver eintragen
  - **Achtung**: Dem Resolver wird blind vertraut!
- Resolver selber aufsetzen
  - Im lokalen Netzwerk oder auf dem Endgerät
- z.B. unbound
  - https://www.nlnetlabs.nl/projects/unbound/about/
  - Teil vieler Firewall-Distros (OPNSense, pfSense)

Setup: «Ich will meine Domain signieren»

- DNSSEC-fähigen DNS-Anbieter verwenden
- Authoritative DNS-Server selbst betreiben
  - Mindestens 2
  - Statische IP-Adressen
  - Dual Stack!
- z.B. Knot DNS
  - https://www.knot-dns.cz/
  - Automatische Zonen-Signierung
  - Autmatischer ZSK-Rollover
  - Wenig Konfigurationsaufwand

Setup: «Ich will einen DS-Record eintragen»

- Webinterface vom Registrar



- Oder vollautomatisch!

Setup: «Vollautomatisch?»

- RFC 8078 (2017)
- 2 neue RRTypes: **CDS**, (CDNSKEY)
  - «Child DS»
  - Sieht gleich aus wie DS
  - ... aber in der Child Zone
  - `s3lph.ch. CDS 3600 15 2 20082CA13AA7F90891EADF82...`
- Parent sucht nach CDS-Records in Child Zones
- ... und setzt entsprechende DS-Records

Setup: «Vollautomatisch!»

- Die Registry muss das unterstützen
  - CZ.NIC (cz)
  - SWITCH (ch, li)
  - ???
- (... oder der Registrar)
  - domainname.shop
- Authoritativer DNS-Server muss das unterstützen
  - Knot: `cds-cdnskey-publish: always`

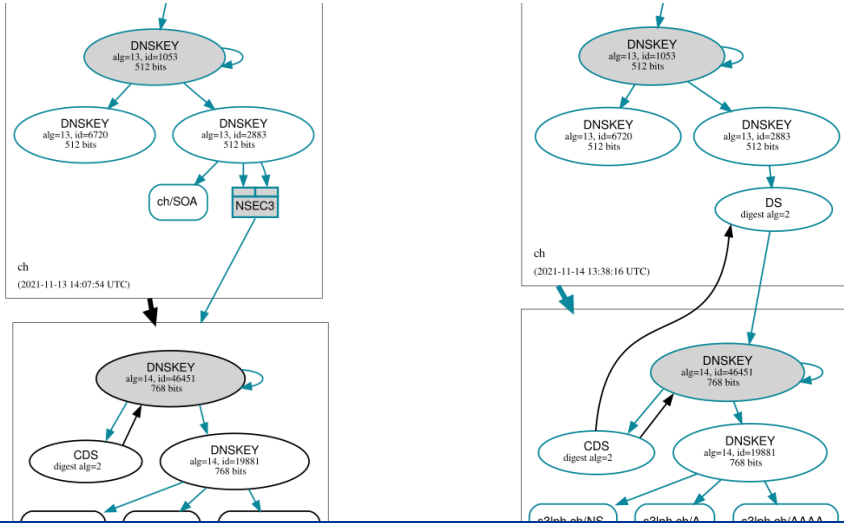
Setup: «Vollautomatisch!»

- Registry definiert Regeln
- Beispiel SWITCH:
  - Chain of Trust muss gültig sein
  - Passender KSK muss vorhanden sein
  - CDS RRSet für 3 Tage unverändert
  - Gleiches CDS RRSet von allen Nameservern
- `https://www.nic.ch/security/cds/`

DNSSEC Bootstrapping

```
zone:
  - domain: s3lph.ch.
    dnssec-signing: on
    dnssec-policy: dnssec-s3lph.ch.

policy:
  - id: dnssec-s3lph.ch.
    algorithm: ed25519
    nsec3: on
    cds-cdnskey-publish: always  # "double-ds" vermeiden
```

DNSSEC Bootstrapping



Automatisierter ZSK-Rollover

```
policy:
  - id: dnssec-s3lph.ch.
    algorithm: ed25519
    nsec3: on
    cds-cdnskey-publish: always

    zsk-lifetime: 30d
```

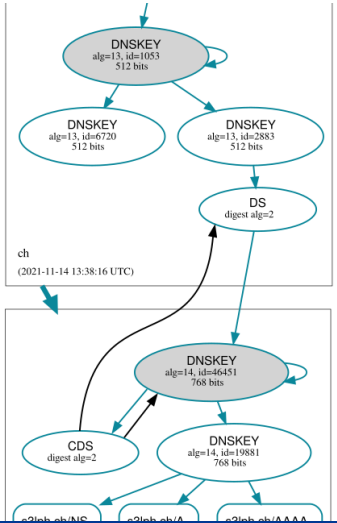
Automatisierter KSK-Rollover

```
policy:
  - id: dnssec-s3lph.ch.
    algorithm: ed25519
    nsec3: on
    cds-cdnskey-publish: always
    zsk-lifetime: 30d

    ksk-lifetime: 180d
    ksk-submission: submission-s3lph.ch.
    propagation-delay: 1h
```

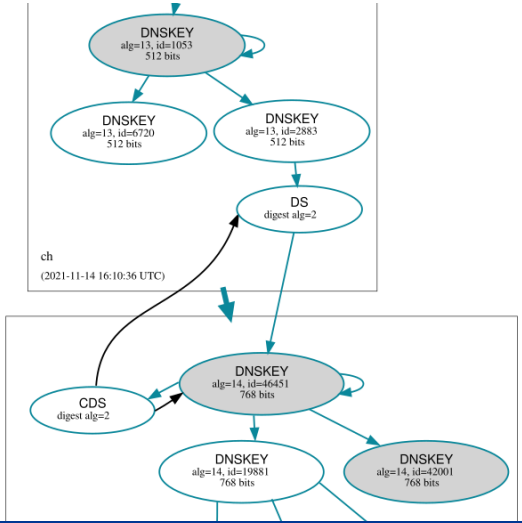
Automatisierter KSK-Rollover

```
submission:
  - id: submission-s3lph.ch.
    check-interval: 1h
    parent: remote-dns.quad9.net

remote:
  - id: remote-dns.quad9.net
    address: "2620:fe::fe"
    address: "2620:fe::9"
    address: "9.9.9.9"
    address: "149.112.112.112"
```

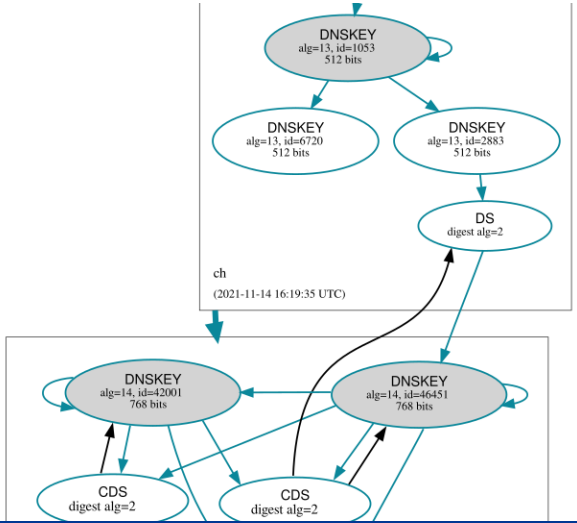
Automatisierter KSK-Rollover



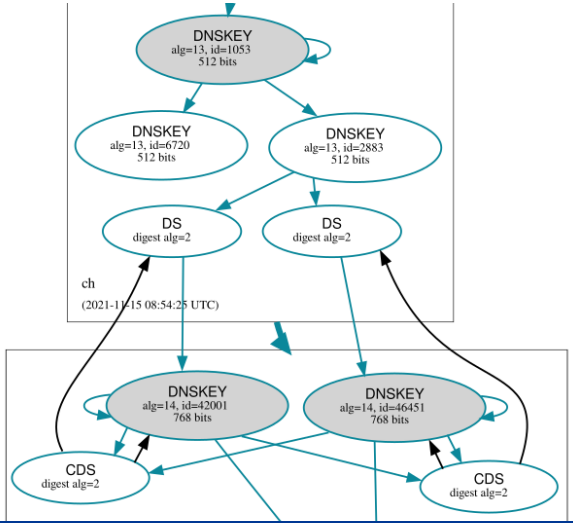
Automatisierter KSK-Rollover



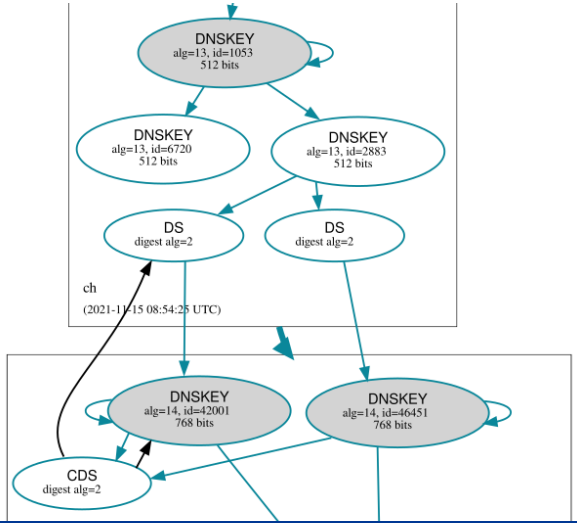
Automatisierter KSK-Rollover



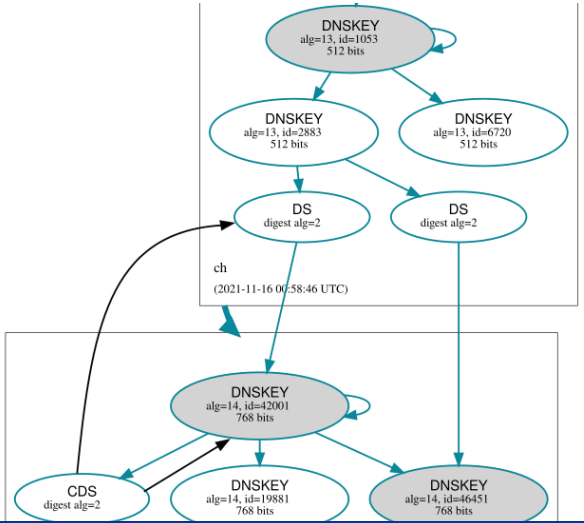
Automatisierter KSK-Rollover



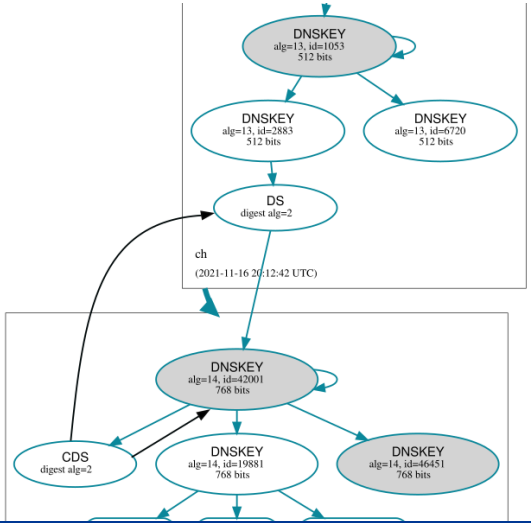
Automatisierter KSK-Rollover



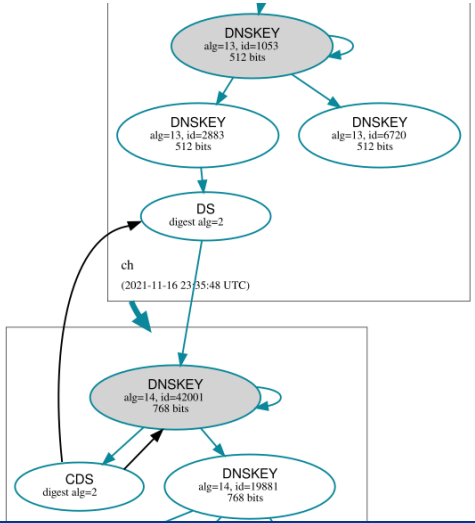
Automatisierter KSK-Rollover



Automatisierter KSK-Rollover



Automatisierter KSK-Rollover



Halbautomatischer KSK-Rollover

- Nur wenige Registries können CDS
- Der grösste Teil ist trotzdem automatisierbar
- Ein einzelner manueller Schritt:
  - CDS → DS
- Monitoring
  - `https://gitlab.com/s3lph/prometheus-dnssec-exporter`

Troubleshooting

- Ungültige Chain of Trust → Zone löst nicht auf
  - Falscher oder fehlender DS-Record
  - Falsche RRSIG
  - Abgelaufene RRSIG
  - Veraltete Algorithmen
- `ch.`-Zone hat eine TTL von 3600
  - neue DS-Records nicht sofort eingetragen
- Kaputtes DNS → alles kaputt

Troubleshooting

- Keys anstarren
  - `keymgr s3lph.ch. list`

```
fe1436 54673 KSK ED25519 pre-active=1655234525 publish=1655238425 ready=1655242325 active=1655429528
43e7e5 59883 ZSK ED25519 publish=1686389225 active=1686393125
5fcc1b 21536 KSK ED25519 publish=1686770525 ready=1686774425
```

- Key-Timestamps modifizieren
  - `keymgr s3lph.ch. set 21536 active=+0`
- KSK-Rollover manuell auslösen
  - `knotc zone-ksk-submitted s3lph.ch.`
  - `knotc zone-key-rollover s3lph.ch. ksk`

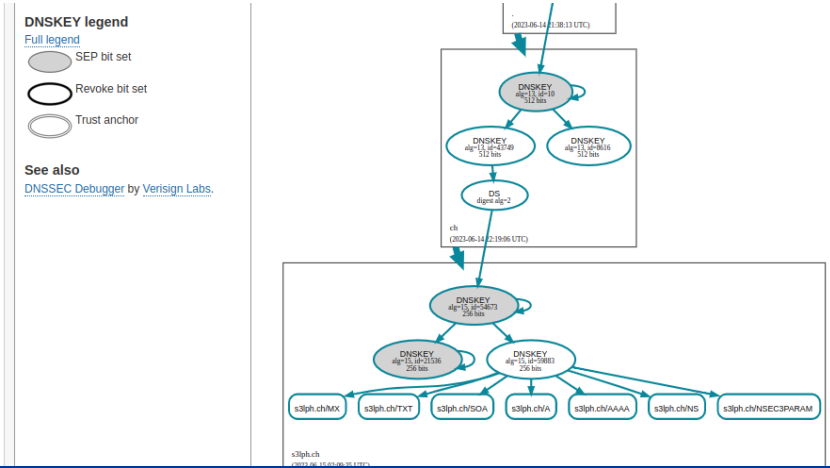
Nützliche Tools: dig

- `dig +dnssec +multi`

```
; <<>> DiG 9.18.15 <<>> +dnssec +multi s3lph.ch dnskey
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28833
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;s3lph.ch.                      IN DNSKEY

;; ANSWER SECTION:
s3lph.ch.               292 IN DNSKEY 256 3 15 (
                               zrxtj9TPFU8YkFz38Yr6Xgzw4UAiRbLqt1mLXcilj0I=
                               ) ; ZSK; alg = ED25519 ; key id = 59883
s3lph.ch.               292 IN DNSKEY 257 3 15 (
                               jHRTmF+YZcoOVDwK90ZpHjHyO1YiB6t2AOpeONRJkao=
                               ) ; KSK; alg = ED25519 ; key id = 21536
s3lph.ch.               292 IN DNSKEY 257 3 15 (
                               sYNO9//iIpczl91X0418Pb4mlQn5tzWSve8ZKsbJLXQ=
```

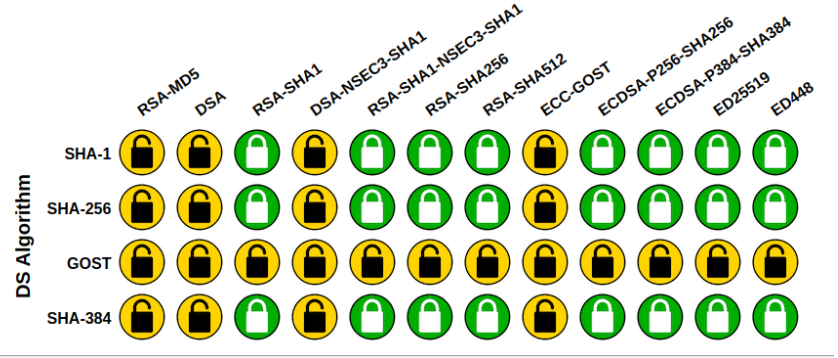
Nützliche Tools: DNSViz

- `https://dnsviz.net`



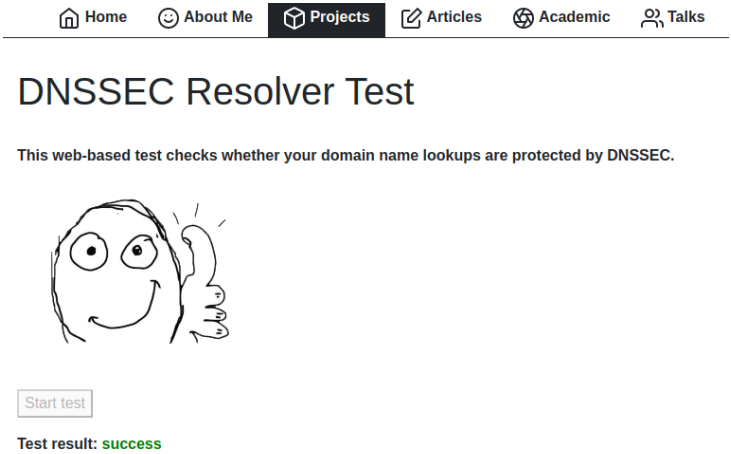
Nützliche Tools: Root Canary Test

- `https://rootcanary.org/test.html`



Nützliche Tools: verteiltesysteme.net

- `https://verteiltesysteme.net/`



Fazit

- DNSSEC-Verbreitung stark zugenommen
- DNSSEC war noch nie so einfach
- Use moar DNSSEC!
- `https://s3lph.me/tag/dnssec.html`

Fragen?

s3lph@s3lph.me

@s3lph@chaos.social

@s3lph:kabelsalat.ch