Fragen und Antworten zu DNSSEC & DANE

Sven Duscha und Bernhard Schmidt

Zeitplan - Mittwoch, 8.November

- 10:00 - 11:00 Kaffee und Begrüßung
- 11:00 - 11:30 DNSSEC und DANE am LRZ
- 11:30 - 12:00 Best practices zur Einführung
- 12:00 - 13:00 Fragen-Session 1
- 13:00 - 14:00 Mittagessen
- 14:00 - 15:00 Fragen-Session 2, Demos
- 15:00 - 15:20 Kaffee
- 15:20 - 16:45 Erfahrungsaustausch, FAQs
- 16:45 - 17:00 Abschluss
- ~17:00 Ende

Fragen zu DNSSEC & DANE am LRZ

Kurze Vorstellungsrunde

- Name, Universität / Hochschule
- schon erste eigene Versuche mit DNSSEC?

DNSSEC am LRZ

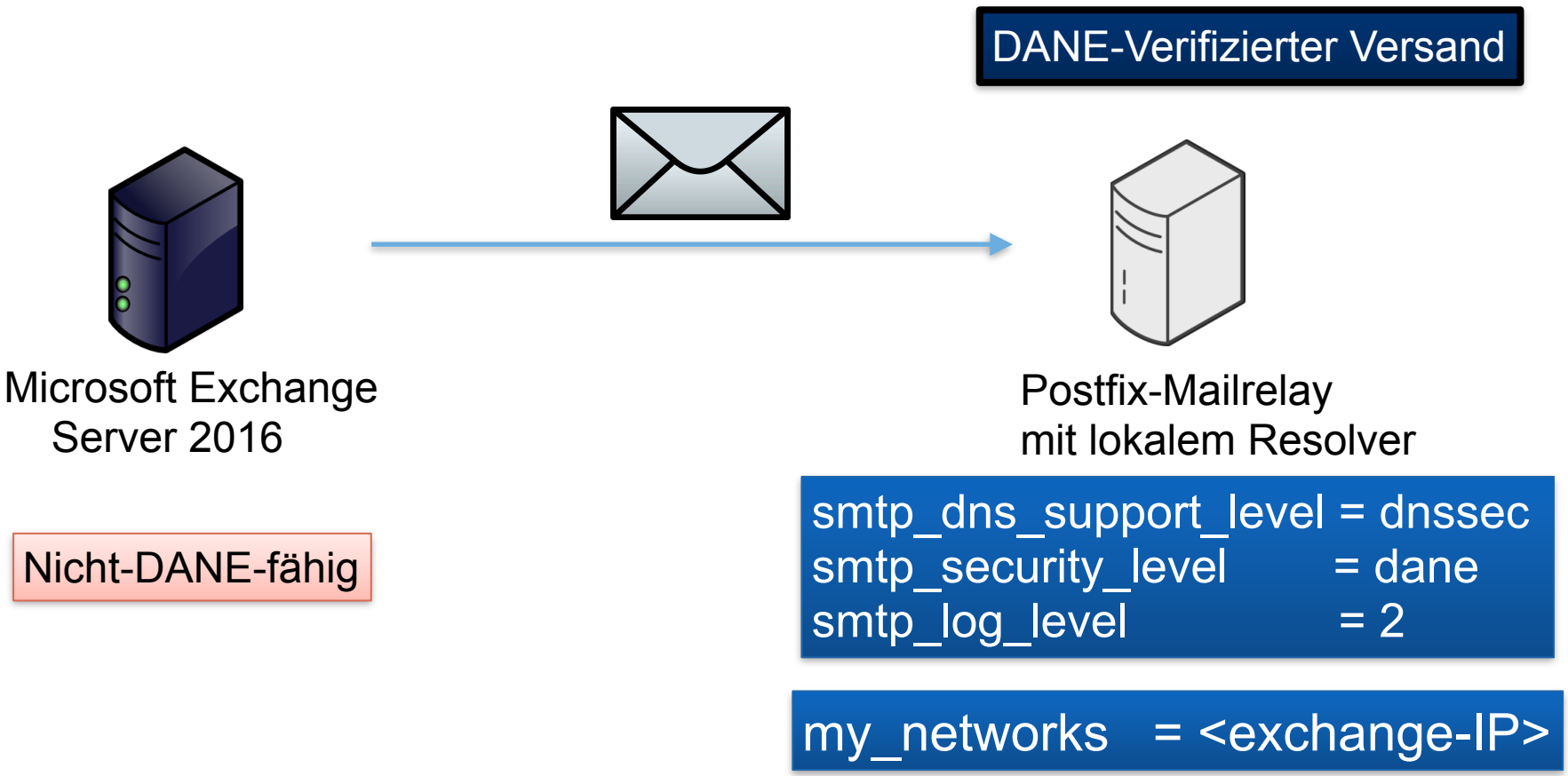
- seit **2015**, badw.de als Versuchsdomain
- 153 signierte Zonen
  von insgesamt 3183 Zonen
  davon 1103 reverse Zonen
- „Signing Proxy“ auf einer VM
- Schlüssel ZSK/KSK pro Zone, in jeweiligen Verzeichnissen
- „key-rolling“ nach Bedarf, kein strikter Zeitplan
- daher kein key-Expiration tag

DANE am LRZ

- seit **2014 outbound DANE** (benötigt kein DNSSEC)
  postout.lrz.de und mailout.lrz.de
- **inbound DANE seit 2015**
  postrelay1.lrz.de und postrelay2.lrz.de
- entsprechende TLSA-Einträge
- Hash des „public key“ mit dem das Zertifikat unterschrieben ist
  → kein Erneuern des TLSA-RR wenn Zertifikat gewechselt wird

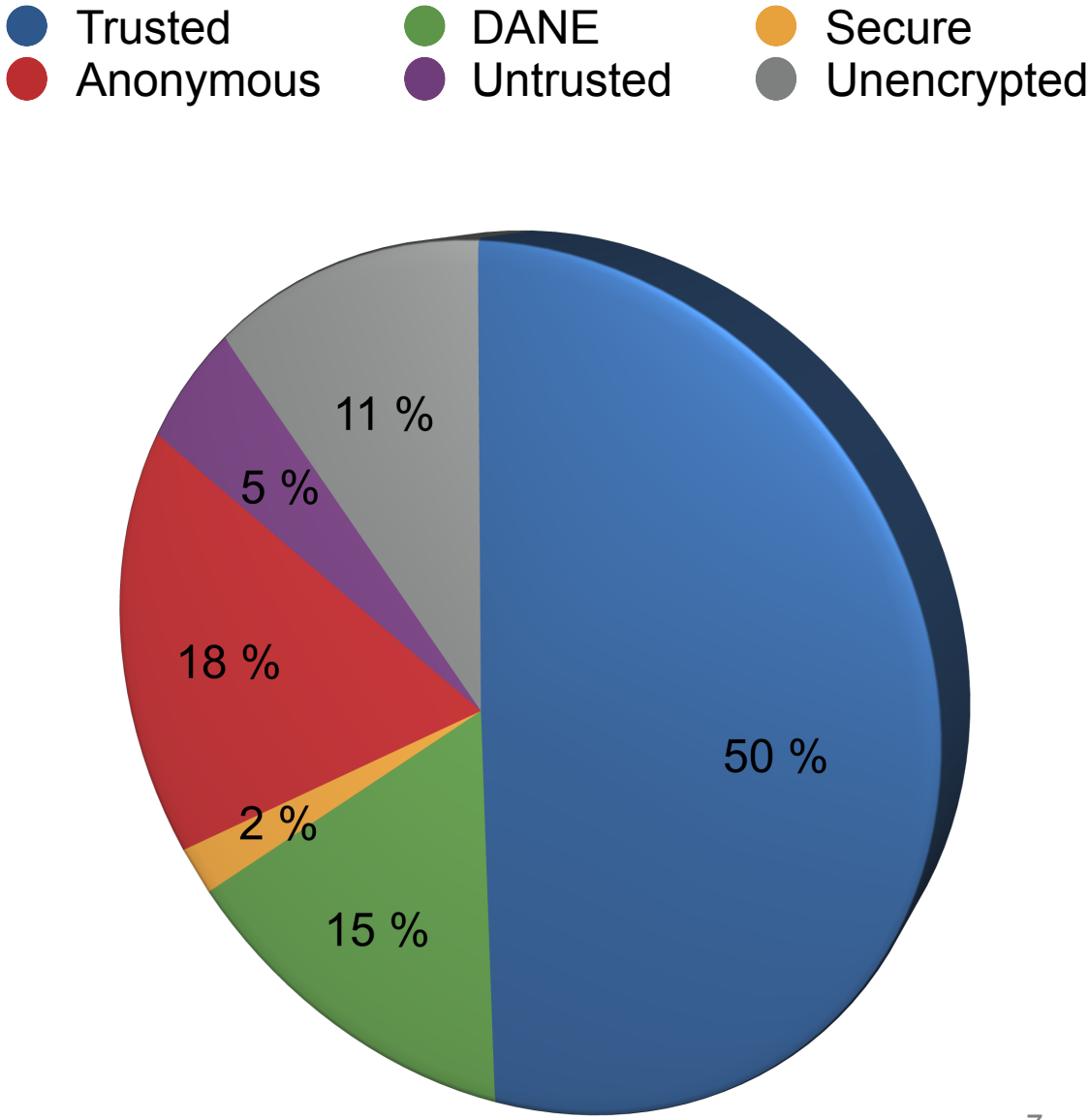
Postfix 2.11 Mailrelay als Ausgangsmailserver

- Für ausgehendes DANE muss der Mailserver die Überprüfung des TLSA-Records unterstützen



DANE - grobe Statistik

LRZ Ausgangsmailserver
Mailout und Postout:

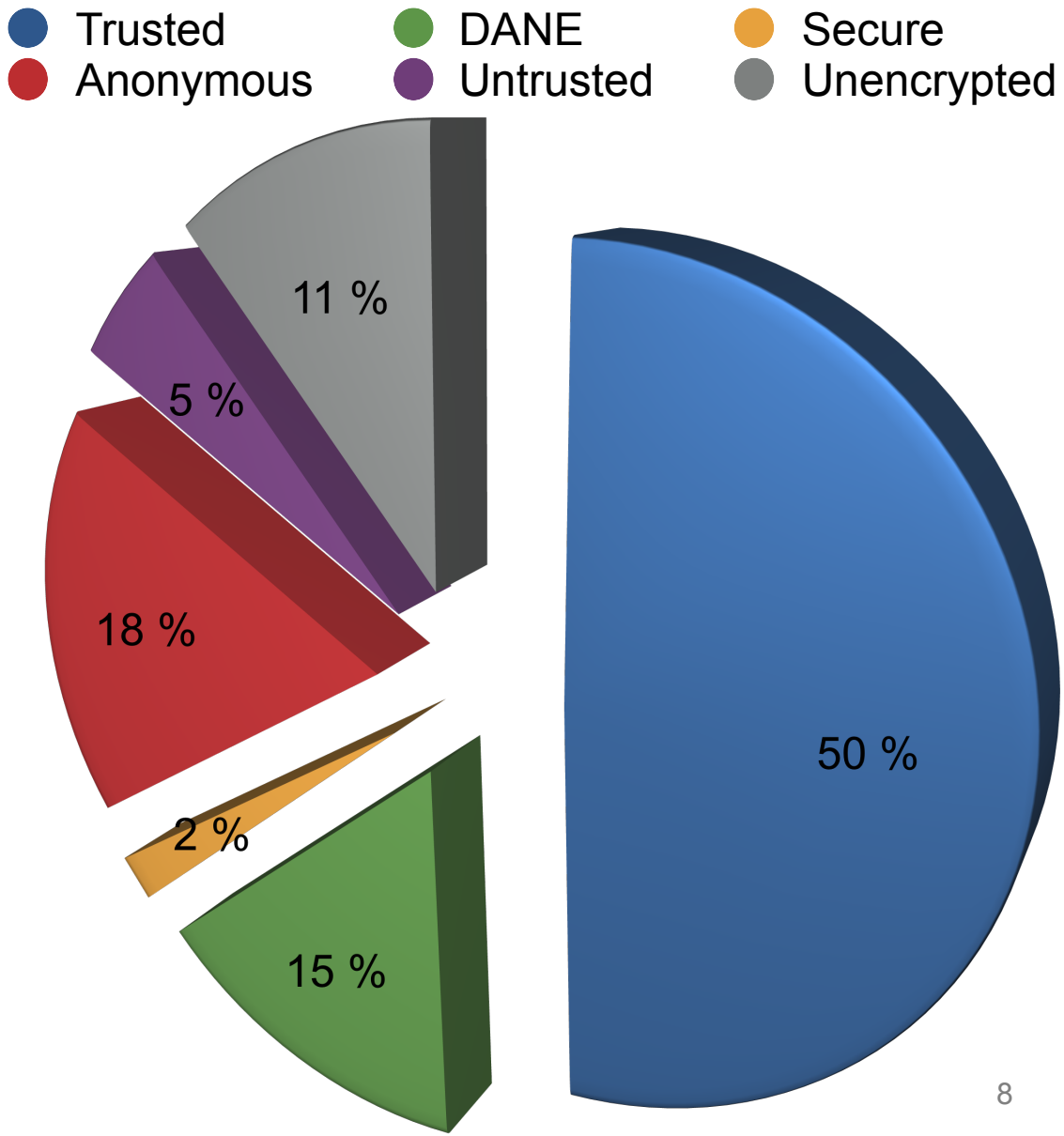


- ~15% DANE-verifiziert
- ~50% trusted TLS
- ~ 2% secure
- ~18% anonymous
- ~ 5% untrusted TLS
- ~11% No encryption

DANE - grobe Statistik

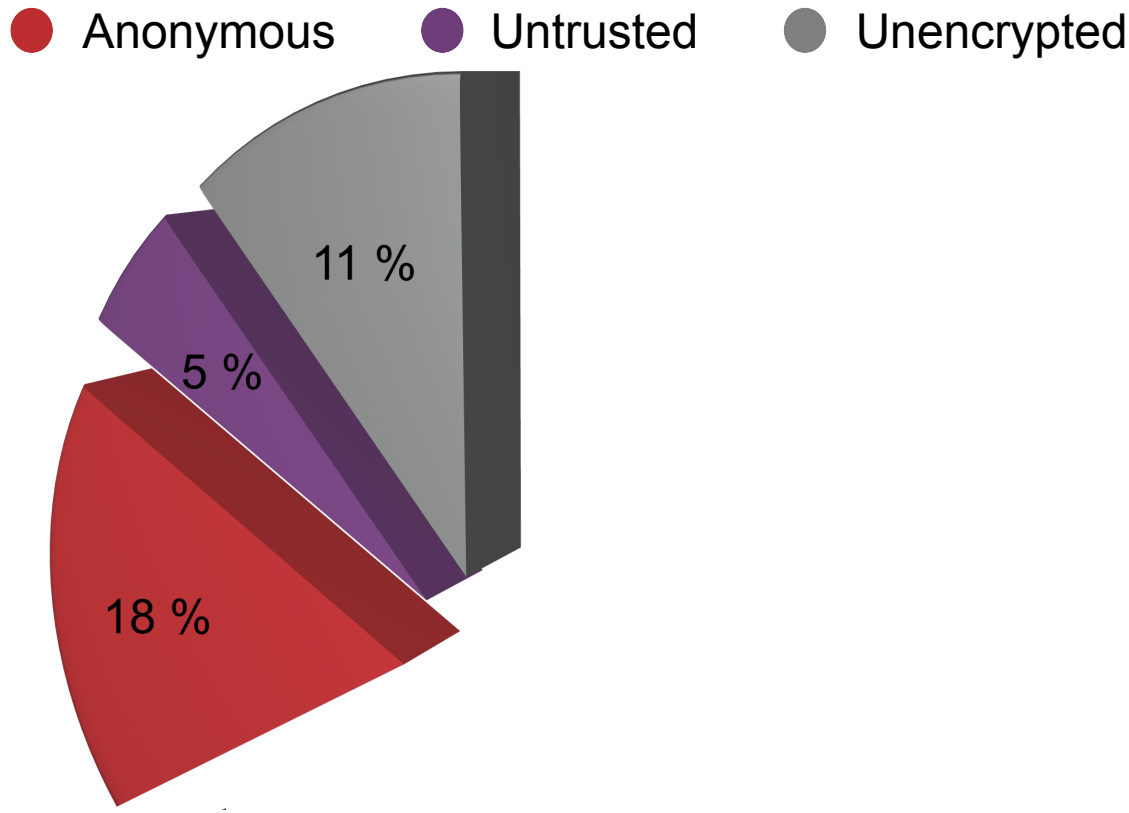
LRZ Ausgangsmailserver
Mailout und Postout:

- ~15% DANE-verifiziert
- ~50% trusted TLS
- ~ 2% secure
- ~18% anonymous
- ~ 5% untrusted TLS
- ~11% No encryption



DANE - grobe Statistik

LRZ Ausgangsmailserver
Mailout und Postout:



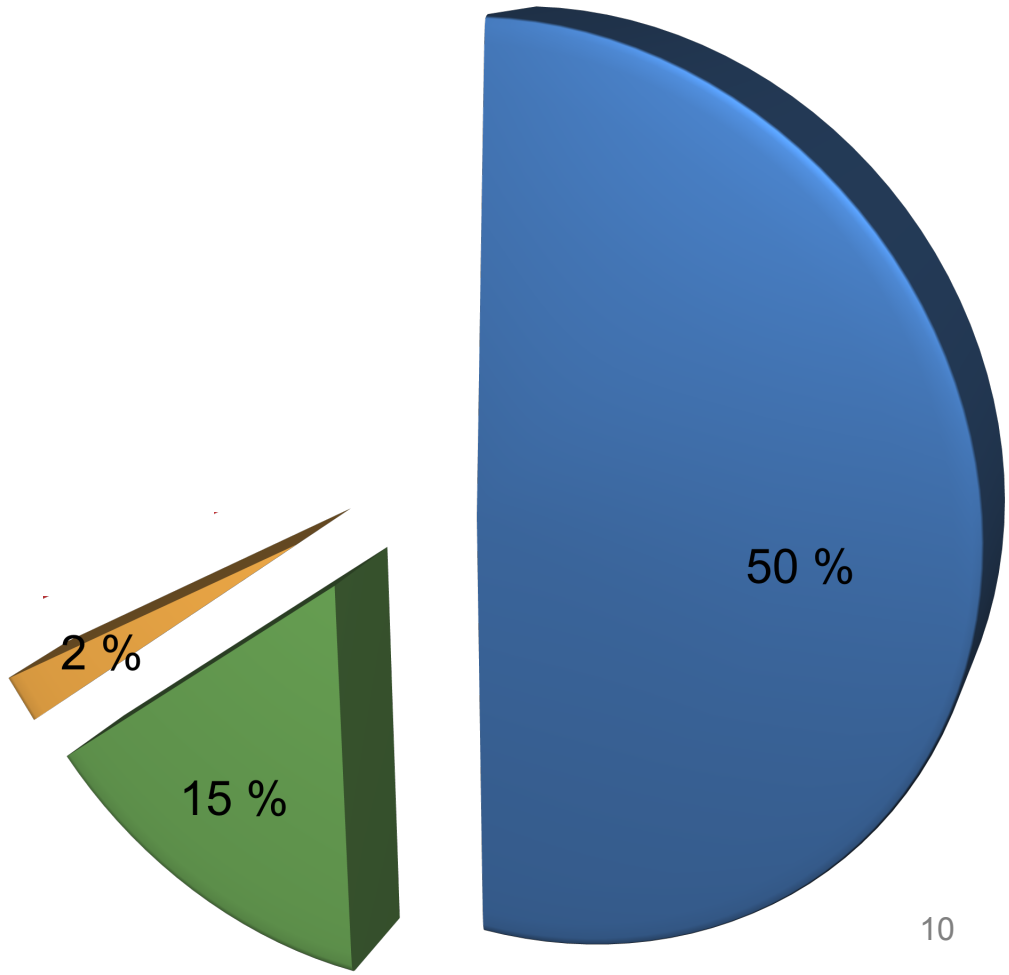
- ~18% anonymous
- ~ 5% untrusted
- ~11% No encryption

= 34% unsichere Verbindungen

DANE - grobe Statistik

LRZ Ausgangsmailserver
Mailout und Postout:

- ~15% DANE-verifiziert
- ~50% trusted TLS
- ~ 2% secure



= 67% sichere Verbindungen

DANE - Statistik nach Mailempfänger

Statistik über einen Zeitraum von vier Tagen

GMX	3486
web.de	2152
Bayerische Staatsregierung	468
Posteo	143
Freenet	140
FAU Erlangen	78
LMU Physik	55
UD Media	40
mail.de	39
Mediabeam (xworks.net)	38
Ruhr-Uni Bochum	37
Bundesregierung	31
Universität Kiel	19
Technische Hochschule Nürnberg	12
Hochschule Augsburg	10

DANE - Statistik nach Mailempfänger

Statistik über einen Zeitraum von vier Tagen

GMX	3486
web.de	2152
Bayerische Staatsregierung	468
Posteo	143
Freenet	140
FAU Erlangen	78
LMU Physik	55
UD Media	40
mail.de	39
Mediabeam (xworks.net)	38
Ruhr-Uni Bochum	37
Bundesregierung	31
Universität Kiel	19
Technische Hochschule Nürnberg	12
Hochschule Augsburg	10

DANE - Statistik nach Mailempfänger

Statistik über einen Zeitraum von vier Tagen

GMX	3486
web.de	2152
Bayerische Staatsregierung	468
Posteo	143
Freenet	140
FAU Erlangen	78
LMU Physik	55
UD Media	40
mail.de	39
Mediabeam (xworks.net)	38
Ruhr-Uni Bochum	37
Bundesregierung	31
Universität Kiel	19
Technische Hochschule Nürnberg	12
Hochschule Augsburg	10

DANE - Statistik nach Mailempfänger

Statistik über einen Zeitraum von vier Tagen

GMX	3486
web.de	2152
Bayerische Staatsregierung	468
Posteo	143
Freenet	140
FAU Erlangen	78
LMU Physik	55
UD Media	40
mail.de	39
Mediabeam (xworks.net)	38
Ruhr-Uni Bochum	37
Bundesregierung	31
Universität Kiel	19
Technische Hochschule Nürnberg	12
Hochschule Augsburg	10

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Best practices zur Einführung von DNSSEC und DANE

Testdomain zum Ausprobieren

- ungenutzte Domain
- oder „Typo“-Domain
- Registrar muss DNSSEC unterstützen (KSK in Parentzone)
- muss Second-Level-Domain sein, weil alle Zonen in der Hierarchie DNSSEC-gesichert sein müssen
  bla.hochschule.de **geht nicht!**
  hoschule.de **geht**

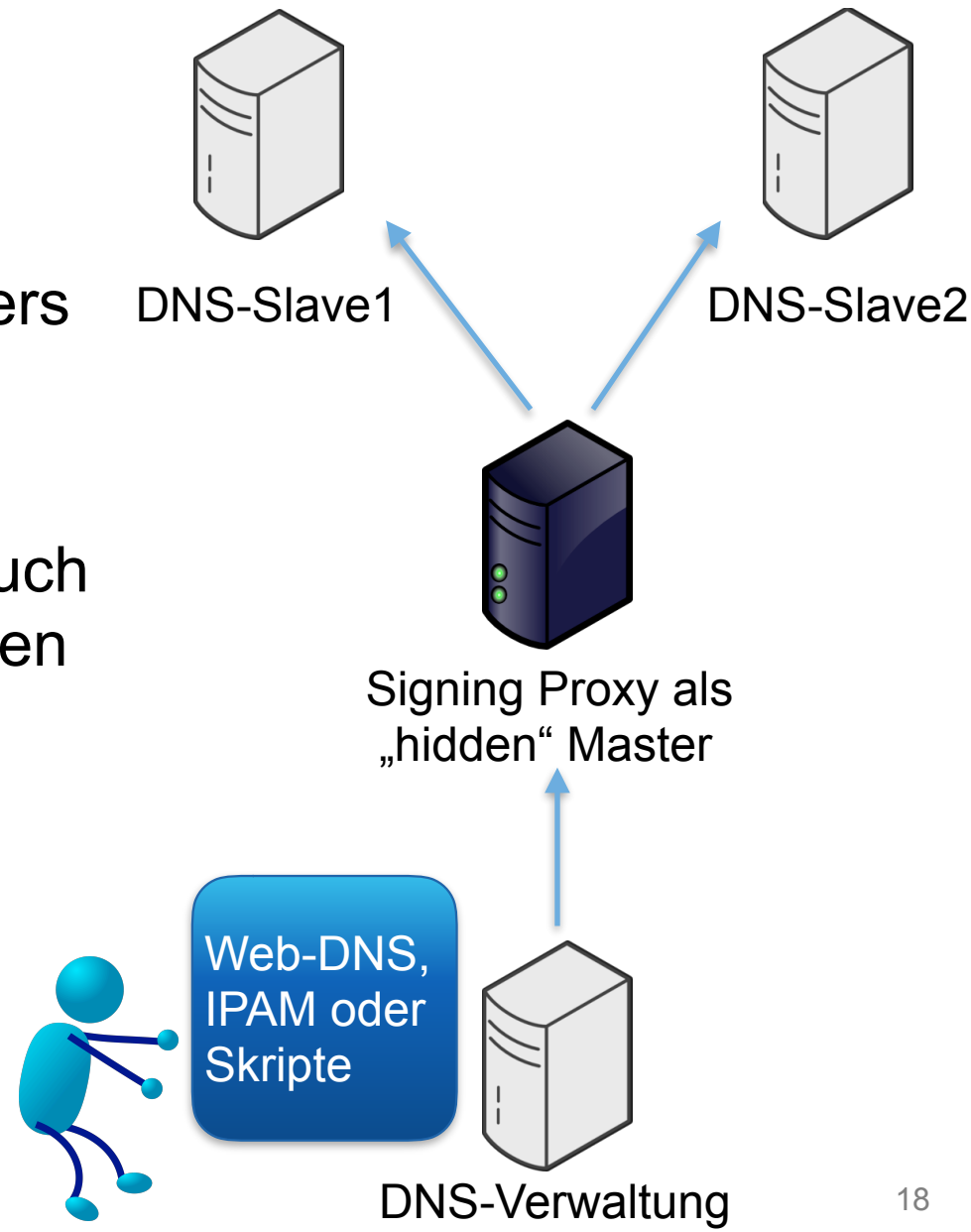
Publizieren und key rollover

- **erst** Zone auf dem Nameserver signieren
- **dann** KSK in der Parentzone, .de., veröffentlichen
- **Key rollover** probieren
  „pre-publish“ Zeiten einhalten
  KSK „double signature“

Signing-Proxy

sichtbar im Internet, NS-Einträge

- virtuell oder physisch
- ntp-Zeitkorrektur für TSIG-transfers
- BIND9
- BIND-9.11 bringt dnssec-keymgr
- dnssec-keymgr lässt sich aber auch auf älterem BIND >=9.9 installieren
- Integration in bestehende DNS-Verwaltung
- über Zonen-Transfers



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Key rollovers - ZSK und KSK

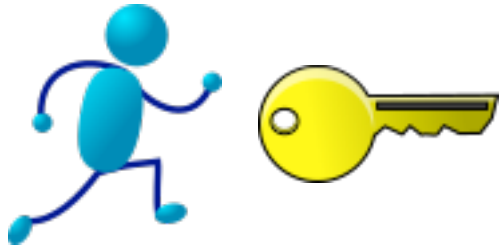
key rollover - allgemein

- sollten gemacht werden
- Schlüssel können kompromittiert werden
- kein fester Zeitrahmen nötig
- Verfahren müssen aber sitzen - daher üben!
- stand-by DNSKEYs für den Notfall
- TTLs der caching Resolver beachten
  mindestens 24 Stunden Vorlauf

Zone-signing key (ZSK) rollover

- relativ schmerzlos
- neuer ZSK mit entsprechenden „publish“ und „activate“ Zeitstempeln („tags“)
- neuen ZSK im Schlüsselverzeichnis zur Verfügung stellen, BIND9 erledigt den Rest (pre-publish, signieren usw.) gemäß „tags“
- empfohlene Methode: pre-publish

Key-signing key (KSK) rollover



- etwas schwieriger, da „out-of-band“ Kommunikation mit der Parentzone
- Veröffentlichen des KSK als DS in der Parentzone
- empfohlen: double signature
- TTL beachten

Pre-publish Methode

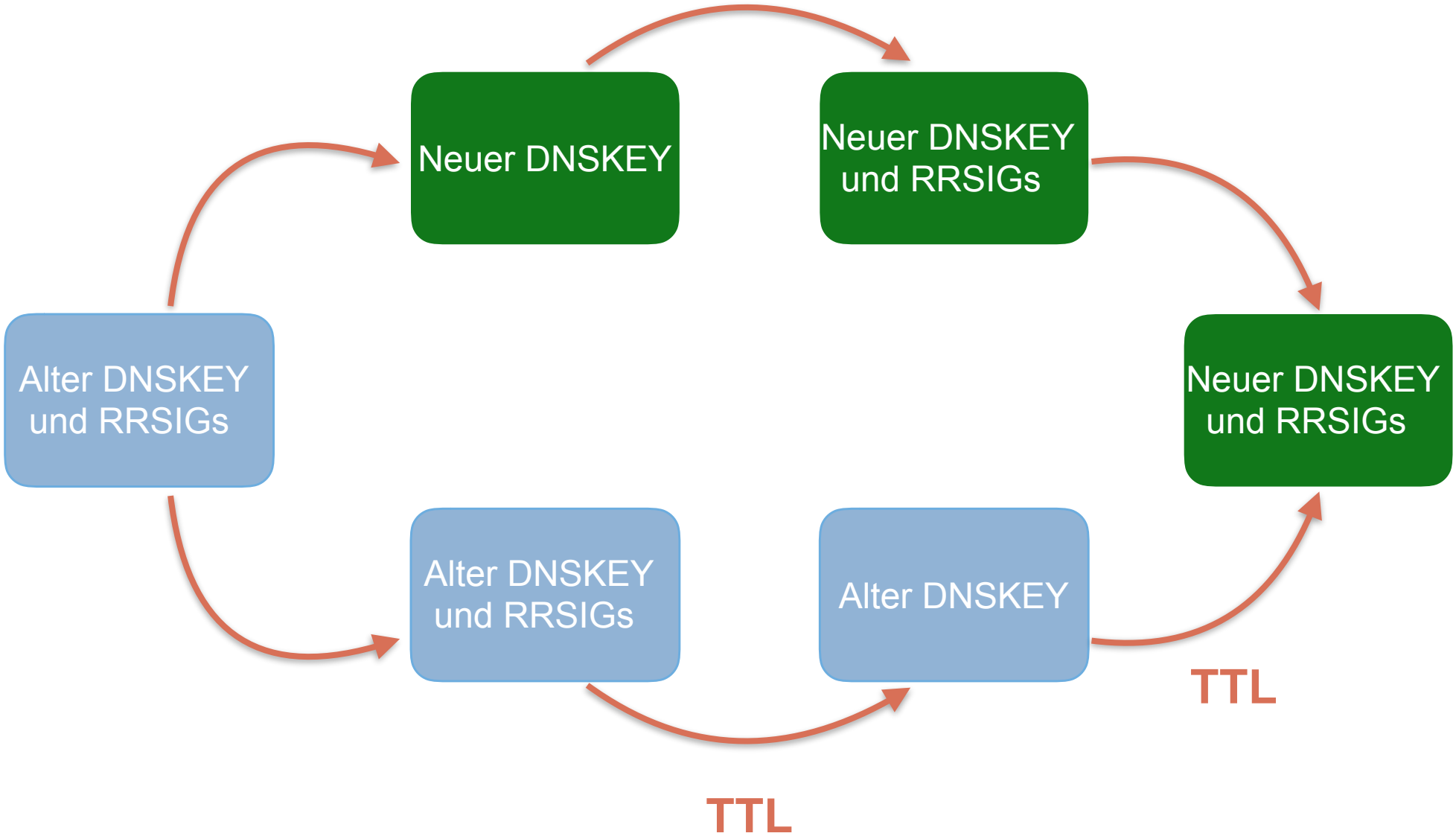


Bild: RIPE NCC

Double Signature Methode

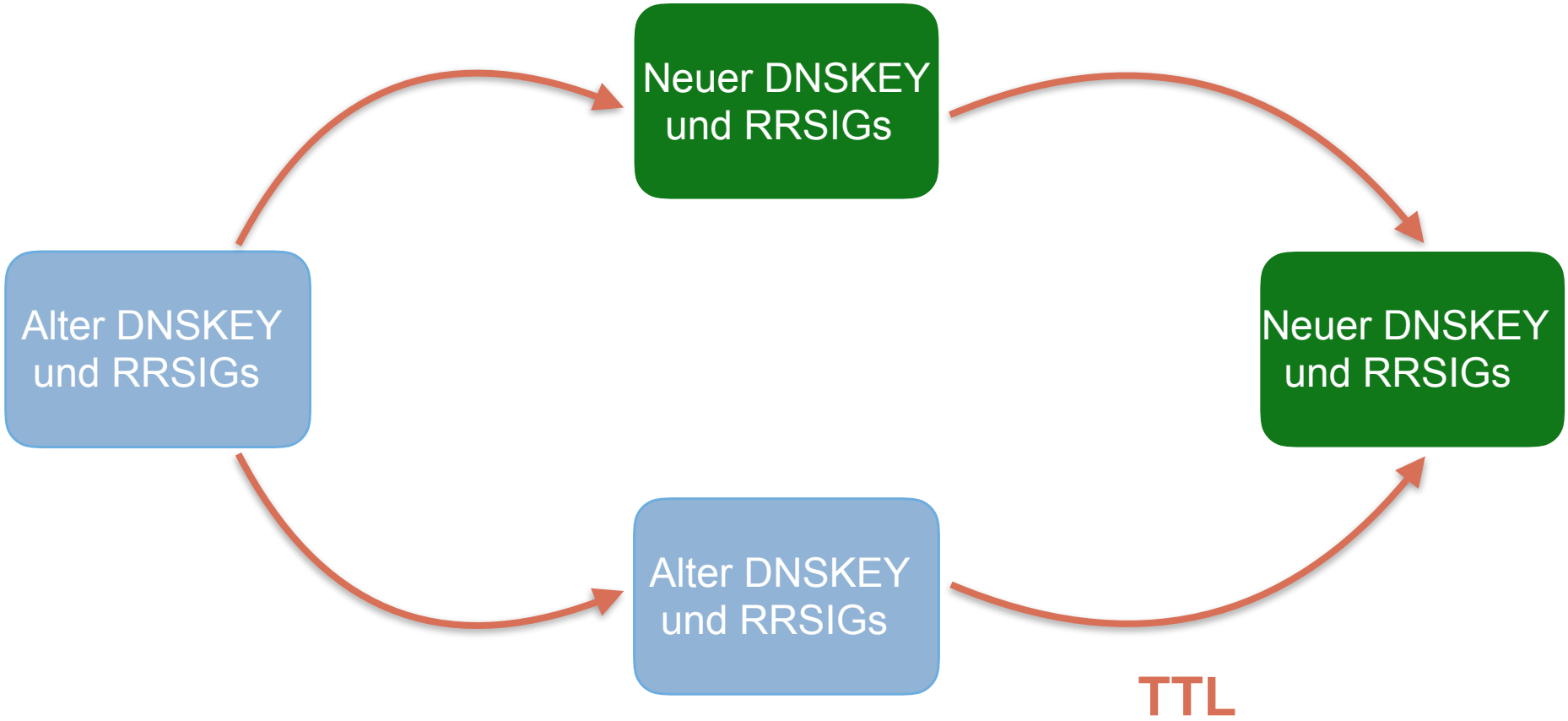


Bild: RIPE NCC

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

DNSSEC und DANE überprüfen

Überprüfung der Konfiguration mit lokalen Skripten

- **named-checkconf** …
  überprüft BIND-Konfiguration
- **named-checkzone** …
  überprüft auf allgemeine DNS Fehler
- **dnssec-verify** oder **ldns-verify-zone (ldns-Tools)** …
  überprüft auf DNSSEC-spezifische Fehler
- **dig axfr** …
  Zonentransfer liefert die korrekte signierte Zone aus?
- **dig DS** …
  welcher KSK ist in der Parentzone aktuell?

Fertige Checkskripte (Nagios/Icinga2-kompatibel) finden sich im DNSSEC-Wiki.

Überprüfen über externe Resolver

- EDSN0-Protokoll: **AA** (Authoritative Answer) und **AD** (Authenticated Data) Flag schließen sich gegenseitig aus
- daher externer Resolver notwendig
- Sichtbarkeit für Benutzer wird überprüft
- Google: 8.8.8.8 8.8.4.4
  OARC: 184.105.193.73 184.105.193.74

AA und AD flag

```
; <<>> DiG 9.11.0-P1 <<>> lrz.de @resolver1.lrz.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45149
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 7
```

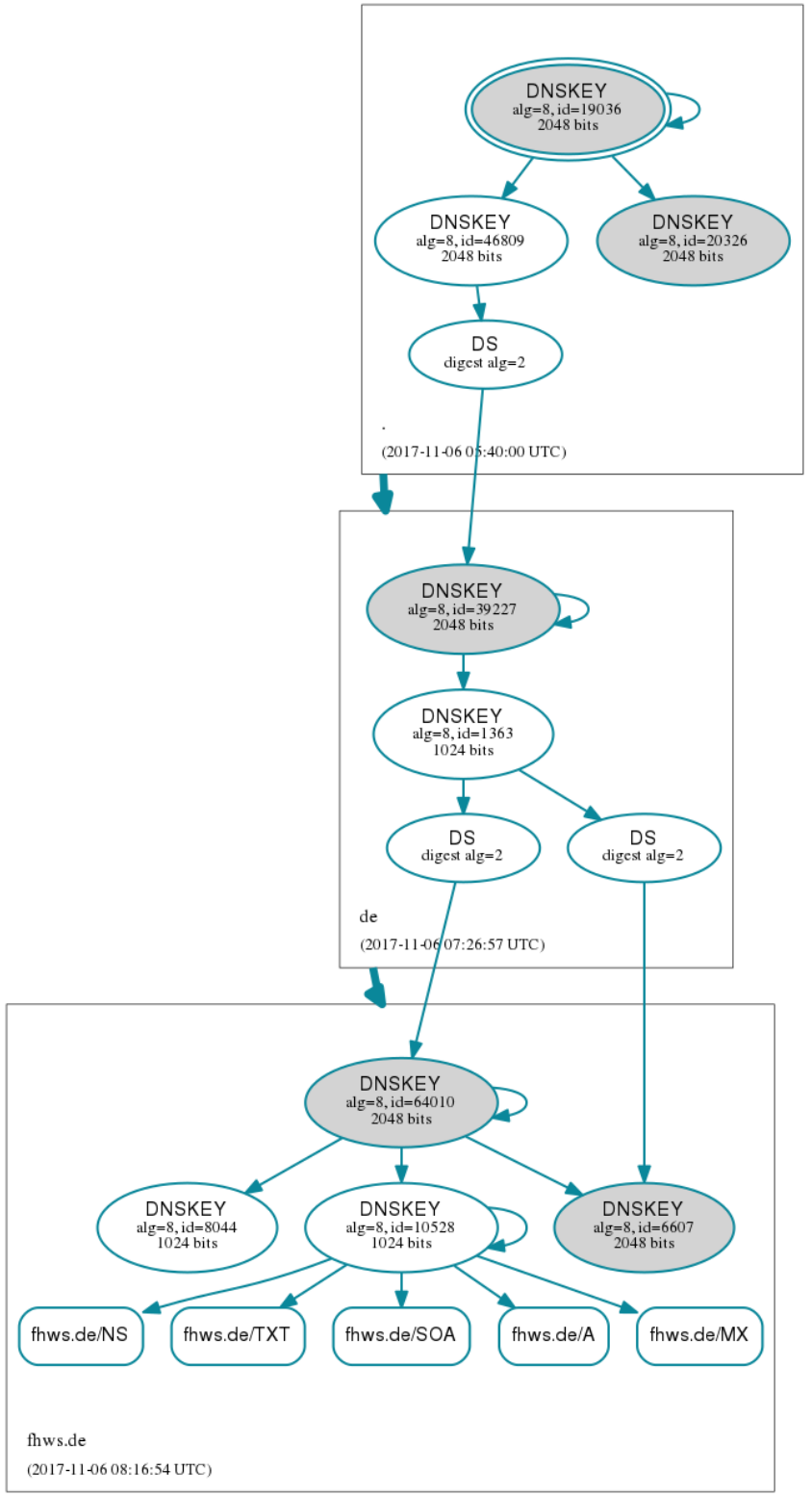
Autoritative Answer bei lokalem Resolver

```
; <<>> DiG 9.11.0-P1 <<>> lrz.de @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1658
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

Authenticated Data bei externem Resolver

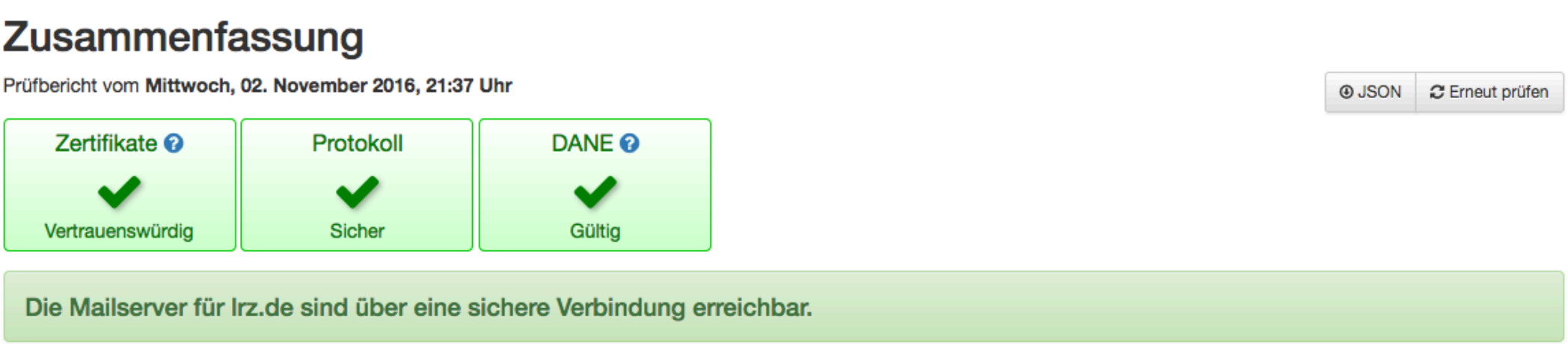
DNSViz

- DNSViz erlaubt eine graphische Überprüfung der DNSSEC-Kette
- DS-Fehler erkennbar
- welche Schlüssel sind publiziert? Aktiv?
- auch als Skript lokal nutzbar



DANE überprüfen

- dig -t TLSA _25._tcp.mailserver.domain.de
- check_dane.py Testskript
- dane.sys4.de Validator und de.ssl-tools.net



de.ssl-tools.net/mailservers/lrz.de

Server

eingehende Mails

Diese Server nehmen E-Mails für **@lrz.de**-Adressen entgegen.

Hostname / IP-Adresse	Priorität	STARTTLS	Zertifikate	Protokoll			
postrelay2.lrz.de 2001:4ca0::103:0:25:1:2	100	unterstützt ✔	postrelay2.lrz.de ✔	**DANE** ✔ gültig **PFS** ✔ unterstützt **Heartbleed** ✔ nicht verwundbar **Schwache Algorithmen** ✔ nicht gefunden		TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	02.11.2016 11.0 s
postrelay2.lrz.de 129.187.254.159	100	unterstützt ✔	postrelay2.lrz.de ✔	**DANE** ✔ gültig **PFS** ✔ unterstützt **Heartbleed** ✔ nicht verwundbar **Schwache Algorithmen** ✔ nicht gefunden		TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	02.11.2016 11.0 s
postrelay1.lrz.de 2001:4ca0::103:0:25:1:1	100	unterstützt ✔	postrelay1.lrz.de ✔	**DANE** ✔ gültig **PFS** ✔ unterstützt **Heartbleed** ✔ nicht verwundbar **Schwache Algorithmen** ✔ nicht gefunden		TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	02.11.2016 11.0 s
postrelay1.lrz.de 129.187.254.158	100	unterstützt ✔	postrelay1.lrz.de ✔	**DANE** ✔ gültig **PFS** ✔ unterstützt **Heartbleed** ✔ nicht verwundbar **Schwache Algorithmen** ✔ nicht gefunden		TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	02.11.2016 11.0 s

DANE https://www.huque.com/dane/testsite/

https://good.dane.huque.com/
TLSA record name: **_443._tcp.good.dane.huque.com.**
There is a valid signed TLSA record (DANE-EE) matching the server certificate at this site.
https://badhash.dane.huque.com/
TLSA record name: **_443._tcp.badhash.dane.huque.com.**
The signed TLSA record (DANE-EE) contains a hash value that doesn't match the server certificate.
https://badparam.dane.huque.com/
TLSA record name: **_443._tcp.badparam.dane.huque.com.**
The signed TLSA record contains invalid (unusable) TLSA parameters.
https://badsig.busted.huque.com/
TLSA record name: **_443._tcp.badsig.busted.huque.com.**
The TLSA record has an incorrect DNSSEC signature.
https://expiredsig.busted.huque.com/
TLSA record name: **_443._tcp.expiredsig.busted.huque.com.**
The TLSA record has an expired DNSSEC signature.
https://good-pkixta.dane.huque.com/
TLSA record name: **_443._tcp.good-pkixta.dane.huque.com.**
The TLSA record (PKIX-TA) has a hash value that correctly matches the PKIX root CA issuer in the server certificate chain.
https://bad-pkixta.dane.huque.com/
TLSA record name: **_443._tcp.bad-pkixta.dane.huque.com.**
The TLSA record (PKIX-TA) has a hash value that doesn't match any certificate issuer in the PKIX chain corresponding to the server certificate.

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

dnssec-keymgr

BIND 9.11 führt dnssec-keymgr ein

- Policy mit Richtlinien zur Schlüsselerzeugung
- Allgemein und pro Zone definierbar
- Algorithmus, Bit-Länge, TTL
- Rollperiod, Prepublish und Postpublish-Zeiten definierbar
- Stand-by keys
- Coverage legt Vorhaltezeitraum fest, für den Schlüssel erzeugt werden

dnssec-keymgr mit BIND 9.9.x

- dnssec-keymgr ist rein in Python implementiert
- Aufruf dient nur der Erzeugung von Schlüsseln, anhand der Meta-Daten vorhandener Schlüssel
- unabhängig von kompilierter BIND-Instanz (**funktioniert in 9.9.x**)
- regelmäßiger Aufruf mit cron-job erzeugt Schlüssel nur bei Bedarf
- damit immer gültige ZSK ohne Admin-Interaktion
- **nicht für KSK wegen „out-of-band“ Kommunikation**

Beispiel Policy-Datei: /etc/dnssec-policy.conf

```
policy default {

        algorithm RSASHA256;
        directory "/var/bind/keys";

        keyttl 10d;
        key-size ksk 2048;
        key-size zsk 2048;

        roll-period zsk 6mo;
        standby ksk 1;
        standby zsk 1;

        pre-publish zsk 20d;
        post-publish zsk 20d;
        pre-publish ksk 60d;
        post-publish ksk 60d;

        coverage 2y;
};

zone ws01.ws.dnssec.bayern {
        policy default;
};
```

Policies definieren Parametersets, die auf Zonen angewendet werden können

z.B. algorithm und key-directory

Schlüssel TTL in der Zone und Schlüssellängen in Bit für KSK und ZSK

Rolling des ZSK, Periode

Anzahl Standby-keys für KSK und ZSK

pre- und postpublish Zeiten für ZSK

pre- und postpublish Zeiten für KSK

Zeitraum, für den Schlüssel vorgehalten werden

wende policy „default“ für diese Zone an

dnssec-keymgr-Aufruf

- dnssec-keymgr muss immer noch regelmäßig aufgerufen werden
- überprüft vorhandene Schlüssel und deren Gültigkeit, erzeugt neue, wenn nötig

  dnssec-keymgr [Zonenname]

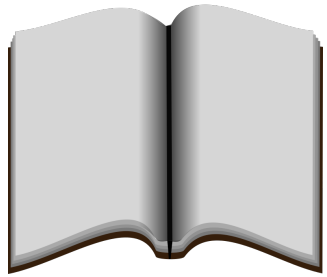
- Ohne Zonennamen, Schlüssel für alle Zonen in Policy-File erzeugen
- Kann leicht als cron-job laufen

  crontab –e

  0 */1 * * * /usr/local/sbin/dnssec-keymgr > /var/log/keymgr.log


lrz
Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften
Weitere Informationsquellen & Fragen

Nützliche Ressourcen - Anleitungen



- DNSSEC HowTo - A tutorial in disguise
  https://www.nlnetlabs.nl/publications/dnssec_howto/dnssec_howto.pdf
- BIND DNSSEC Guide
  https://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html
- BIND Automatic Signing
  http://www.average.org/dnssec/dnssec-configuring-auto-signed-dynamic-zones.txt
- White paper Deploying DNSSEC
  https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf
- Heise Artikel http://www.heise.de/netze/artikel/Transitschutz-DNSSEC-und-DANE-auf-Linux-Servern-konfigurieren-2636175.html

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

T-Shirt für DANE-fähige Mailserver…

I Love Dane *by ilovemyshirt* Zazzle