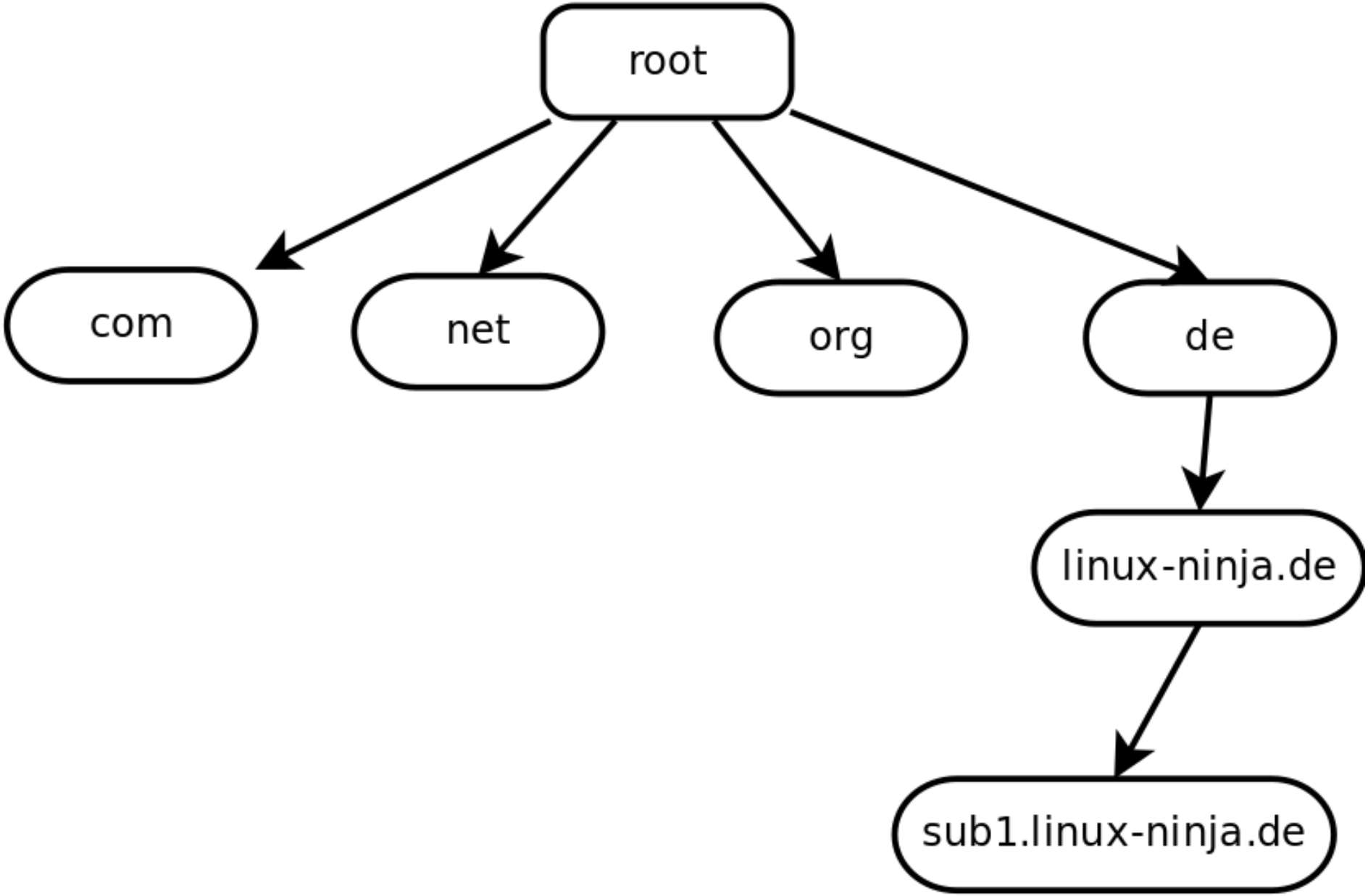
DNSSEC - make DNS more secure

Vortrag LUGOR, 24.02.2020

Ulf Volmer

DNS Overview

- global verteilte Datenbank
- Baumstruktur
- eingebaute Renundanz
- Eintrage werden gecached


root
com
net
org
de
linux-ninja.de
sub1.linux-ninja.de

DNS Records

- primär: Auflösung Name in IP

  A und AAAA Record

- sekundär: Auflösung IP in Name

  PTR Record

- weiterhin: Dienstekonfiguration, Keys, etc.

  NS, MX, SRV, TXT Records

Transport per UDP

schnell, unverschlüsselt

man in the middle

cache poisoning

DNSSEC

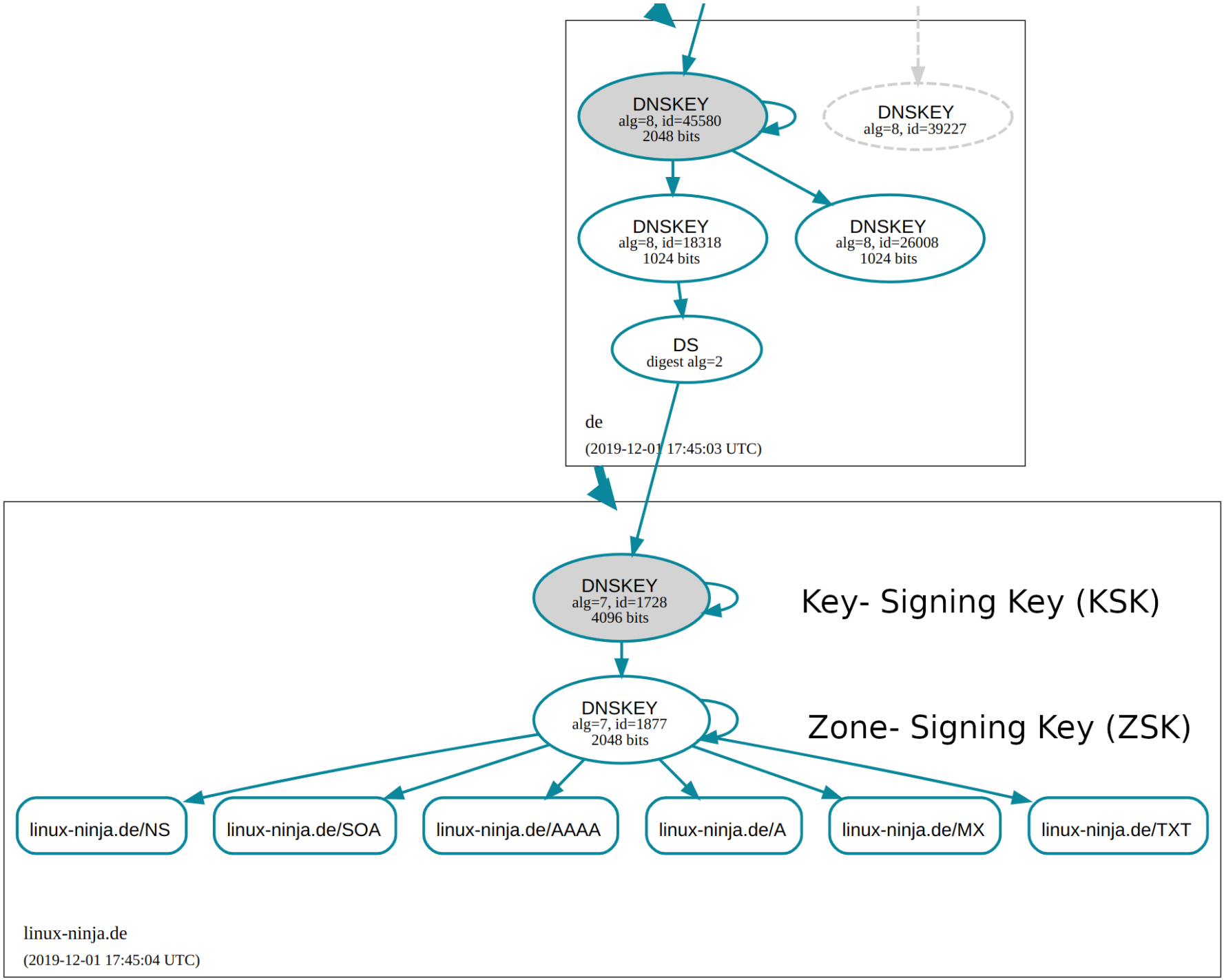
- 2005, RFC 4033 - somit ähnliches Schicksal wie IPv6
- abwärtskompatibel
- auf Basis der Resolver, Clients bleiben außen vor
- bei Fehlern/Manipulationen keine Antwort
- priv/pub Key signiert Records, Pubkey wird in der übergeordneten Zone eingetragen

neue Record Typen

- DNSKEY (public Key, üblicherweise zwei, KSK, ZSK)
- DS (Fingerprint des public Key, Parent Zone)
- RRSIG (Signatur eines Records)
- NSEC(3) (Abwesenheit eines Records)

neuer Record RRSIG, pro Record

```
linux-ninja.de.          2443 IN A 78.47.159.18
linux-ninja.de.          2443 IN RRSIG A 7 2 38400 (
                                 20200310220002 20200209220002
                                 5qmA7aIC77rax3BBsnvaINYcsTtYVb
                                 ykCWOZzCsl0X1GHtxZteeMYEibsTrf
                                 EEeaqGckeGA1NH7GLnkP78rt/XKeP9
                                 iqHUNWnya/ryTV/sR/4VOUwauLMQsC
                                 GKs0/6YQo7Sw3wy9VEEL3h6YJOLyCs
                                 8jFDlz6mWLH0f9kxN+RN7GUvynXsJ+
                                 wkOgJhZhAh3GW59/HMXIwXUAkBur24
                                 fwiJNulCFrs0olDS8vfCoQuYJEYxw/
```


DNSKEY
alg=8, id=45580
2048 bits
DNSKEY
alg=8, id=39227
DNSKEY
alg=8, id=18318
1024 bits
DNSKEY
alg=8, id=26008
1024 bits
DS
digest alg=2
de
(2019-12-01 17:45:03 UTC)
DNSKEY
alg=7, id=1728
4096 bits
Key- Signing Key (KSK)
DNSKEY
alg=7, id=1877
2048 bits
Zone- Signing Key (ZSK)
linux-ninja.de/NS
linux-ninja.de/SOA
linux-ninja.de/AAAA
linux-ninja.de/A
linux-ninja.de/MX
linux-ninja.de/TXT
linux-ninja.de
(2019-12-01 17:45:04 UTC)

Signaturen

- expire, -> cronjob
- KSK: signiert den ZSK, wird upstream hinterlegt
- ZSK: signiert die Zone

```
DOMAIN=linux-ninja.de
cd /etc/named
# zone signing key
dnssec-keygen -a NSEC3RSASHA1 -b 2048 -n ZONE $DOMAIN
# key signing key
dnssec-keygen -f KSK -a NSEC3RSASHA1 -b 4096 -n ZONE $DOMAIN
# DNSKEY records in das Zonfile includen
for key in K${DOMAIN}*.key
do
   echo "\$INCLUDE $key">> ${DOMAIN}.hosts
done
# zonefile signieren, salt ist random
dnssec-signzone -A -3 $(head -c 1000 /dev/random | sha1sum | \
cut -b 1-16) -N INCREMENT -o ${DOMAIN} -t ${DOMAIN}.hosts
# named.conf.local: $DOMAIN.hosts to $DOMAIN.hosts.signed
vim named.conf.local
systemctl reload named
```

Verschlüsselung

- DoH (DNS over HTTPS)
- DoT (DNS over TLS)

beides schick, kein Ersatz, nur Ergänzung zu DNSSEC

DANE

- ermöglicht das Ablegen von TLS Public Keys im DNS
- Vorgaben zur CA im DNS
- somit werden CAs weitgehend obsolete
- derzeit (leider) nur Relevanz bei SMTP

ssh Hostkey Fingerprints im DNS

```
dig -t sshfp jh.linux-ninja.de
cat >> ~/.ssh/config <<EOF
Host jh.linux-ninja.de jh.linux-ninja.net
   VerifyHostKeyDNS yes
EOF
ssh -p 61022 jh.linux-ninja.de
```

SSHFP records werden mit ssh-keygen erzeugt.

Zahlen

- $\sim$ 50% aller Resolver in DE unterstützen DNSSEC
- $\sim$ 1% aller DE- Domains sind DNSSEC validiert

das geht noch was!

Nachteile

- keine Verschlüsselung, ggf. mit DoT kombinieren
- Resolver und Strecke zum Resolver muß vertrauenswürdig sein
- Für Laptops in fremden Netzen bietet sich ein lokaler Resolver (unbound) an

hilfreiche dig Kommandos

```
dig linux-ninja.de
dig -t soa sub3.linux-ninja.de
dig linux-ninja.de +dnssec +multi
dig linux-ninja.de +sigchase
dig linux-ninja.de +sigchase +trace
dig dnssec-failed.org +cdflag @::1
```

hilfreiche Online- Tools

- https://dnsviz.net/
- https://zonemaster.net
- http://dnssec-debugger.verisignlabs.com/

Dankeschön für die Aufmerksamkeit

- Mail u.volmer@u-v.de
- Matrix: @uvolmer:matrix.u-v.de
- XMPP: ulf@jabber.u-v.de
- https://u-v.de/DNSSEC/