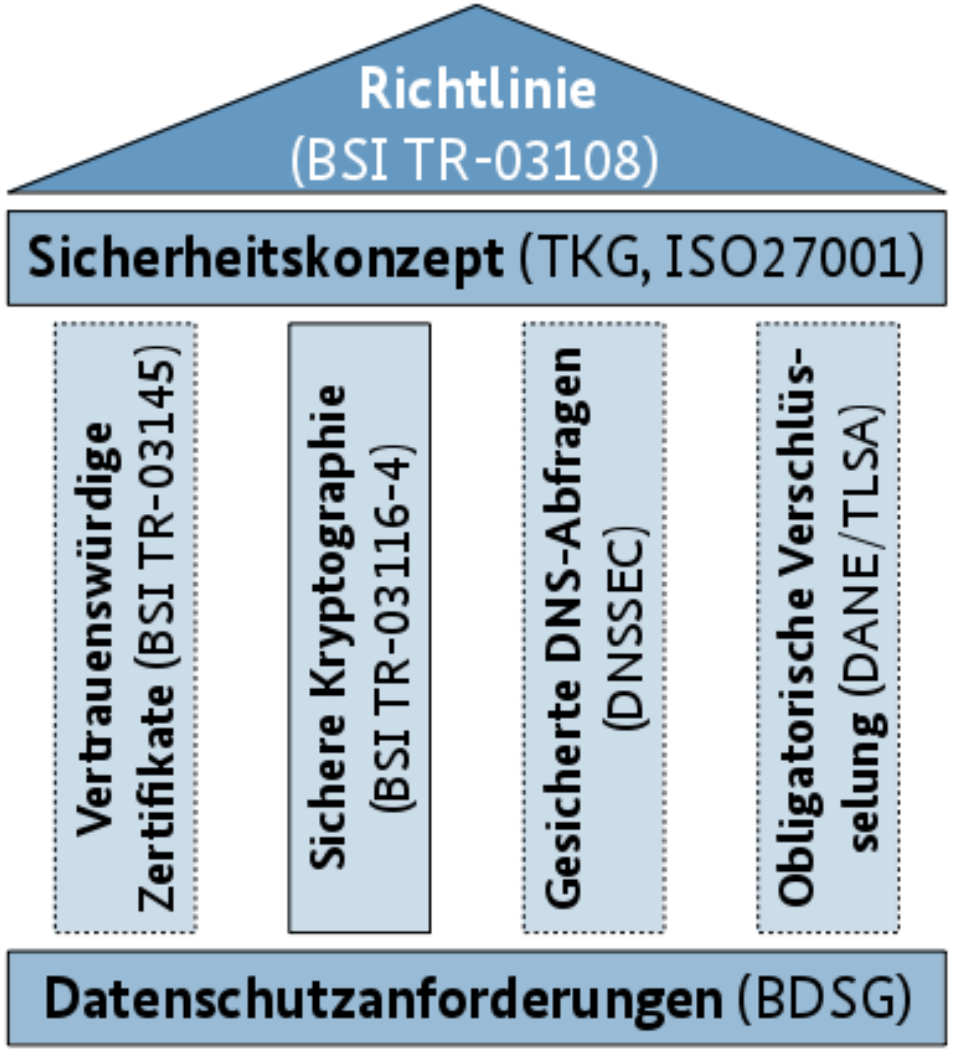
Sicherer E-Mail-Dienste-Anbieter

basierend auf

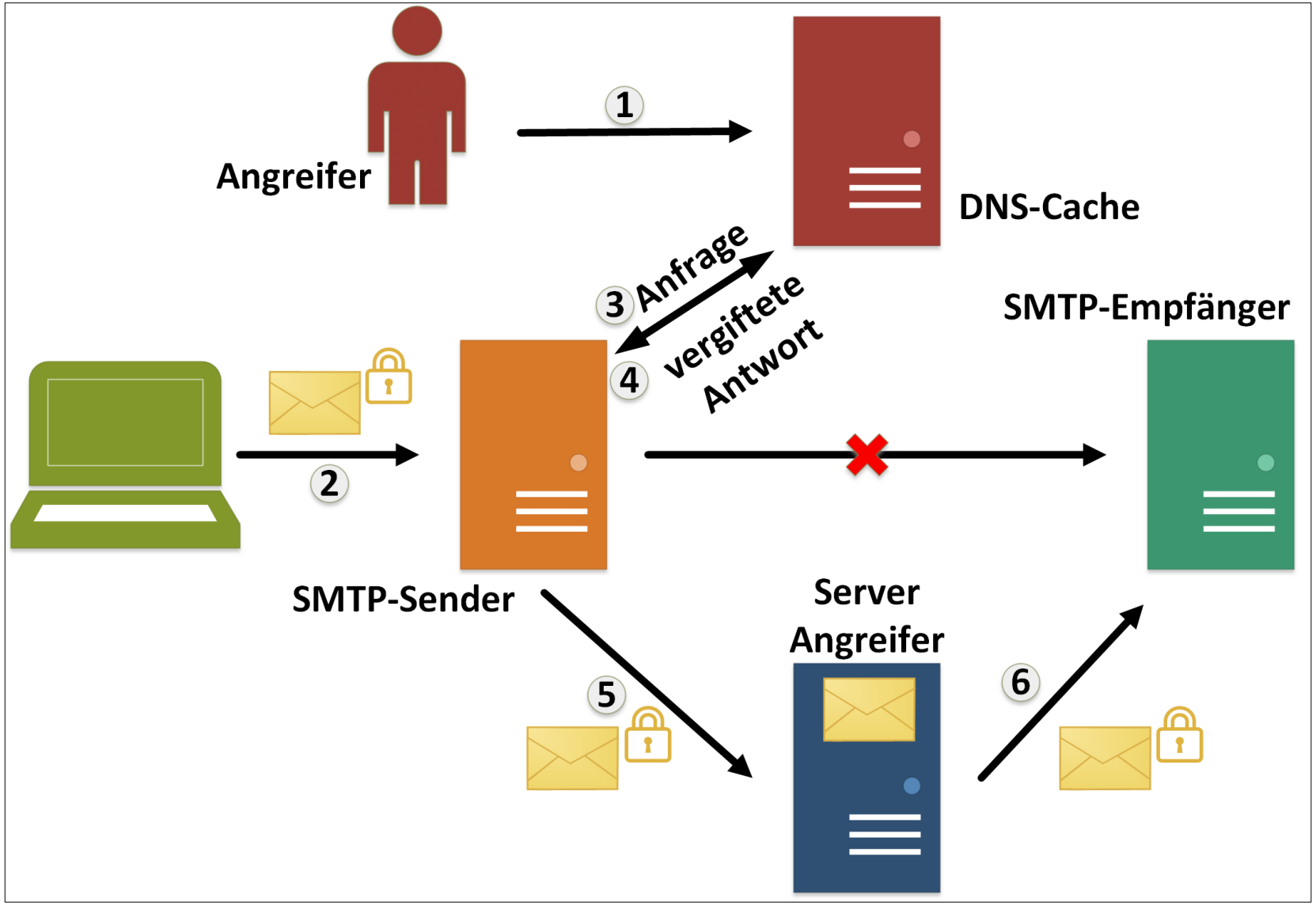
Domain Name System Security Extension (DNSSec)
&
DNS-based Authentication of Named Entities (DANE)

Aufgabenstellung

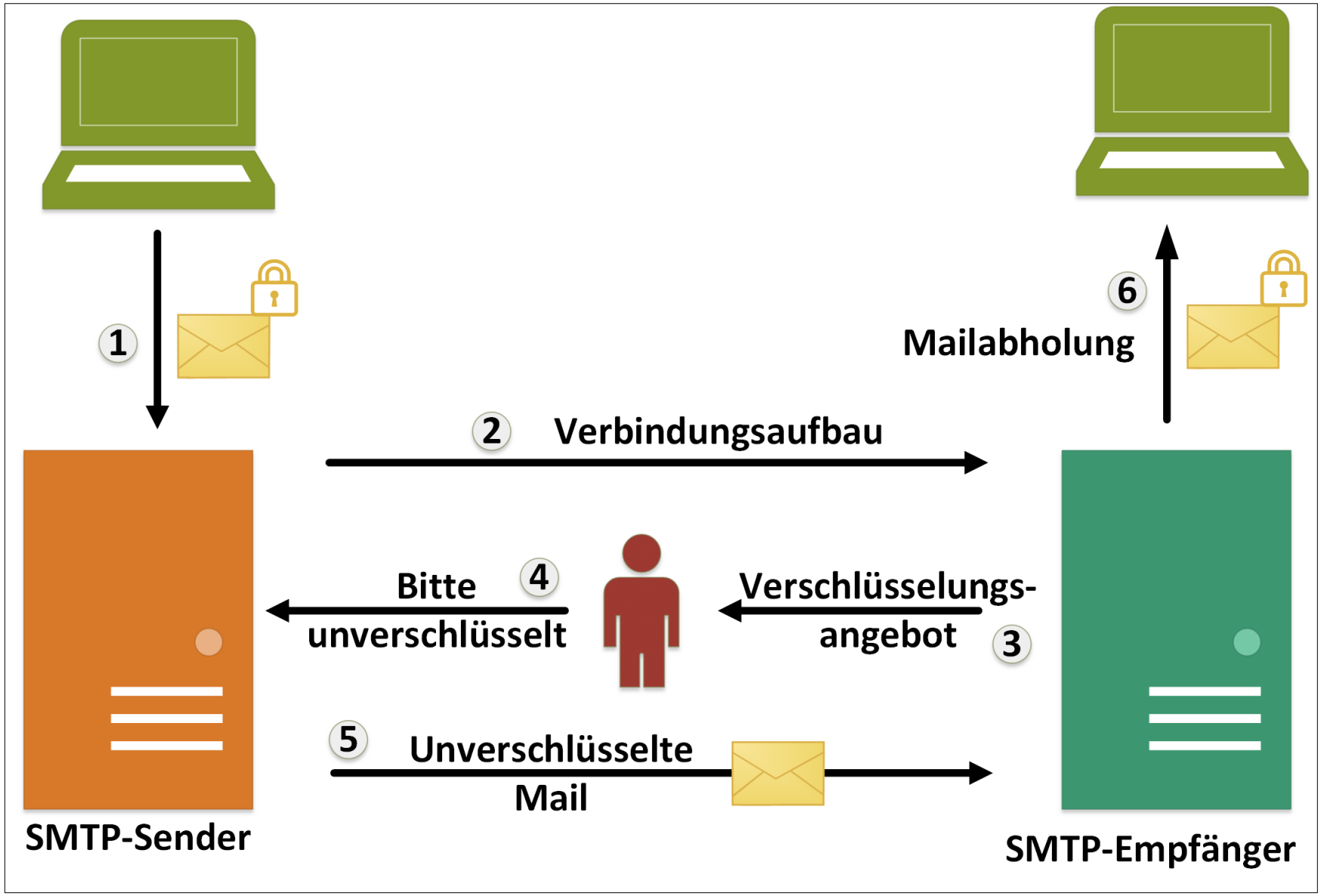
- Gesicherte DNS-Abfragen (DNSSec)
- Vertrauenswürdige Zertifikate
- Sichere Kryptographie
- Obligatorische Verschlüsselung (DANE/TLSA)



E-Mail: DNS-Cache-Poisoning und Umleitungsangriffe

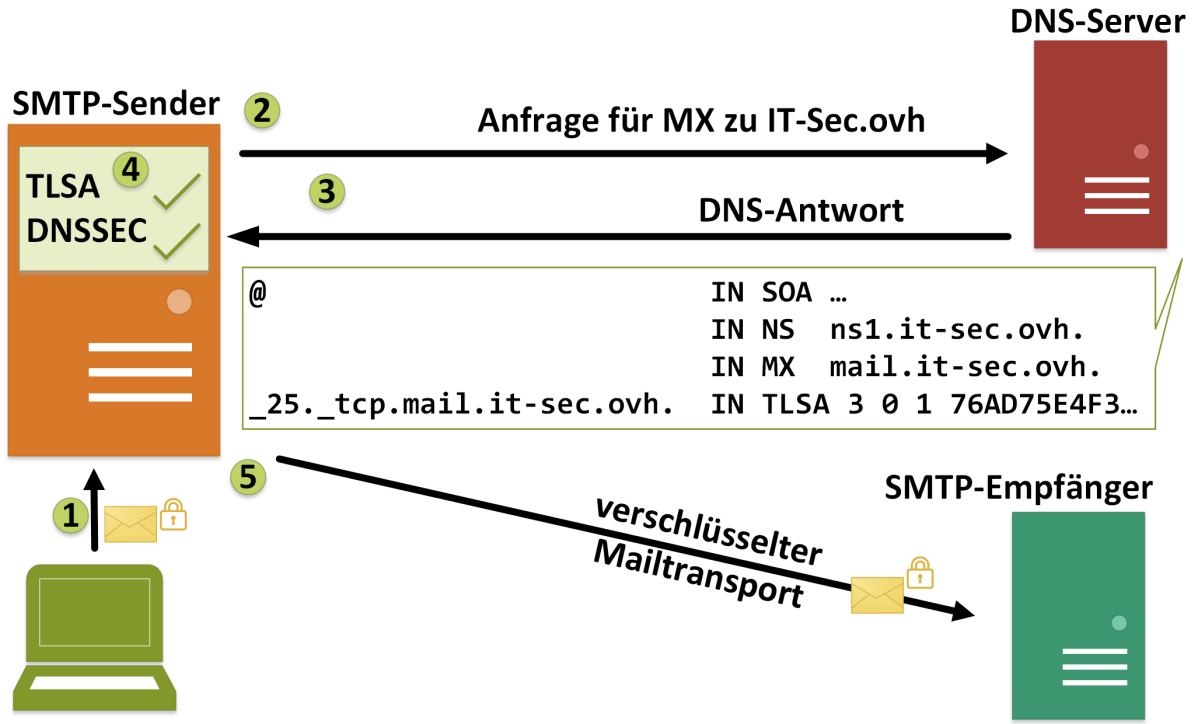


E-Mail: Downgrade Angriffe, MITM



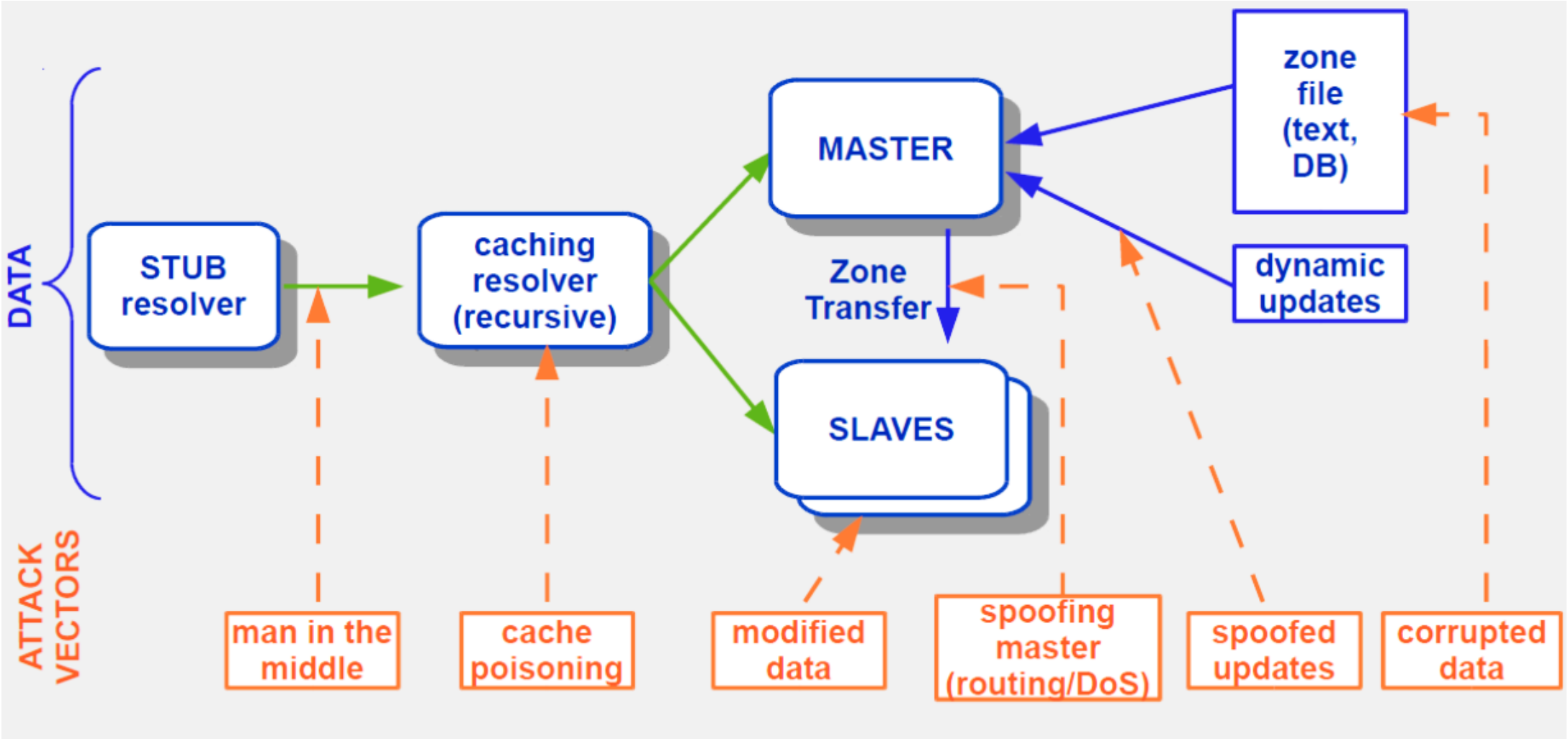
DNS-based Authentication of Named Entities (DANE)

- Baut auf DNSSec auf und nutzt TLSA Records (Transport Layer Security RR)
- Pinning von Zertifikaten oder Public-Keys (mittels TLSA-Records)
- DNSSec bietet zwei Varianten von Authenticated Denial of Existence
- Unterbindet Man-in-the-Middle und Klartext-Downgrade



DNS & DNSSec

DNS Angriffspunkte



DNSSec – DNS Security Extension

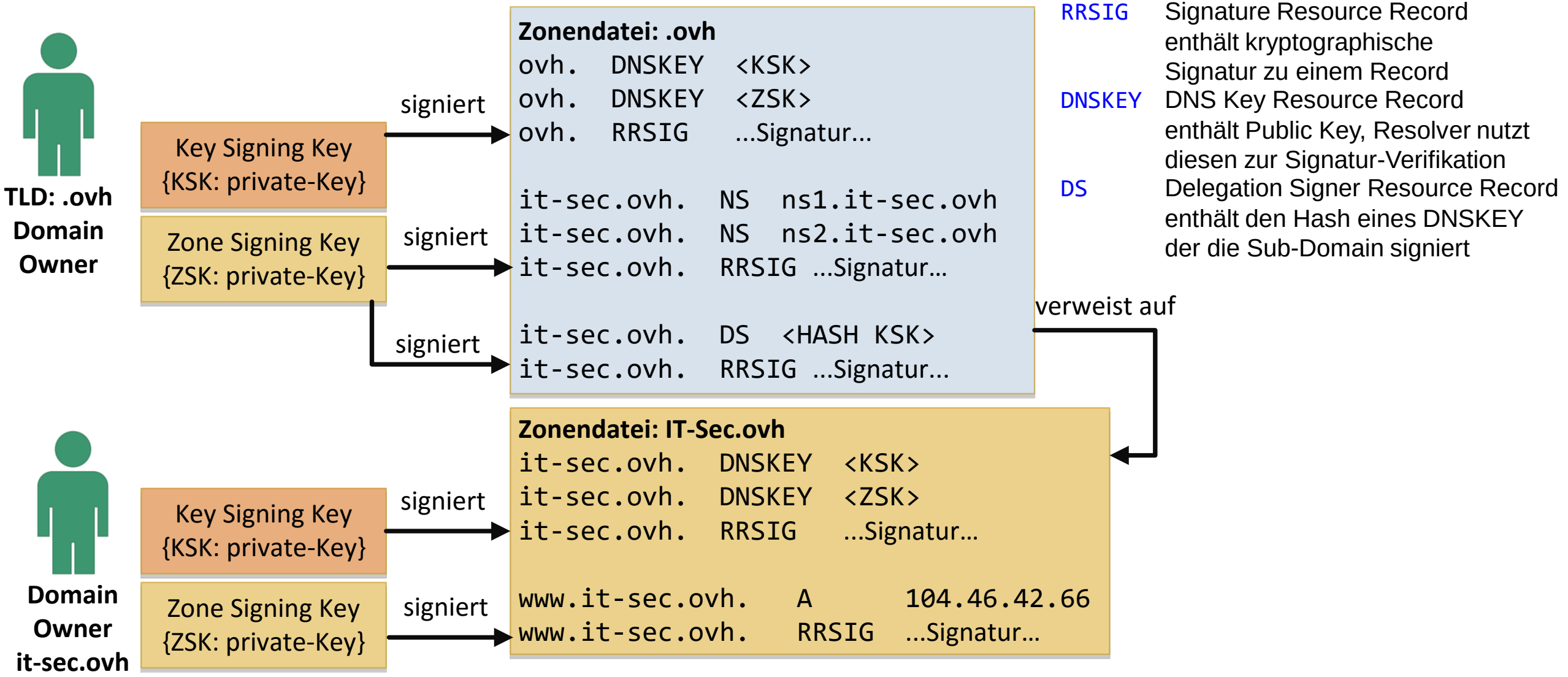
- Integritätsschutz
- Asymmetrische Kryptographie
  - RSA Signaturen
  - SHA2 Hashes
- Neue Resource-Record-Typen

`RRSIG` Signature Resource Record
enthält die kryptographische Signatur zu einem Record

`DNSKEY` DNS Key Resource Record
enthält den Public Key, wird von Resolver zur Signatur-Verifikation genutzt

`DS` Delegation Signer Resource Record (in der darüber liegenden Parent-Zone)
enthält den Hash eines DNSKEY (typischerweise des Key Signing Keys)

DNSSec – Zusammenwirken der Einträge



RRSIG Signature Resource Record enthält kryptographische Signatur zu einem Record

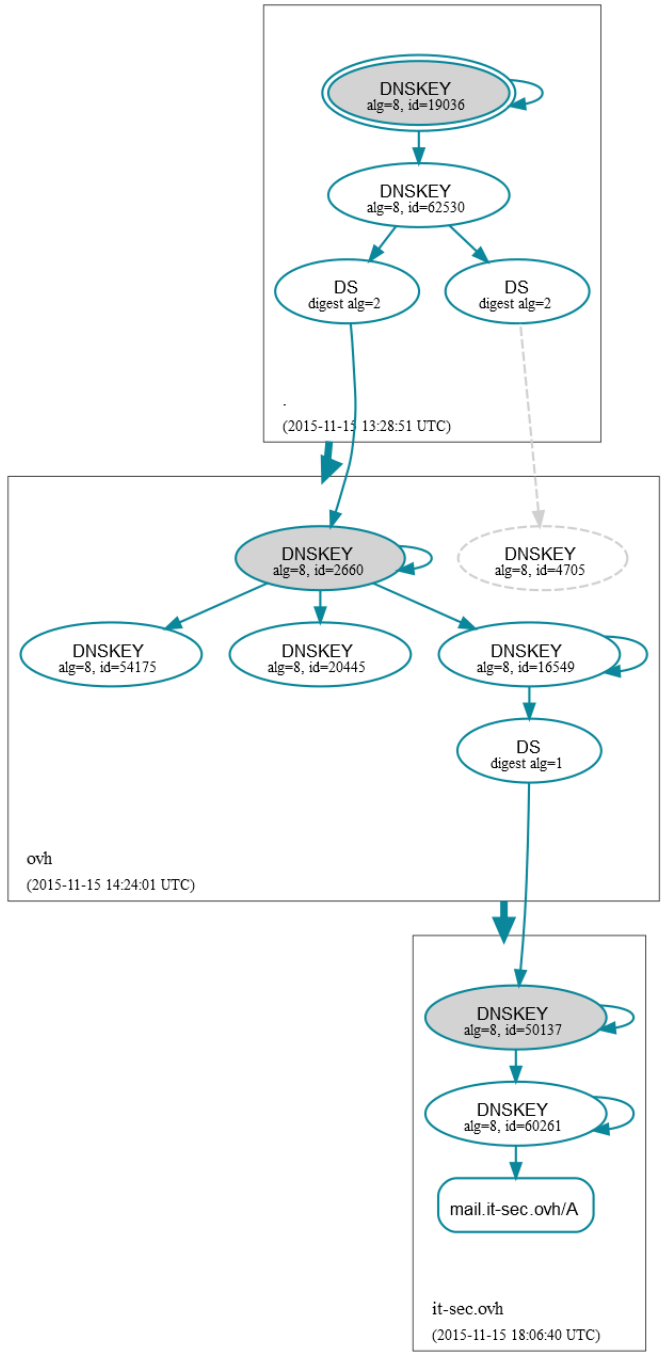
DNSKEY DNS Key Resource Record enthält Public Key, Resolver nutzt diesen zur Signatur-Verifikation

DS Delegation Signer Resource Record enthält den Hash eines DNSKEY der die Sub-Domain signiert

Beispiel: mail.it-sec.ovh
Analyse mit dnsviz.net

- URL: http://dnsviz.net/d/mail.it-sec.ovh/dnssec/

- Hash-Funktion: SHA256
- Key-Signing-Keys: RSA 2048
- Zone-Signing-Keys: RSA 1024



Beispiel: DNSSec Query

```
root@Sec-NS2:~# dig @localhost www.isc.org. A +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> @localhost www.isc.org. A +dnssec +multiline
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52840
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.                   IN A

;; ANSWER SECTION:
www.isc.org.            60 IN A 149.20.64.69
www.isc.org.            60 IN RRSIG A 5 3 60 (
                                20151107032012 20151008032012 6003 isc.org.
                                CVlfW5gDT9owDi+kdUZrYChhtK28aRxAdYeAWZ5ObtbI
                                HOdH4HQl++JD3N4wizi7vpSvyGTLDmrPaN8K7KmTF7B2
                                IG1/FGg00mGkgk1NzeT3V1O0RlUq9Gv9HX438om52D+O
                                1lWXK6FLHXOZVdTUrQ2LlY0bMaI41zp3RfEgD+s= )
```

DNS – Unterdrückung von Records (z.B. TLSA, …)

- DNS Request ohne Antwort -> NXDOMAIN
- Was wenn jemand absichtlich Antwort unterdrückt? –> DNSSec deckt das auf!

```
dig @localhost test.it-sec.ovh. A +dnssec +multiline
…
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10100
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
…
srv2.it-sec.ovh.        1200 IN NSEC www.it-sec.ovh. A RRSIG NSEC
srv2.it-sec.ovh.        1200 IN RRSIG NSEC 8 3 1200 (
                                20151106174146 20151007164146 60261 it-sec.ovh.
                                gkj1G5Kb4m3VrUOEdFvMNTr/yr/3kKqInowg76MeG1y4
                                1PoWkVzUlqwkigusu/o+8UBU0tXelVEd/zEdhYnoLLSL
                                HI+BY1n4W8PAJNBSkmpmO/RBHvLo22NBTRalbu9tPJCy
                                m4fal290QArggg5+Cc0R7a+FCmgjOh3bmqW/srs= )
```

Authenticated Denial of Existence: NSEC

- NXDOMAIN – Die angefragte Domain / angefragter Eintrag existiert nicht
- NSEC Records = Next Secure, bilden verkettete Liste
- Zone: `it-sec.ovh`

```
demo        IN  A    10.11.12.13
ns1         IN  A    40.74.62.0
ns2         IN  A   104.46.42.66
srv1        IN  A    40.74.62.0
srv2        IN  A   104.46.42.66
www         IN  A   104.46.42.66
```

```
demo NSEC ns1
ns1  NSEC ns2
ns2  NSEC srv1
srv1 NSEC srv2
srv2 NSEC www
www  NSEC demo
```

NSEC – Zone Walking

- Problem: Zone-Walking möglich – egal?

```
root@Sec-NS2:~# aptitude install ldnsutils

root@Sec-NS2:~# ldns-walk @localhost it-sec.ovh
it-sec.ovh.     it-sec.ovh. A NS SOA MX RRSIG NSEC DNSKEY
demo.it-sec.ovh. A RRSIG NSEC
mail.it-sec.ovh. A RRSIG NSEC
ns1.it-sec.ovh. A RRSIG NSEC
ns2.it-sec.ovh. A RRSIG NSEC
srv1.it-sec.ovh. A RRSIG NSEC
srv2.it-sec.ovh. A RRSIG NSEC
www.it-sec.ovh. A RRSIG NSEC

root@Sec-NS2:~# ldns-walk @localhost de.
de.     Zone does not seem to be DNSSEC secured,or it uses NSEC3.
root@Sec-NS2:~# ldns-walk @localhost at.
at.     Zone does not seem to be DNSSEC secured,or it uses NSEC3.
```

```
root@Sec-NS2:~# ldns-walk @localhost .
.       . NS SOA RRSIG NSEC DNSKEY
aaa. NS DS RRSIG NSEC
aarp. NS DS RRSIG NSEC
abb. NS DS RRSIG NSEC
abbott. NS DS RRSIG NSEC
abogado. NS DS RRSIG NSEC
ac. NS DS RRSIG NSEC
academy. NS DS RRSIG NSEC
accenture. NS DS RRSIG NSEC
…

root@Sec-NS2:~# ldns-walk @localhost br.
br.     br. NS SOA RRSIG NSEC DNSKEY
0800.br. NS DS RRSIG NSEC
acai.br. NS RRSIG NSEC
ace.br. NS RRSIG NSEC
ad1.br. NS RRSIG NSEC
adm.br. NS DS RRSIG NSEC
administracao.br. NS RRSIG NSEC
adolec.br. NS RRSIG NSEC
adv.br. NS DS RRSIG NSEC
…
```

Authenticated Denial of Existence

- Problem: Zone-Walking, z.B. in der Zone .at oder der Zone .br
- NSEC3 = Next Secure v3 oder NSEC Hashed Autenticated Denial of Existence
- Anstatt im Klartext lesbarer NSEC Einträge werden Hashes verwendet

NSEC	Next Secure Resource Record
NSEC3	Next Secure v3 (oder NSEC Hash) Resource Record
NSEC3PARAM	NSEC3 Parameter

NSEC Hashed Autenticated Denial of Existence

```
dig @localhost test.it-sec.ovh. A +dnssec +multiline
…
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22518
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1
…
IF6JDFQA8OILAS7OEKML1RPDCV2GMHN5.it-sec.ovh. 1200 IN NSEC3 1 0 100
                                                 578C30CC6333ADF7EA61A5DA07142D20 (
                                 V6OLG2RU8PQ5FU45JNU02J5HRUTIRPM9
                                 A RRSIG )
IF6JDFQA8OILAS7OEKML1RPDCV2GMHN5.it-sec.ovh. 1200 IN RRSIG NSEC3 8 3 1200 (
                                 20151109145641 20151010145608 60261 it-sec.ovh.
                                 nXELoGANXMzLnY4n2sLzEs2n9MkCD1mS/M7SV1G+6yPP
                                 Q/h0b4AZwAERa7znbEVkuCCw0aAKr/w9GeArhxD/wALF
                                 kYILbWpm9XSc1D4NXhdC9UA44+kAKRo90jimutUSDoAz
…
```

```
dig @localhost it-sec.ovh nsec3param +dnssec +multiline
…
;; ANSWER SECTION:
it-sec.ovh.             0 IN NSEC3PARAM 1 0 100 578C30CC6333ADF7EA61A5DA07142D20
```

```
root@Sec-NS2:~#
ldns-nsec3-hash -a 1 -t 100 -s 578C30CC6333ADF7EA61A5DA07142D20 test.it-sec.ovh.
oeapkduouj10ukpio42bv4qst7goj5sn.
```

DNSSec - Aktivierung

- DNSSec fast 10 Jahre alt, alle gängigen BIND-Versionen geeignet
- Neue Bind-Version (z.B. v9.9.x) jedoch deutlich komfortabler
- BIND als iterativer Resolver
  - beherrscht DNSSec
  - Konfiguration (aktivieren) genügt
  - ROOT-Key im Paket
- BIND als autoritativer Nameserver für Zone

DNSSec Resolver

- do Flag (DNSec unterstützt)
- ad Flag – Authenticated Data
- NOERROR
  (Fehlschlag wäre: SERVFAIL)
- RRSIG Signature RR
- 5 = RSA/SHA1
  (8 = RSA/SHA256)
- Ablaufdatum Signatur
- Signaturzeitpunkt
- 6003 = DNSKey Key-Tag

```
root@Sec-NS2:~# dig @localhost www.isc.org. A +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> @localhost www.isc.org. A +dnssec +multiline
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52840
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.                   IN A

;; ANSWER SECTION:
www.isc.org.            60 IN A 149.20.64.69
www.isc.org.            60 IN RRSIG A 5 3 60 (
                                20151107032012 20151008032012 6003 isc.org.
                                CVlfW5gDT9owDi+kdUZrYChhtK28aRxAdYeAWZ5ObtbI
                                HOdH4HQl++JD3N4wizi7vpSvyGTLDmrPaN8K7KmTF7B2
                                IG1/FGg00mGkgk1NzeT3V1O0RlUq9Gv9HX438om52D+O
                                1lWXK6FLHXOZVdTUrQ2LlY0bMaI41zp3RfEgD+s= )

;; Query time: 5127 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct 11 15:33:23 CEST 2015
;; MSG SIZE  rcvd: 223
```

DNSSec fähiger autoritativer Server

- Inline-Signing Modus für automatisierten DNSSec-Betrieb
- Vom Admin verwaltete Zonen-Files ohne RRSIG, DNSKEY, NSEC, NSEC3 Einträge

- dnssec-keygen … für Generierung von Key-Signing-Keys und Zone-Signing-Keys

```
root@Sec-NS2:/etc/named/domains/keys#
dnssec-keygen -a RSASHA256 -b 1024 it-sec.ovh
Generating key pair..++++++ .............++++++
Kit-sec.ovh.+008+60261

root@Sec-NS2:/etc/named/domains/keys#
dnssec-keygen -a RSASHA256 -b 2048 -f KSK it-sec.ovh
Generating key pair.........................+++ .........................+++
Kit-sec.ovh.+008+50137
```

DNSSec fähiger autoritativer Server, Zonen-Konfig

- `Key-Directory`
- `Inline-Signing`
- `maintain` -> auto KeyChange

```
key ns1.it-sec.ovh_ns2.it-sec.ovh
                        { algorithm hmac-sha256;
                          secret "B8BJ/Kgf4g3xDHXbT3x6lWfbdwXXMuXetqX6J1vz/Kk=";
                        };

server 40.74.62.0       { keys { ns1.it-sec.ovh_ns2.it-sec.ovh; }; };

zone "it-sec.ovh"        IN { type master; file "/etc/named/domains/zone_it-sec.ovh";
                              key-directory "/etc/named/domains/keys";
                              inline-signing yes; auto-dnssec maintain;
                              allow-transfer { key ns1.it-sec.ovh_ns2.it-sec.ovh; };
                              also-notify { 40.74.62.0; };
                            };
```

- Zone-Transfer (AXFR) zu den Secondary Nameservern
  - Mittels Transaction Signatures (TSIG) per shared Secret abgesichert
  - beinhaltet alle DNSSec Einträge
  - Am Secondary daher kein Schlüsselmaterial
  - Hidden Master möglich

DNS Zonen-Einträge

```
$TTL 20M                ; Time To Live (wie lange sollen Resolver die Antworten cachen)
                        ; Zone-Origin (FQDN des prim. NameSrv)
                        ; Zone-Contact (Mail-Adresse des DNS-Admin, @ = Punkt!)
@ IN SOA ns1.it-sec.ovh. dns-admin.hitco.at. (
     2015091301         ; Serial, z.B. YYYYMMDDrr
             20M        ; Refresh (Wartezeit fuer Sec-NameSrv)
             2M         ; Retry (Wartezeit fuer Sec-NameSrv bei Zone-Transfer Fehlschlag)
             25D        ; Expire (Wie lang soll Sec-NameSrv Zone behalten)
             20M )      ; TTL Negativ Cache (wie lange soll NXDomain gecached werden)

@                       IN      NS      ns1.it-sec.ovh.
@                       IN      NS      ns2.it-sec.ovh.

ns1             IN      A       40.74.62.0
srv1            IN      A       40.74.62.0
ns2             IN      A       104.46.42.66
srv2            IN      A       104.46.42.66

@               IN      MX 10   mail.it-seco.ovh.
@               IN      A       81.89.102.244
www             IN      A       81.89.102.244
```

DNS Zone

- Binärfile
- .signed
- RRSIG
- DNSKEY
- NSEC3
- NSEC3PARAM

```
root@Sec-NS2:/etc/named/domains#
named-checkzone -D -i full -f raw it-sec.ovh zone_it-sec.ovh.signed >/tmp/zone.txt
zone it-sec.ovh/IN: loaded serial 2015110510 (DNSSEC signed)
OK

vi /tmp/zone.txt
```

sec-ns2.cloudapp.net - PuTTY

```
it-sec.ovh.                                  1200 IN SOA       ns1.it-sec.ovh. dns-admin.hitco.at. 2015101049 1200 120 2160000 1200
it-sec.ovh.                                  1200 IN RRSIG     SOA 8 2 1200 20151109155608 20151010145608 60261 it-sec.ovh. R/5zQI3HV
it-sec.ovh.                                  1200 IN NS        ns1.it-sec.ovh.
it-sec.ovh.                                  1200 IN NS        ns2.it-sec.ovh.
it-sec.ovh.                                  1200 IN RRSIG     NS 8 2 1200 20151027155425 20150927154023 60261 it-sec.ovh. EHLTAwuFsw
it-sec.ovh.                                  1200 IN A         104.46.42.66
it-sec.ovh.                                  1200 IN RRSIG     A 8 2 1200 20151027155425 20150927154023 60261 it-sec.ovh. o7p8S25ZPSn
it-sec.ovh.                                  1200 IN MX        10 mail.hitco.at.
it-sec.ovh.                                  1200 IN RRSIG     MX 8 2 1200 20151027155425 20150927154023 60261 it-sec.ovh. v1+CE/5i70
it-sec.ovh.                                  1200 IN DNSKEY    256 3 8 AwEAAcScX9FiKgA+S0Q8Cwmz5WnPPJK0qWPMsbG2AJtibCiWh9nQzR60 lQ11P
it-sec.ovh.                                  1200 IN DNSKEY    257 3 8 AwEAAd8F8FNYQQFl0pjZTclbUzSzWpgPt3kgHDXWrU1OXSk9++ykoWRW WX0qH
it-sec.ovh.                                  1200 IN RRSIG     DNSKEY 8 2 1200 20151027164023 20150927154023 50137 it-sec.ovh. ISzN7S
it-sec.ovh.                                  1200 IN RRSIG     DNSKEY 8 2 1200 20151027164023 20150927154023 60261 it-sec.ovh. tC/Vzs
it-sec.ovh.                                  0 IN NSEC3PARAM   1 0 100 578C30CC6333ADF7EA61A5DA07142D20
it-sec.ovh.                                  0 IN RRSIG        NSEC3PARAM 8 2 0 20151109155512 20151010145608 60261 it-sec.ovh. DLa2Z
demo.it-sec.ovh.                             1200 IN A         10.11.12.13
demo.it-sec.ovh.                             1200 IN RRSIG     A 8 3 1200 20151106174146 20151007164146 60261 it-sec.ovh. nCpDoRQ+Ap4
mail.it-sec.ovh.                             1200 IN A         104.46.42.66
mail.it-sec.ovh.                             1200 IN RRSIG     A 8 3 1200 20151108094640 20151009084640 60261 it-sec.ovh. VPvSqdeWMh/
ns1.it-sec.ovh.                              1200 IN A         40.74.62.0
ns1.it-sec.ovh.                              1200 IN RRSIG     A 8 3 1200 20151027155425 20150927154023 60261 it-sec.ovh. igQv55U74PF
ns2.it-sec.ovh.                              1200 IN A         104.46.42.66
ns2.it-sec.ovh.                              1200 IN RRSIG     A 8 3 1200 20151027155425 20150927154023 60261 it-sec.ovh. GZvdpip5/dO
srv1.it-sec.ovh.                             1200 IN A         40.74.62.0
srv1.it-sec.ovh.                             1200 IN RRSIG     A 8 3 1200 20151027155425 20150927154023 60261 it-sec.ovh. Lo7OZBBBfj4
srv2.it-sec.ovh.                             1200 IN A         104.46.42.66
srv2.it-sec.ovh.                             1200 IN RRSIG     A 8 3 1200 20151027163736 20150927154023 60261 it-sec.ovh. O5jlJoqg5NT
www.it-sec.ovh.                              1200 IN A         104.46.42.66
www.it-sec.ovh.                              1200 IN RRSIG     A 8 3 1200 20151027163736 20150927154023 60261 it-sec.ovh. uh0cdXgfd/w
1S49DQ0MKAF3R2P35E1EHFCO1HJ2A59P.it-sec.ovh. 1200 IN NSEC3     1 0 100 578C30CC6333ADF7EA61A5DA07142D20 3032QR57IAH4LSL1M5BOA9E58BVCC
1S49DQ0MKAF3R2P35E1EHFCO1HJ2A59P.it-sec.ovh. 1200 IN RRSIG     NSEC3 8 3 1200 20151109155512 20151010145608 60261 it-sec.ovh. rqGRGlN
3032QR57IAH4LSL1M5BOA9E58BVCC0QL.it-sec.ovh. 1200 IN NSEC3     1 0 100 578C30CC6333ADF7EA61A5DA07142D20 42CJEDTQ5GI8NB4A1SRF3U2TJBUHO
3032QR57IAH4LSL1M5BOA9E58BVCC0QL.it-sec.ovh. 1200 IN RRSIG     NSEC3 8 3 1200 20151109155512 20151010145608 60261 it-sec.ovh. Spsgr2b
42CJEDTQ5GI8NB4A1SRF3U2TJBUHOQ7B.it-sec.ovh. 1200 IN NSEC3     1 0 100 578C30CC6333ADF7EA61A5DA07142D20 4G5DO1AG96IT1BVRKN903FQFJOKHO
                                                                                                                              1,1           Top
```

Re-Signing, Schlüsselwechsel

- Signatur der Zonen-Einträge: Default 30 Tage gültig, Re-Signing alle 7½ Tage
  Konfiguration mittels `sig-validity-interval`

- Auto-DNSSec maintain:
- Key-Verzeichnis wird überwacht, ZSK-Schlüsselwechsel (halb)automatisch
- Ablaufdatum festlegen

```
root@Sec-NS2:/etc/named/domains/keys#
dnssec-settime -I 20160101 -D 20160201 Kit-sec.ovh.+008+60261.key
./Kit-sec.ovh.+008+60261.key
./Kit-sec.ovh.+008+60261.private
```

- Successor erstellen

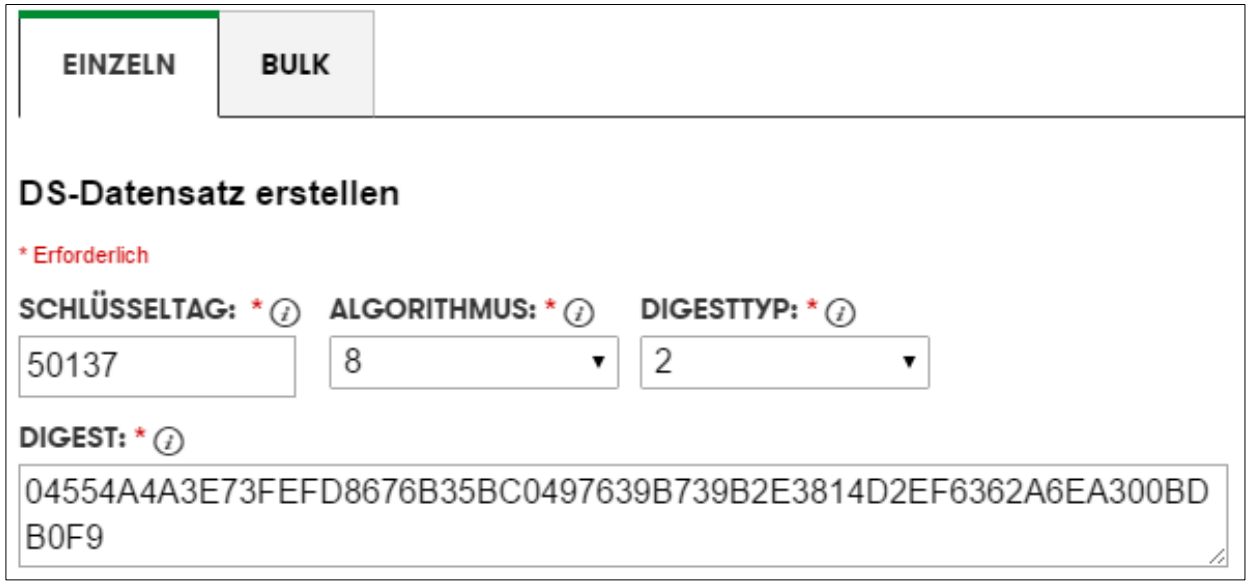
```
root@Sec-NS2:/etc/named/domains/keys# dnssec-keygen -S Kit-sec.ovh.+008+60261.key
Generating key pair.........................++++++
.................................................++++++
Kit-sec.ovh.+008+23040
```

Beispiel: Wechsel des Zone Signing Key (ZSK)

```
root@Sec-NS2:/etc/named/domains/keys# cat Kit-sec.ovh.+008+60261.key
; This is a zone-signing key, keyid 60261, for it-sec.ovh.
; Created: 20150913210726 (Sun Sep 13 23:07:26 2015)
; Publish: 20150913210726 (Sun Sep 13 23:07:26 2015)
; Activate: 20150913210726 (Sun Sep 13 23:07:26 2015)
; Inactive: 20160101000000 (Fri Jan  1 01:00:00 2016)
; Delete: 20160201000000 (Mon Feb  1 01:00:00 2016)
it-sec.ovh. IN DNSKEY 256 3 8 AwEAAcScX9FiKgA+S0Q8Cwmz5WnPPJK0qWPMsbG2AJtibCiWh9nQzR60
lQ11PGVaFpPSOsMWuFnu5tPtwLlx1v2Ij/eIhAD2t+BCx+MVoWpbgaIf
9OiMPah4HskTxJ1SgsNdqSWi6XUdXd/TtJYwFvox9Hf2t8V/cvO8BmIj Ee57UWk1

root@Sec-NS2:/etc/named/domains/keys# cat Kit-sec.ovh.+008+23040.key
; This is a zone-signing key, keyid 23040, for it-sec.ovh.
; Created: 20151106161238 (Fri Nov  6 17:12:38 2015)
; Publish: 20151202000000 (Wed Dec  2 01:00:00 2015)
; Activate: 20160101000000 (Fri Jan  1 01:00:00 2016)
it-sec.ovh. IN DNSKEY 256 3 8 AwEAAcn4kzhhjVxHgZi4nFZuIuq4plb2IzJPQNuLnDgzcqu03ULkNdId
Sg8EaiFGEJgoQ2yJu8XcsqnhBntNsPMHsia3RpMKVWGF9ruSPZ1+pG/7
tp8CVMt3xhmBnri9jdm+1CGrBKP4zg8dwHbNmdPyIOkLwnLrQfJrTpLW Wrfl1zd1
```

DNSSec - Aktivierung

- Erzeugung Schlüssel, Signatur der Zone, Replikation auf sekundäre Server
- Eintragung des KSK in der darüber liegenden Zone mittels Domain-Registrar

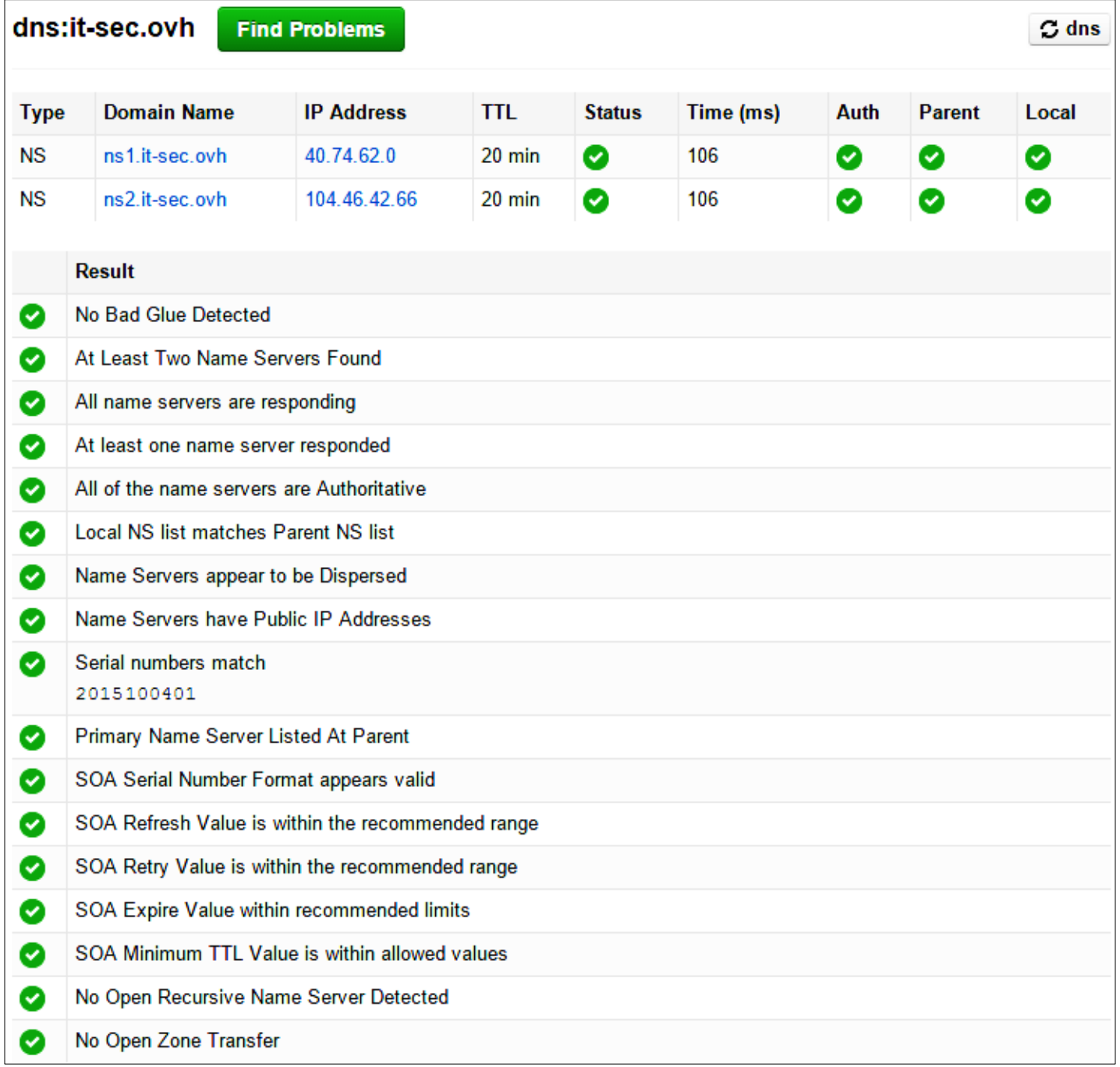


Best Practise und Learnings

- Inline-Signing und automatisches Key-Maintaining nutzen
- RSA / SHA256 nutzen
  - RSA verpflichtend unterstützt
  - DSA möglich, nicht Pflicht, nutzt niemand
  - ECDSA – im Kommen, Unterstützung noch nicht breit genug
  - SHA256 breit unterstützt, SHA1 wird ausgephast
- ZSK: 1024 bit -> kurze Signaturen, nicht langfristig sicher, NIST: 1 Jahr
- KSK: 2048 bit -> ausreichend sicher für ein paar Jahre, NIST: 5 Jahre
- KeyGen: Entropie nötig! Auf vServern HAVEGED nötig!
  Hardware Volatile Entropy Gathering and Expansion Daemon

DNS-Check

- mxtoolbox.com
- Allgemeiner DNS-Check



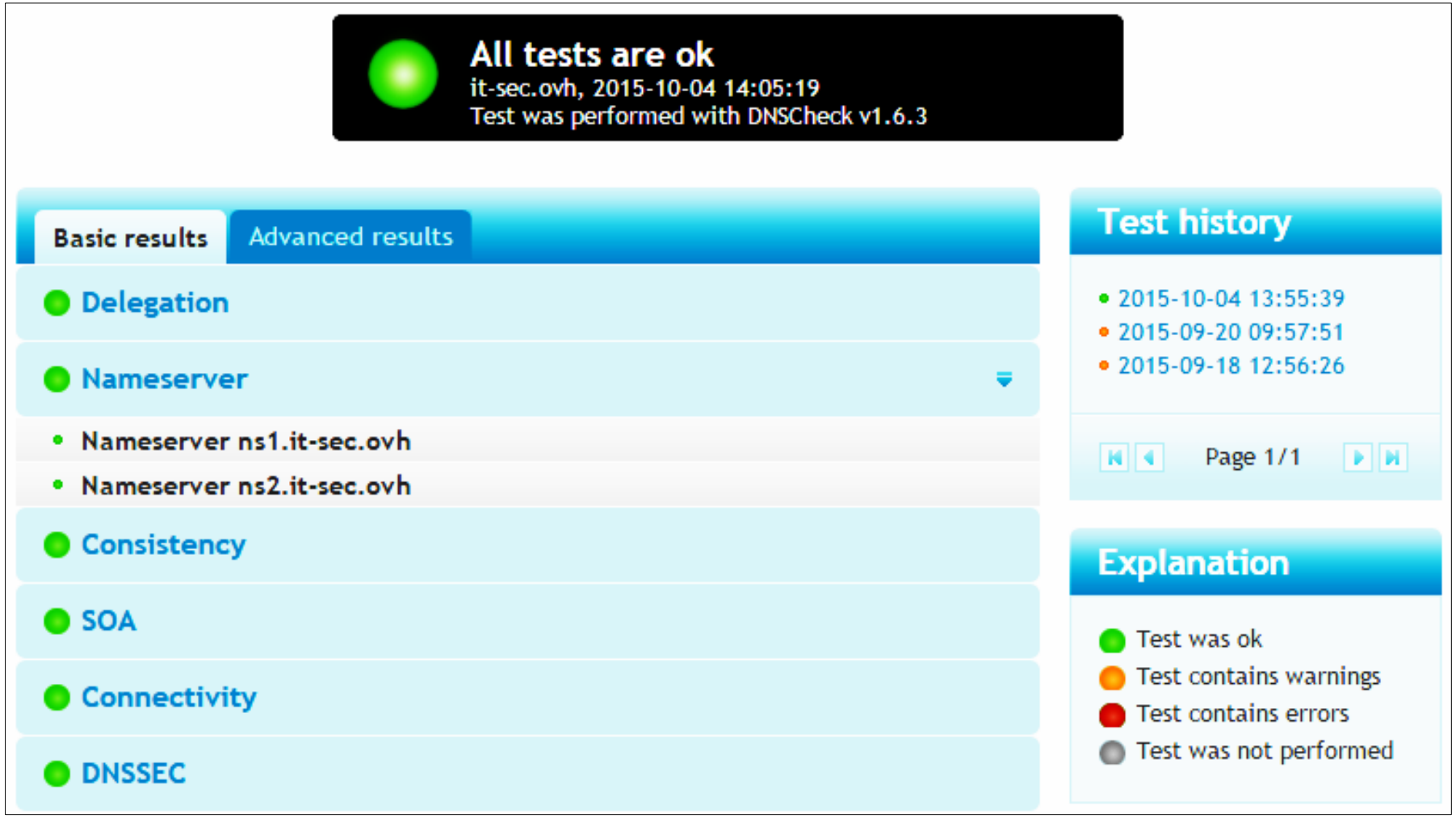
dns:it-sec.ovh Find Problems dns

Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	ns1.it-sec.ovh	40.74.62.0	20 min	✓	106	✓	✓	✓
NS	ns2.it-sec.ovh	104.46.42.66	20 min	✓	106	✓	✓	✓

	Result
✓	No Bad Glue Detected
✓	At Least Two Name Servers Found
✓	All name servers are responding
✓	At least one name server responded
✓	All of the name servers are Authoritative
✓	Local NS list matches Parent NS list
✓	Name Servers appear to be Dispersed
✓	Name Servers have Public IP Addresses
✓	Serial numbers match 2015100401
✓	Primary Name Server Listed At Parent
✓	SOA Serial Number Format appears valid
✓	SOA Refresh Value is within the recommended range
✓	SOA Retry Value is within the recommended range
✓	SOA Expire Value within recommended limits
✓	SOA Minimum TTL Value is within allowed values
✓	No Open Recursive Name Server Detected
✓	No Open Zone Transfer

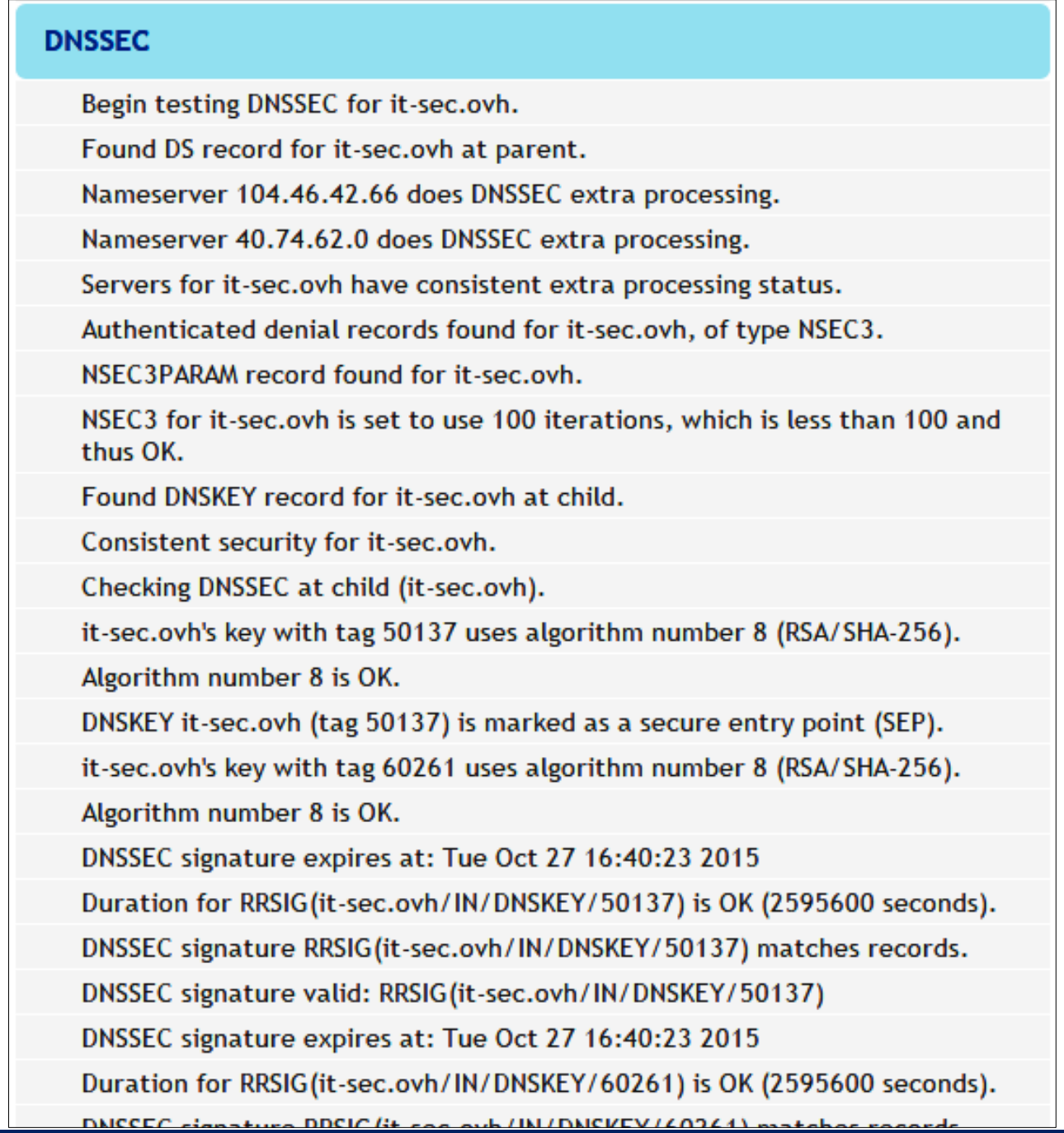
DNSSec-Check

- dnscheck.iis.se
- Summary



DNSSec-Check

- dnscheck.iis.se
- Details



DNSSec-Debugger

- dnssec-debugger.verisignlabs.com

.	Found 3 DNSKEY records for . DS-19036/SHA-1 verifies DNSKEY-19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG-19036 and DNSKEY-19036/SEP verifies the DNSKEY RRset
ovh	Found 2 DS records for ovh in the . zone Found 1 RRSIGs over DS RRset RRSIG-62530 and DNSKEY-62530 verifies the DS RRset Found 3 DNSKEY records for ovh DS-2660/SHA-256 verifies DNSKEY-2660/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG-2660 and DNSKEY-2660/SEP verifies the DNSKEY RRset
it-sec.ovh	Found 1 DS records for it-sec.ovh in the ovh zone Found 1 RRSIGs over DS RRset RRSIG-54175 and DNSKEY-54175 verifies the DS RRset Found 2 DNSKEY records for it-sec.ovh DS-50137/SHA-1 verifies DNSKEY-50137/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG-50137 and DNSKEY-50137/SEP verifies the DNSKEY RRset it-sec.ovh A RR has value 104.46.42.66 Found 1 RRSIGs over A RRset RRSIG-60261 and DNSKEY-60261 verifies the A RRset

Checking DS between ovh and it-sec.ovh

Found 1 DS records for it-sec.ovh in the ovh zone

Found 1 RRSIGs over DS RRset

```
it-sec.ovh. 172800 IN RRSIG DS 8 2 172800 ( 20151124193614 20150925193614 54175 ovh.
Qy9h5Bmrbjl3Rnre6xHPcyCUne9LcU2X+JaBNXI/c+s2t/VYTex0EUX4ELf1Y84iJucpa3l7Tj0A
iTFEg4zyztEWbks/Q69QM/TUKmGdd0Fv5Ao9kVmF44RFIarmgBU/RaETYB77FfcaBO8E9wb2K8nd DuYWYXjucY9EERKBKwk= )
```

RRSIG-54175 and DNSKEY-54175 verifies the DS RRset

DS-50137/SHA-1 is now in the chain-of-trust

```
it-sec.ovh. 172800 IN DS 50137 8 1 a755cafc6b341759bb369b7c36b3661af2d4f221
```

Found 2 DNSKEY records for it-sec.ovh

```
it-sec.ovh. 1200 IN DNSKEY 256 3 8 ( AwEAAcScX9FiKgA+S0Q8Cwmz5WnPPJK0qWPMsbG2AJtibCiWh9nQzR60lQ11PGVaFpPSOsMWuFnu
5tPtwLlx1v2Ij/eIhAD2t+BCx+MVoWpbgaIf9OiMPah4HskTxJ1SgsNdqSWi6XUdXd/TtJYwFvox 9Hf2t8V/cvO8BmIjEe57UWk1 ) ; Key ID = 60261
```

```
it-sec.ovh. 1200 IN DNSKEY 257 3 8 ( AwEAAd8F8FNYQQFl0pjZTclbUzSzWpgPt3kgHDXWrU1OXSk9++ykoWRWWX0qHbPCiFklDU1C8U94
/wxhiYzafyGMYm/Tf4D/tU9WoWo3q+bRnHeBP2Jg9AgzPN8E7Q0ZZztbGnpKajlBvWjjSU2Qfd/w
WvmHS/3lzb1fQPwNL5HX0SsDB4wOEqC0Q18RNGHjmxLrOoIYi0z7QZNtp/EOMJ2ANHmF4SjJZV2e
QgMroN8KGdxaAlGivdknZFiT99RUj+PzXm7vINEpABxrBv5V8qG5aUWQuwHIhXW7EvRp1O3iHCm/ xMFflmMXNNMJtVMe4PkqyTbBPlezxDysu6mQcg1pzpU= ) ;
Key ID = 50137
```

DNSKEY-50137/SEP is now in the chain-of-trust

DS-50137/SHA-1 verifies DNSKEY-50137/SEP

Found 2 RRSIGs over DNSKEY RRset

```
it-sec.ovh. 1200 IN RRSIG DNSKEY 8 2 1200 ( 20151027164023 20150927154023 50137 it-sec.ovh.
ISzN7SfAE1r2fvioUrTEmpJ3Ip9N7gjZ0TFM/jZ3joEy1uhyMAjBVXseYZwr21py1AFUUqsFmGY9
21Gu6vHBaUNFAP2s8IDA+i368h6SBBOY67r4znUSNuVEUejhB/aHBc1HlZCPF3lPzAKFWK3byWz8
ixaxJdGYLQdYROviUWNSh8HWzsfCp++0feSQCHaBR2nI6IefnsoHdAj0TMk4fYydcrfuSoEpuPuK
b5R6VXvZ/+6xRHwjXXKDBDo6LO6RE3jAqkxiRIk4PICsv43rAEmHIiq3kwQ+KchCpD6fHPdF47ma dKsKHMhdYFyYKljdGX6txxaHLzoaH2+ss8/lIA== )
```

```
it-sec.ovh. 1200 IN RRSIG DNSKEY 8 2 1200 ( 20151027164023 20150927154023 60261 it-sec.ovh.
tC/Vzs8pJAiYOC88ALyN2cA0hiyGy3eiIzO05pPz+8aRXQV9RqnLpNF2bJUrlEmWRtGXkinGkrc9
TDGwlzu8y4vyNiOsT6gNnALLCfL3iq1PDCe7cfKOAbHVSXW5dQSq8k6yM0H8/ghIk9eYfuJKTQsh F42JsmMy4Xq48YQ6C5Y= )
```

RRSIG-50137 and DNSKEY-50137/SEP verifies the DNSKEY RRset

RRSIG-60261 and DNSKEY-60261 verifies the DNSKEY RRset

DNSKEY-60261 is now in the chain-of-trust

it-sec.ovh is authoritative for it-sec.ovh

it-sec.ovh A RR has value 104.46.42.66

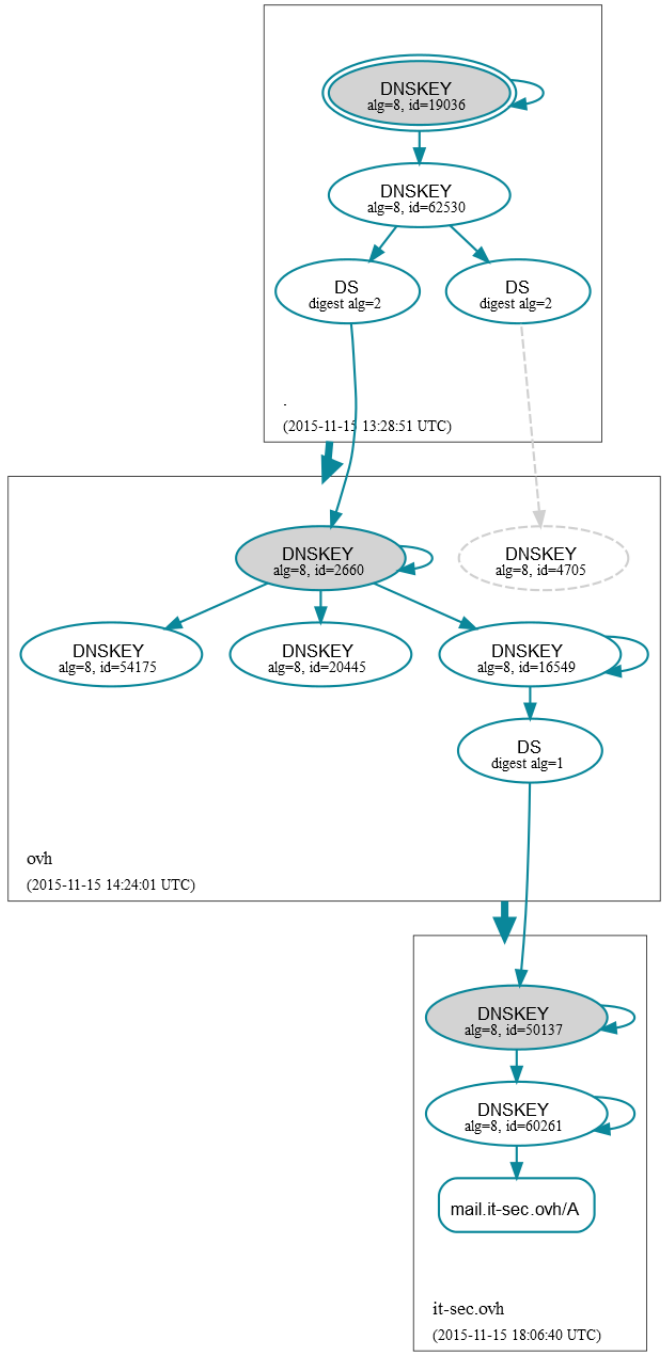
Found 1 RRSIGs over A RRset

```
it-sec.ovh. 1200 IN RRSIG A 8 2 1200 ( 20151027155425 20150927154023 60261 it-sec.ovh.
o7p8S25ZPSnFGFCbsjY/HMGBWQhCn3LRggmgxHghl8E318EoHlvbIKbGFUrSAxYrQAy8+OzMFU0A
OkbcYZItNZgVi9+hsDT8SrMTdxWBh4pvFgQ2wpmd+QRkwBqlg4qvHyqa6E1ScItWBXGb5VvjMsn+ RCWRo7WAgKiDh71feKc= )
```

RRSIG-60261 and DNSKEY-60261 verifies the A RRset

Analyse mit dnsviz.net

- Grafische Darstellung
- Zeigt Zone-Delgation
- Grafische Veranschaulichung der Key-/Trust-Hierarchie

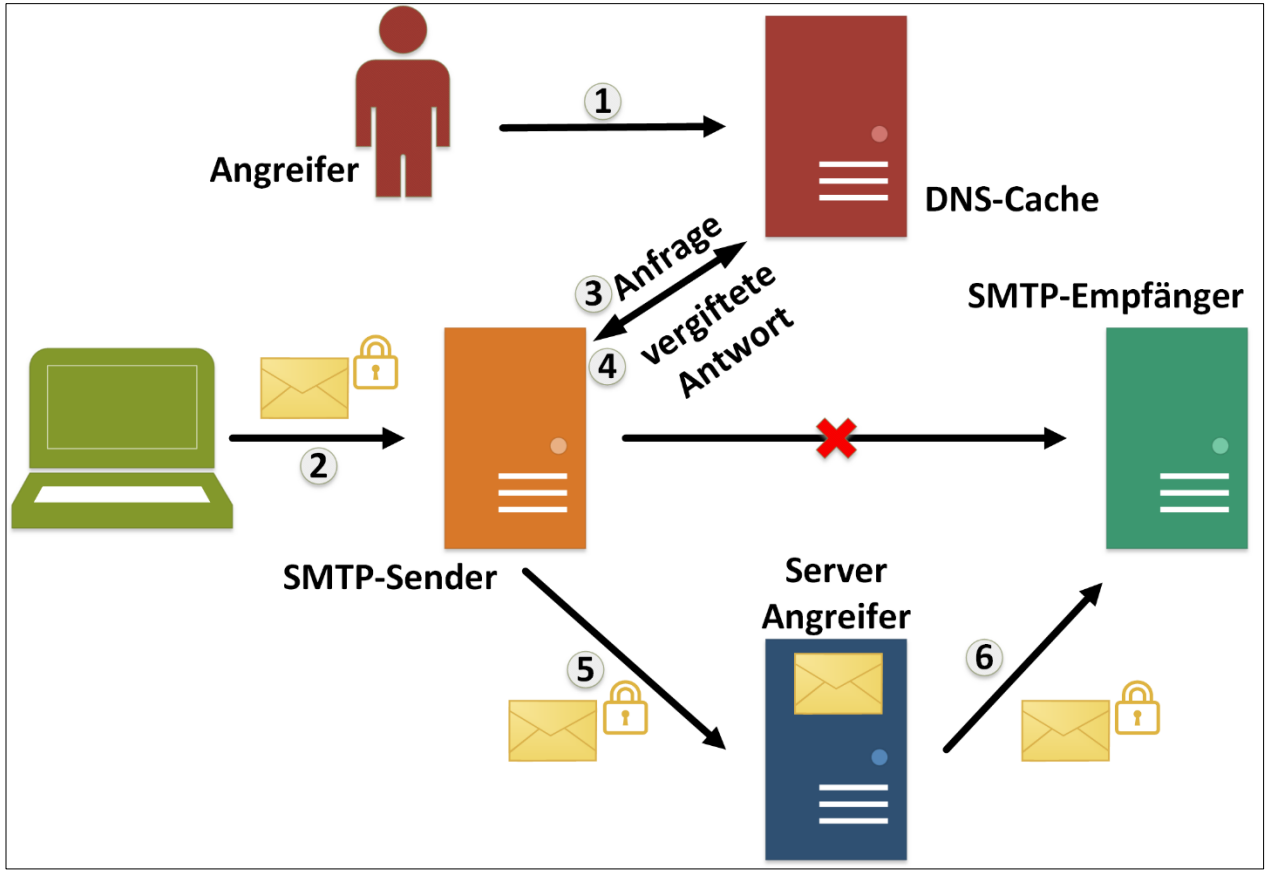


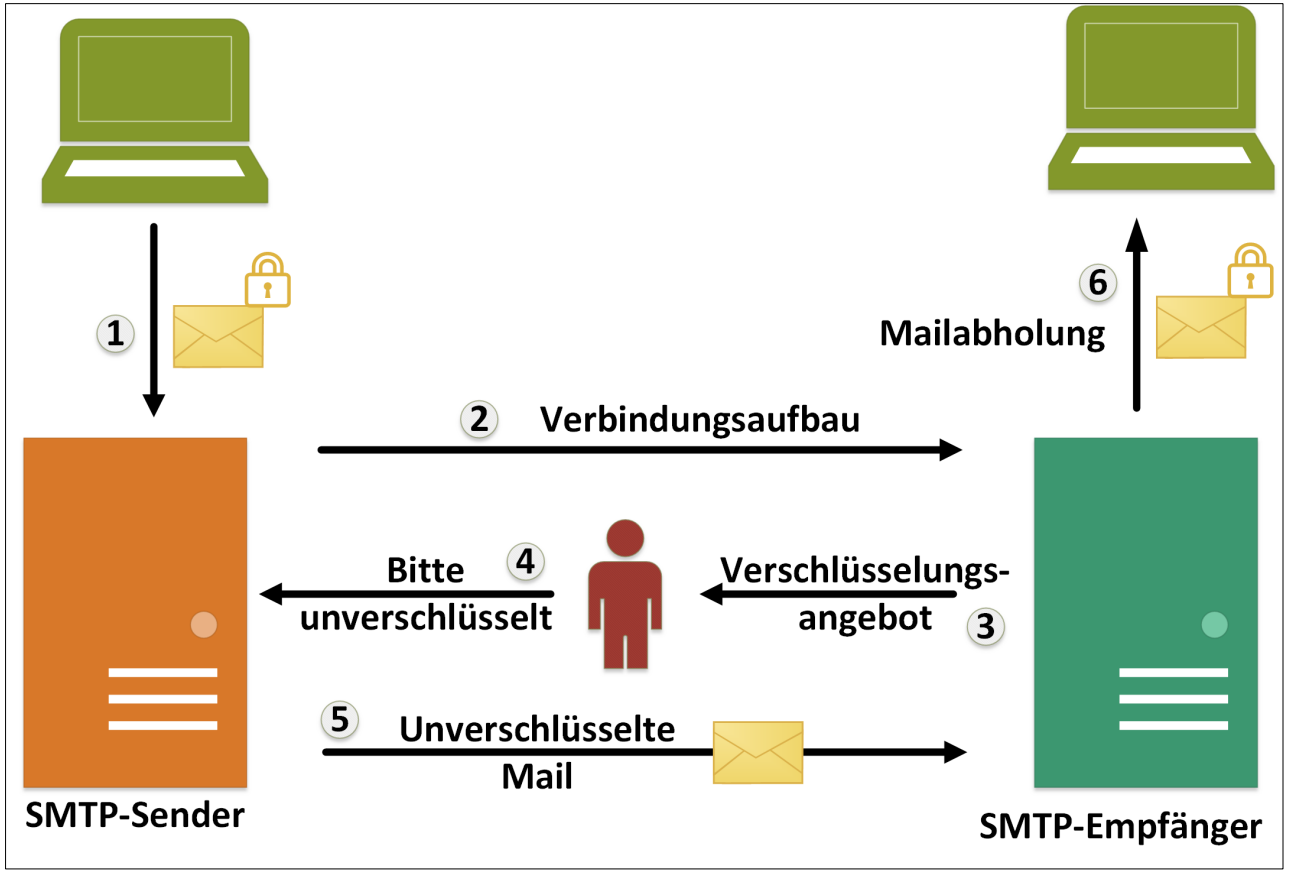
DANE

DNS-based Authentication of Named Entities (DANE)

Rückblick: SMTP Transport, Angriffe

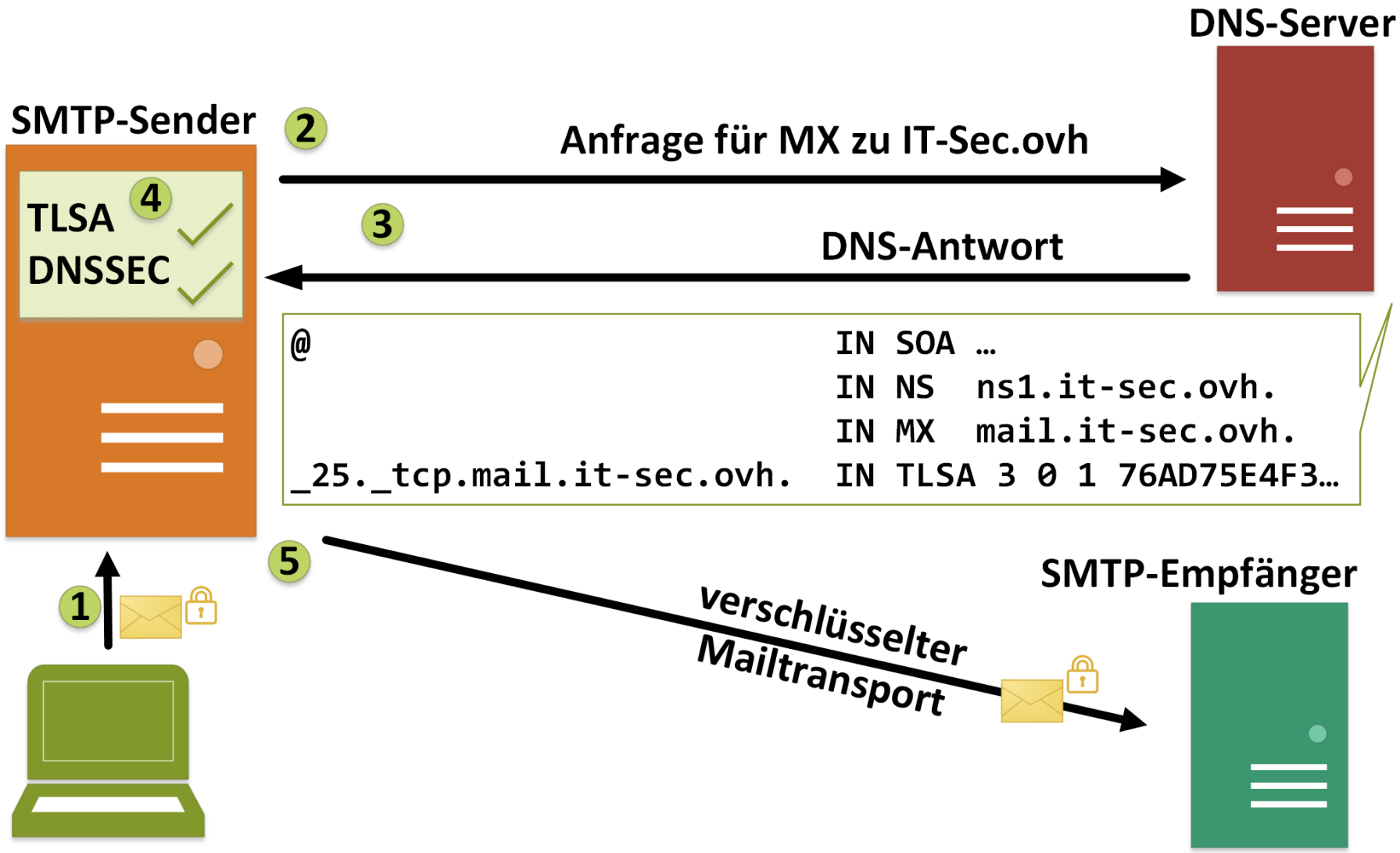
- Umlenkung, MITM, Downgrade, …





DNS-based Authentication of Named Entities (DANE)

- Existenz des TLSA-Records und NSEC/NSEC3 verhindern Downgrade
- Inhalt des TLSA-Records pinnt Zertifikate oder pinnt CAs oder pinnt PublicKeys



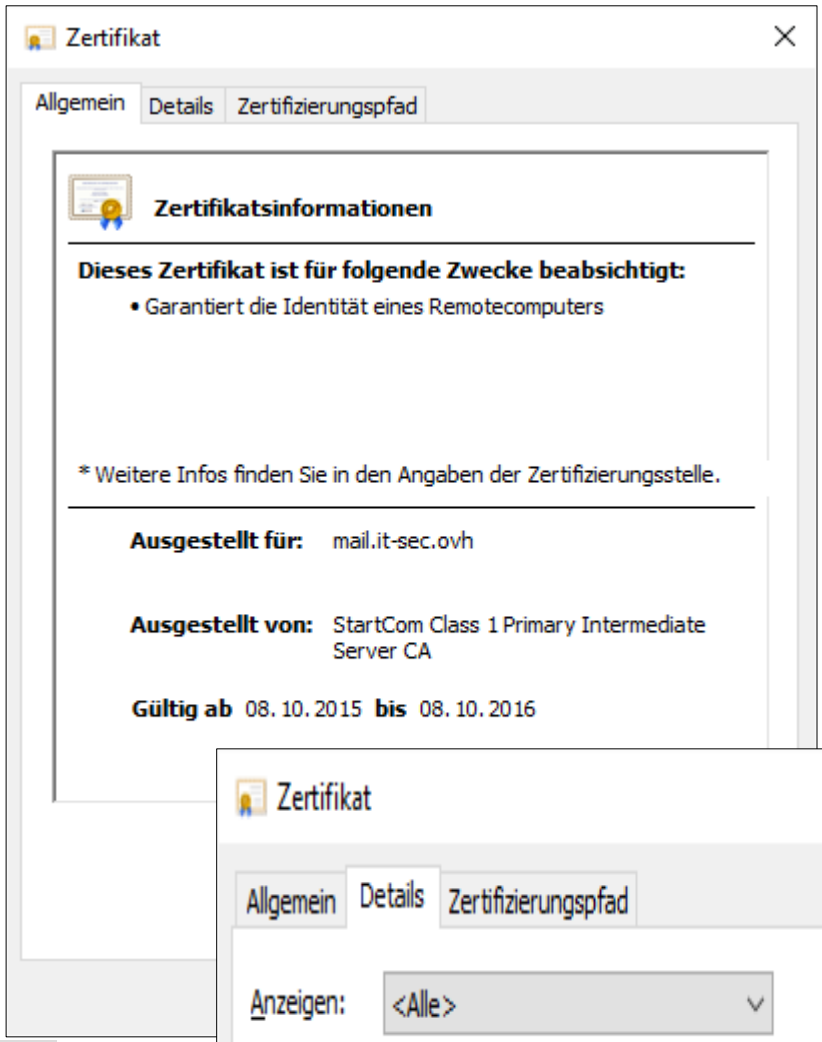
DANE baut auf TLS auf -> benötigt Zertifikate

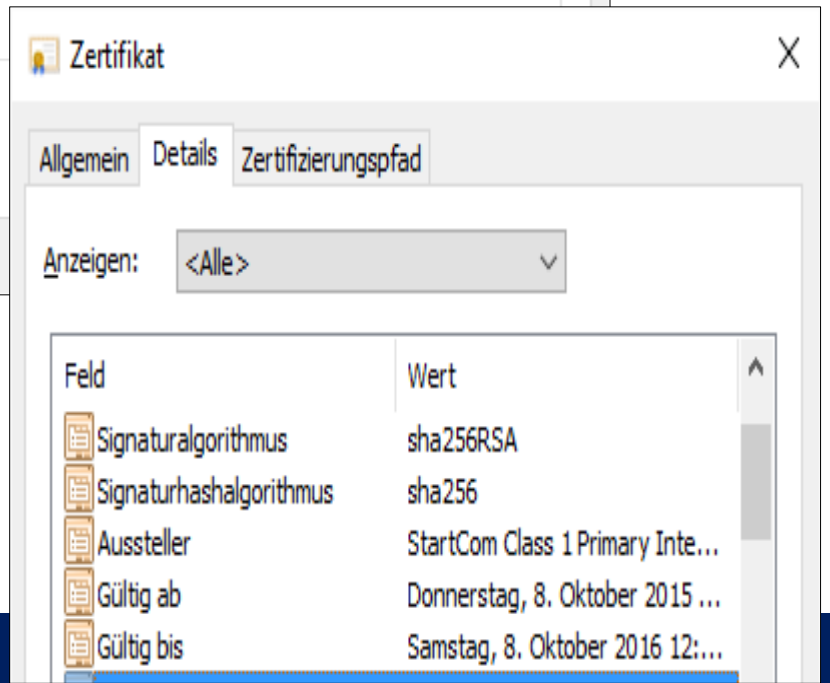
- Könnten Self-Signed sein
- Jedoch besser aus getrusteter CA, da DANE noch Nischen-Technologie

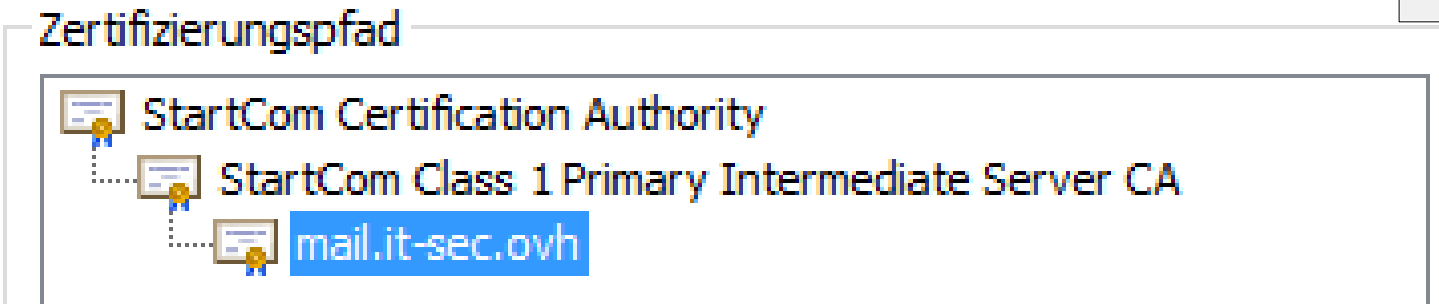
- Kostenfrei Domain-Validated (DV) TLS-Server Zertifikate:
  - StartCom Ltd.: https://www.startssl.com/
  - ISRG (Internet Security Research Group) & Mozilla: https://letsencrypt.org/
  - WoSign: https://www.wosign.com/english/freeSSL.htm

Zertifikat ausstellen:
Typische Vorgangsweise

- RSA Schlüsselpaar generieren
- CSR erstellen
- CSR an CA übermitteln
- Zertifikat erhalten
- Zertifikat + CertChain installieren





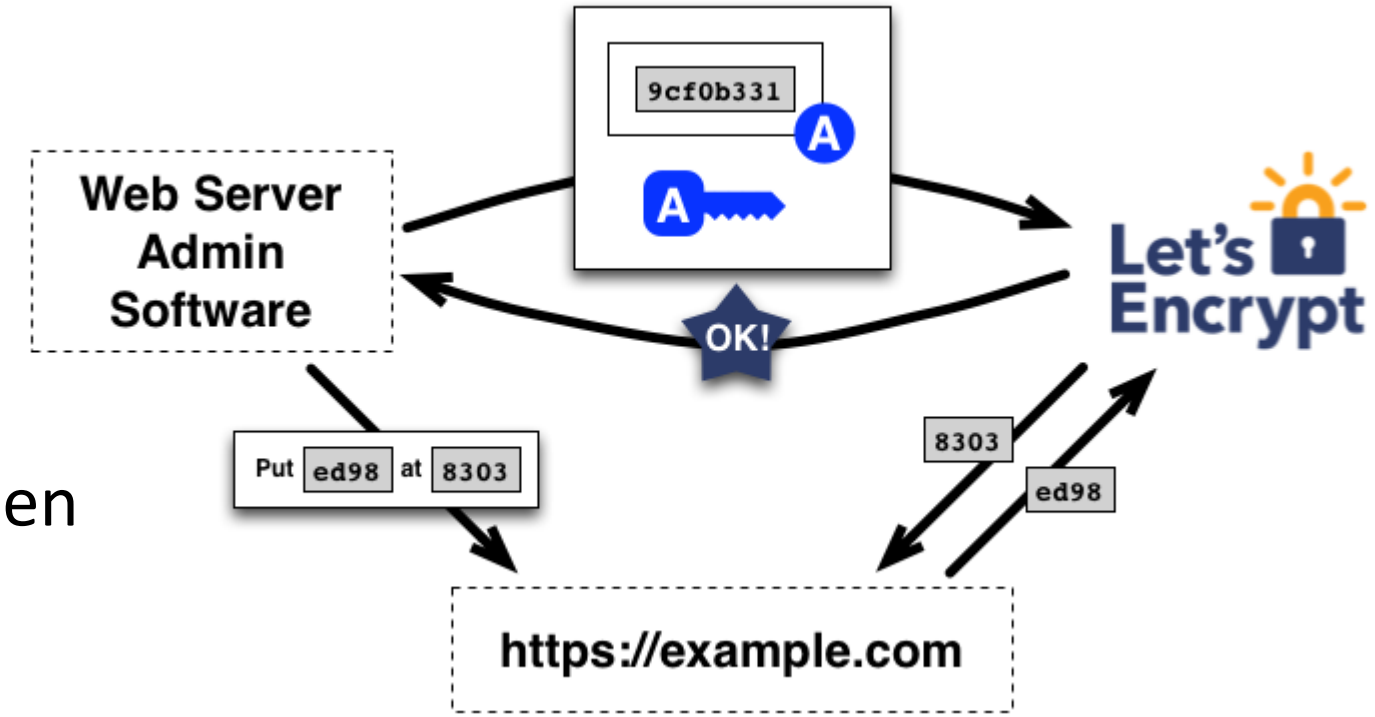


Alternative: Let's Encrypt

- Automatisierter DV-Vorgang
- Python Client

- Zertifikatserneuerung vollautomatisch alle 60 Tage

- CSR-Nutzung möglich
  -> Schlüsselpaar kann gleich bleiben



TLSA Record für DANE Transport Layer Security Protocol

- DNSSec Voraussetzung
- TLSA RR
  - Pinning
  - Zertifikat oder CA

```
root@Sec-NS2:/etc/ssl/private#
openssl x509 -in mail.it-sec.ovh.crt -outform DER | openssl sha256
(stdin)= 91ba252c1e6bd40767d646070c015d0b9edad8957f04880b3a6b1c63abfc4d43

openssl x509 -in www.it-sec.ovh.crt -outform DER | openssl sha256
(stdin)= 1597dc6d11cf983dee0d0c7094daff635dfc5ffa3fe9390d021a121a36e8e92e
```

  - Zertifikats-Hash

```
root@Sec-NS2:/etc/ssl/private#
openssl x509 -noout -fingerprint -sha256 -in www.it-sec.ovh.crt
SHA256 Fingerprint=15:97:DC:6D:11:CF:98:3D:EE:0D:0C:70:94:DA:FF:63:5D:FC:
                   5F:FA:3F:E9:39:0D:02:1A:12:1A:36:E8:E9:2E
```

  - oder PubKey-Hash

```
root@Sec-NS2:/etc/ssl/private# openssl x509 -in mail.it-sec.ovh.crt -pubkey -noout |
 openssl rsa -pubin -outform der | openssl dgst -sha256 -hex
writing RSA key
(stdin)= a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a6c6f0c16b5
```

DANE: PubKey Hash -> TLSA Record

- Im Zonen-File der Domain wird ein TLSA-Record ergänzt

Der TLSA-Record ist wie folgt aufgebaut [RFC-6698, Kapitel 7]:

```
_25._tcp.mail    IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…
```

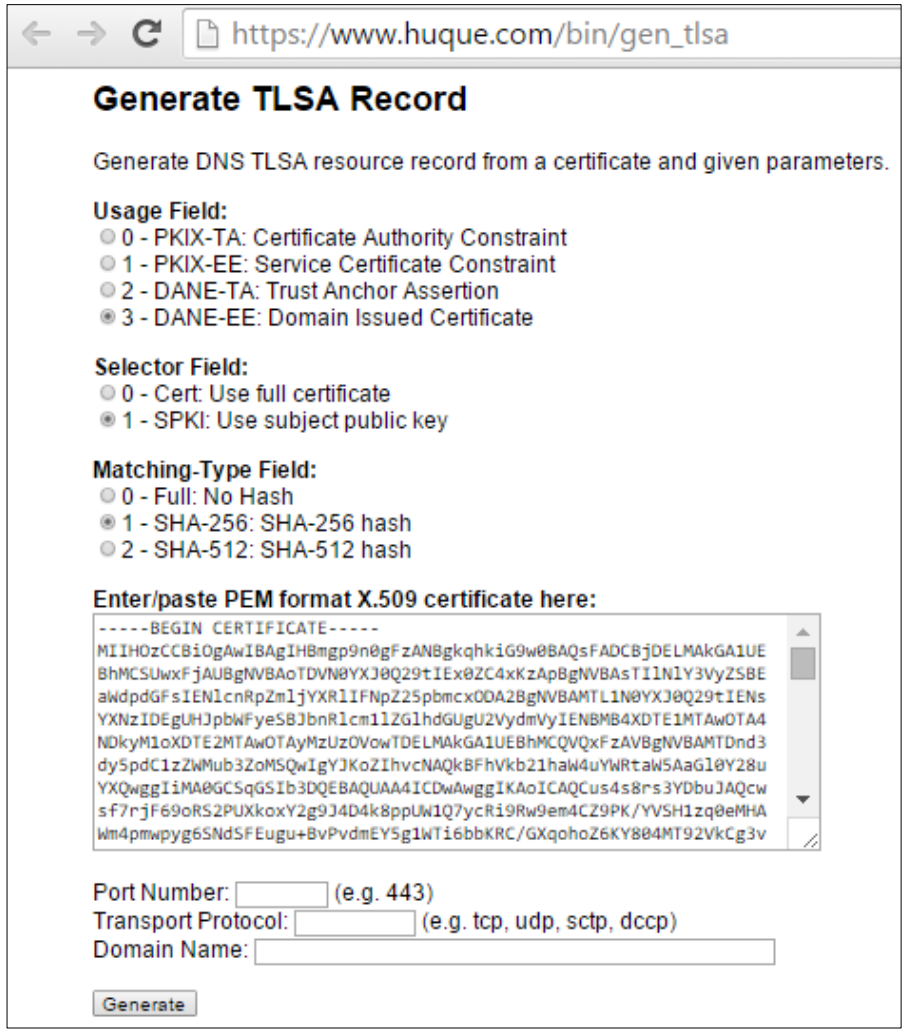
`_25._tcp.mail`	Port 25, Protokoll TCP, Host mail.it-sec.ovh
`IN TLSA`	Ein Record vom Typ TLSA
`3`	Usage = Domain-issued certificate, das heißt der Fingerprint wurde anhand des verwendeten Zertifikats ermittelt, das Zertifikat muss hierzu nicht zwingend von einer getrusteten CA ausgestellt sein. Alternativ dazu könnte auch eine CA oder ein Trust-Anchor verwendet werden.
`0 | 1`	Selector: 0 = Hash des ganzen Zertifikates / 1 = Hash des PublicKey
`1`	Matching Type – entspricht SHA-256
`a46dd6b2…`	der zuvor ermittelte Zertifikats-Fingerprint

Absicherung: SMTP, HTTPS, IMAPS, POP3S

```
root@Sec-NS2:/etc/named/domains# vi zone_it-sec.ovh
…
; DANE / TLSA fuer SMTP und HTTPS: mail.it-sec.ovh (Selector 1 = PubKey)
_25._tcp.mail    IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…
_443._tcp.mail   IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…

; DANE / TLSA fuer HTTPS: it-sec.ovh und www.it-sec.ovh (Selector 1 = PubKey)
_443._tcp.www    IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…
_443._tcp        IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…

; DANE / TLSA fuer POP3S und IMAPS: mail.it-sec.ovh (Selector 1 = PubKey)
_995._tcp.mail   IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…
_993._tcp.mail   IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a…
…
```

Preisfrage: Warum Hash überall gleich?

Komfortable Alternative: TLSA Record Generator



Generate TLSA Record

Generate DNS TLSA resource record from a certificate and given parameters.

Certificate Information:

Serial : 66829f67d2017
Issuer : C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom Class 1 Primary Intermediate Server CA
Subject: C=AT, CN=www.it-sec.ovh/emailAddress=domain.admin@hitco.at
Subject Alternative Name(s): DNS:www.it-sec.ovh, DNS:it-sec.ovh
Certificate Inception: 2015-10-09 08:49:23+00:00 UTC
Certificate Expiration: 2016-10-09 02:35:39+00:00 UTC

TLSA Parameters:

Usage: 3 - DANE-EE: Domain Issued Certificate
Selector: 1 - SPKI: Subject Public Key
Matching Type: 1 - SHA-256: SHA-256 Hash

Service Parameters:

Port: 25
Transport: tcp
Domain name: mail.it-sec.ovh.

Generated DNS TLSA Record:

```
_25._tcp.mail.it-sec.ovh. IN TLSA 3 1 1 a46dd6b2cb43b1f32445d1778410a55d1298c712942483aef03c1a6c6f0c16b5
```

Zertifikatswechsel – Erneuerung der TLSA-Records?

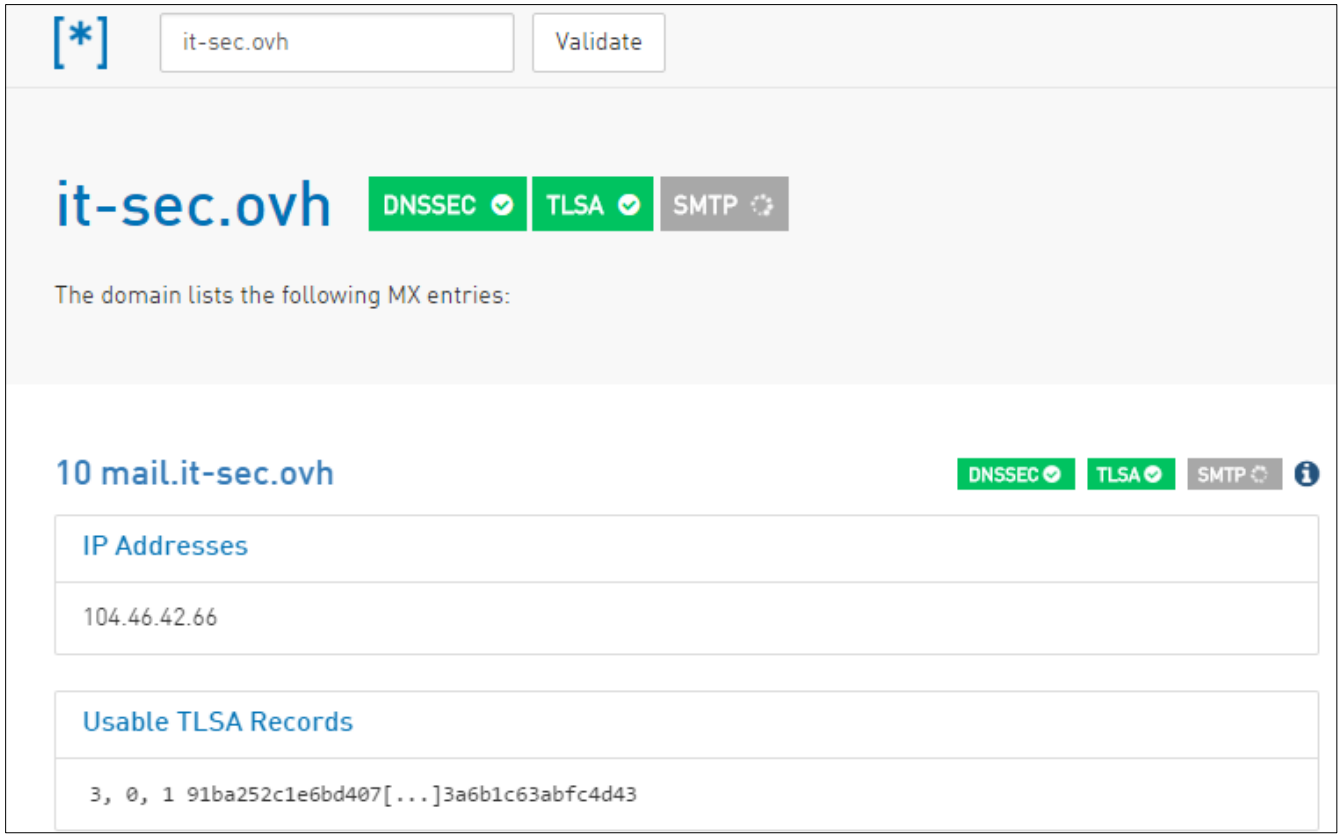
- Wenn gleiches Schlüsselpaar (CSR) weiterverwendet wird nicht nötig
- Ansonsten: TTL beachten, Gültigkeitszeitraum im Auge behalten
- Mehrere TLSA Records parallel für gültig erklären (Überlappender Zeitraum)

- Let‘s Encrypt: Nicht den Default-Automatismus nutzen, sondern CSR

Prüfung TLSA-Record

- Check mit: dane.sys4.de
- Check mit dig

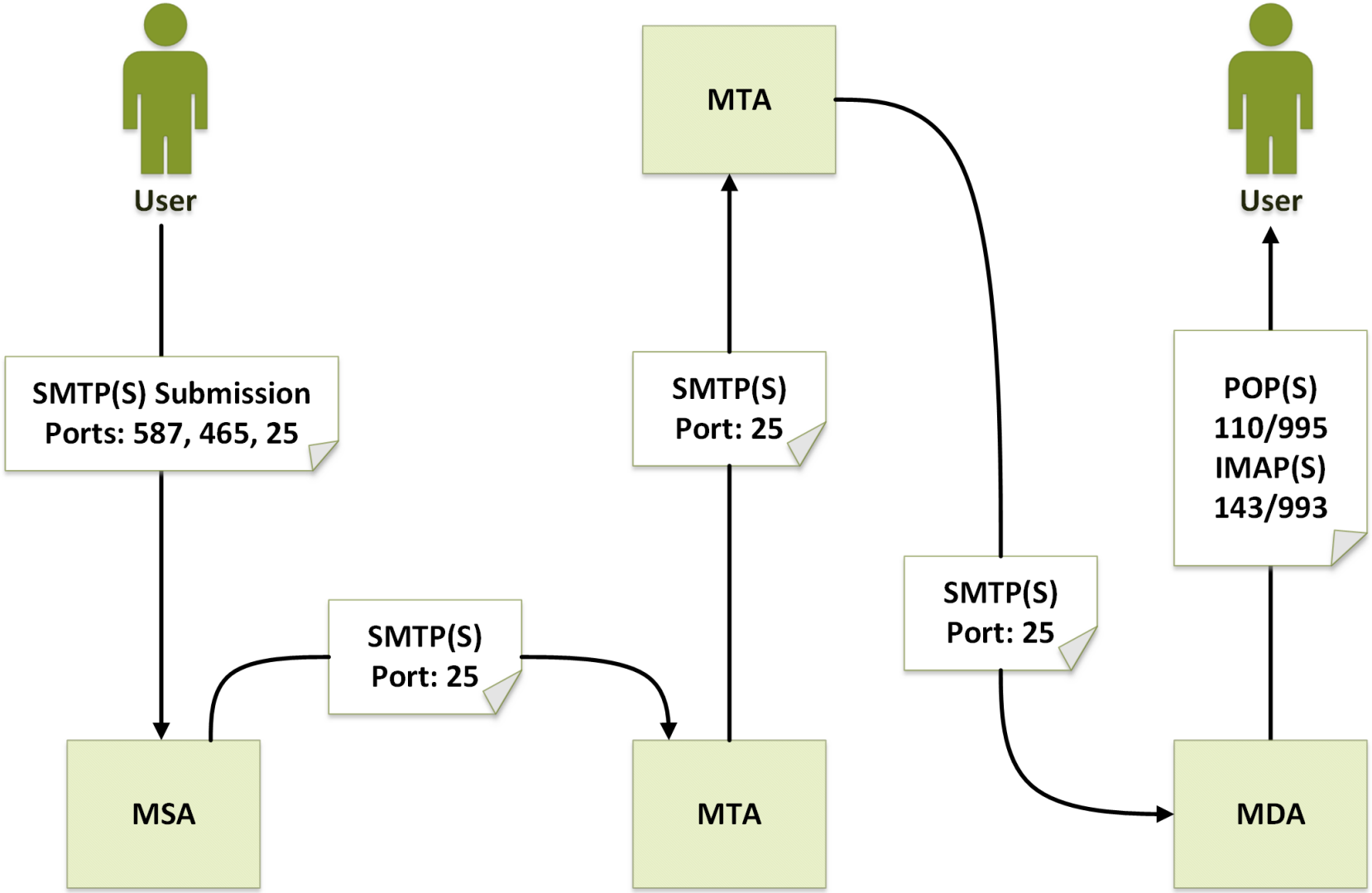
- Mehr Checks später (MailServer)




```
root@Sec-NS2:~# dig +dnssec +noall +answer +multi _25._tcp.mail.it-sec.ovh TLSA
_25._tcp.mail.it-sec.ovh. 1200 IN TLSA 3 1 1 (
                               A46DD6B2CB43B1F32445D1778410A55D1298C7129424
                               83AEF03C1A6C6F0C16B5 )
_25._tcp.mail.it-sec.ovh. 1200 IN RRSIG TLSA 8 5 1200 (
                               20151123165240 20151024155240 60261 it-sec.ovh.
                               LmdSnSHnZKvPiu93SDawfSihB+ye1txY30etpKBhAj5K … = )
```

Mailserver

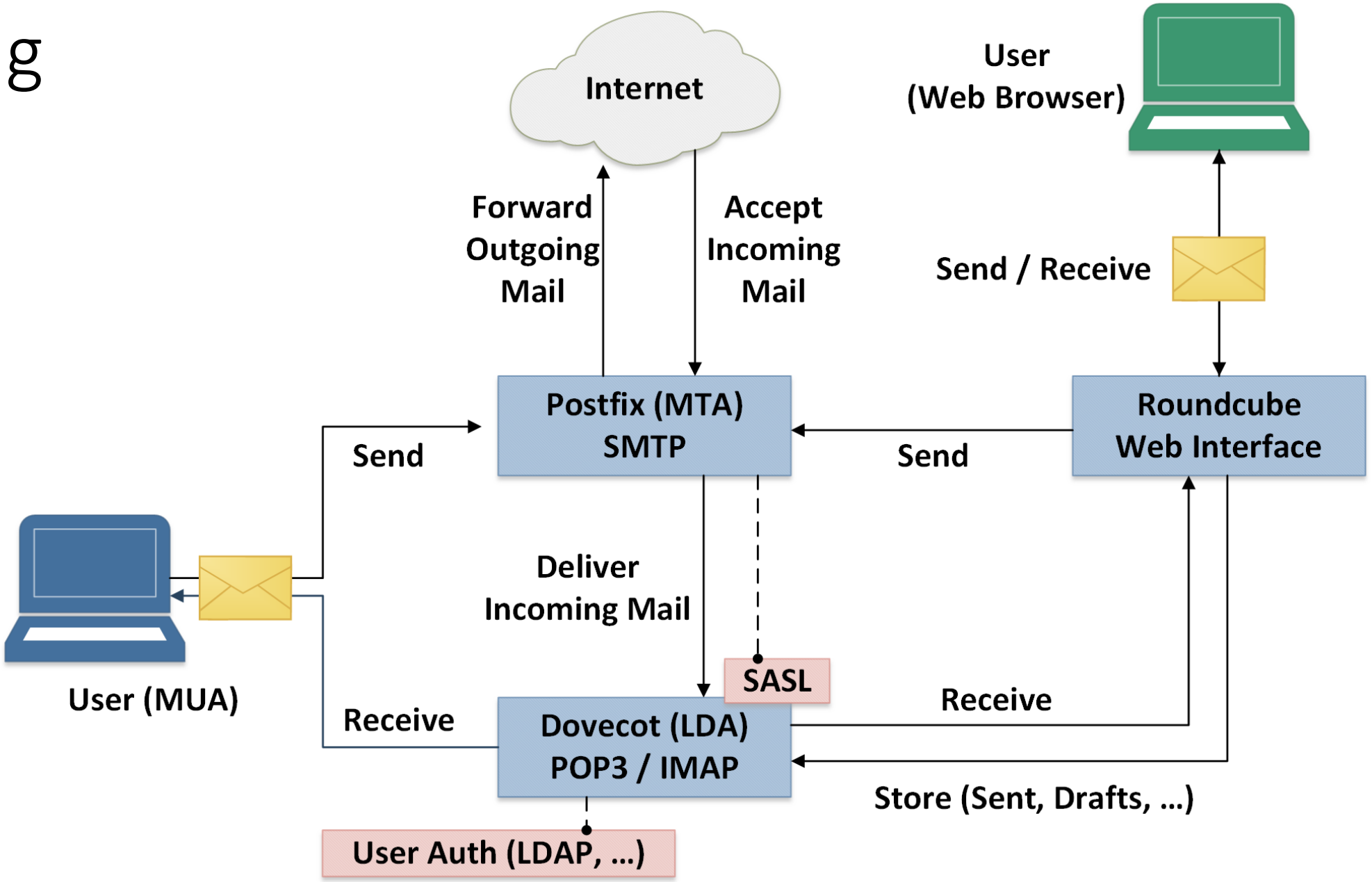
MTA, LDA, MDA, Anbindung MUA, WebMail, …



Realisierung

- CentOS 7.2
- **Debian 8.2**

- BIND **9.9**.4 / **9.9**.
- Postfix **2.11**.3
- Dovecot 2.2
- Apache 2.4.10
- PHP 5.6.13
- MySQL 5.5.46
- RoundCube 1.1.



Mailserver mit DANE – Alternativen?

- Postfix 2.11 erst ab Debian 8 bzw. Ubuntu 14.04 LTS verfügbar
  < 2.11 unter RHEL, CentOS, SLES, …
  evtl. (zuverlässige) Drittanbieter-Pakete nutzen?!
- EXIM ab v4.85
  Weder in Debian noch Ubuntu LTS noch CentOS noch SLES verfügbar
- SendMail – aktuelle 8.15.2 immer noch kein DANE
- Microsoft Exchange – kein DANE
  Drittanbieter-Erweiterung: CryptoFilter

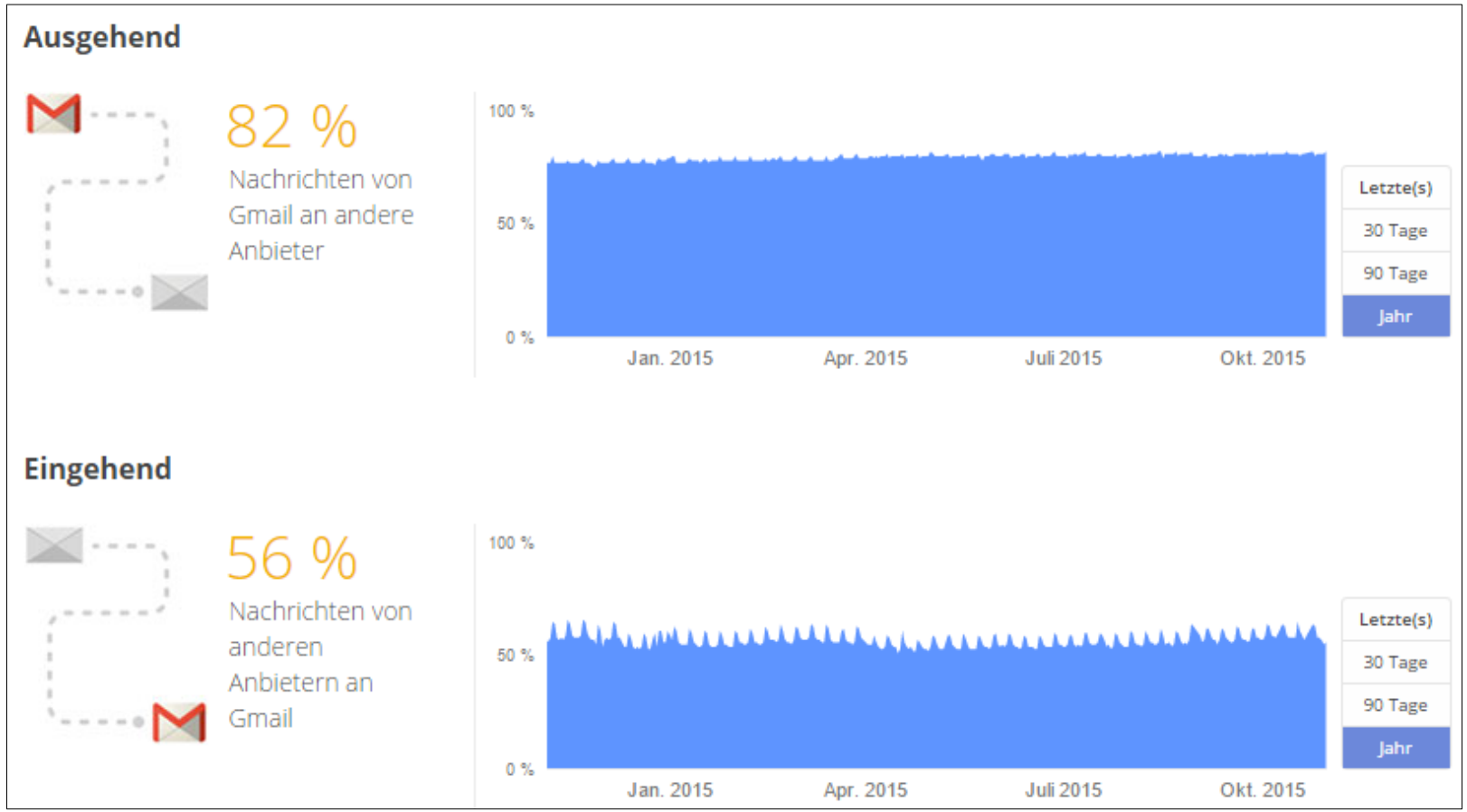
Postfix-Konfiguration

- Allgemein: Mailserver-Konfiguration grundsätzlich (beim ersten mal) knifflig
- Zertifikat + Chain konfigurieren
- SSL/TLS konfigurieren – für MTA: Default-Config (Cipher)
  schlechte Crypto besser als gar keine Krypto (Plaintext-Fallback)
- Submission-Port: Mandatory TLS, nur „gute“ Cipher-Suiten erlaubt
- Authentifizierung nur mit STARTTLS und am Submission-Port zulassen
- DANE: straight forward

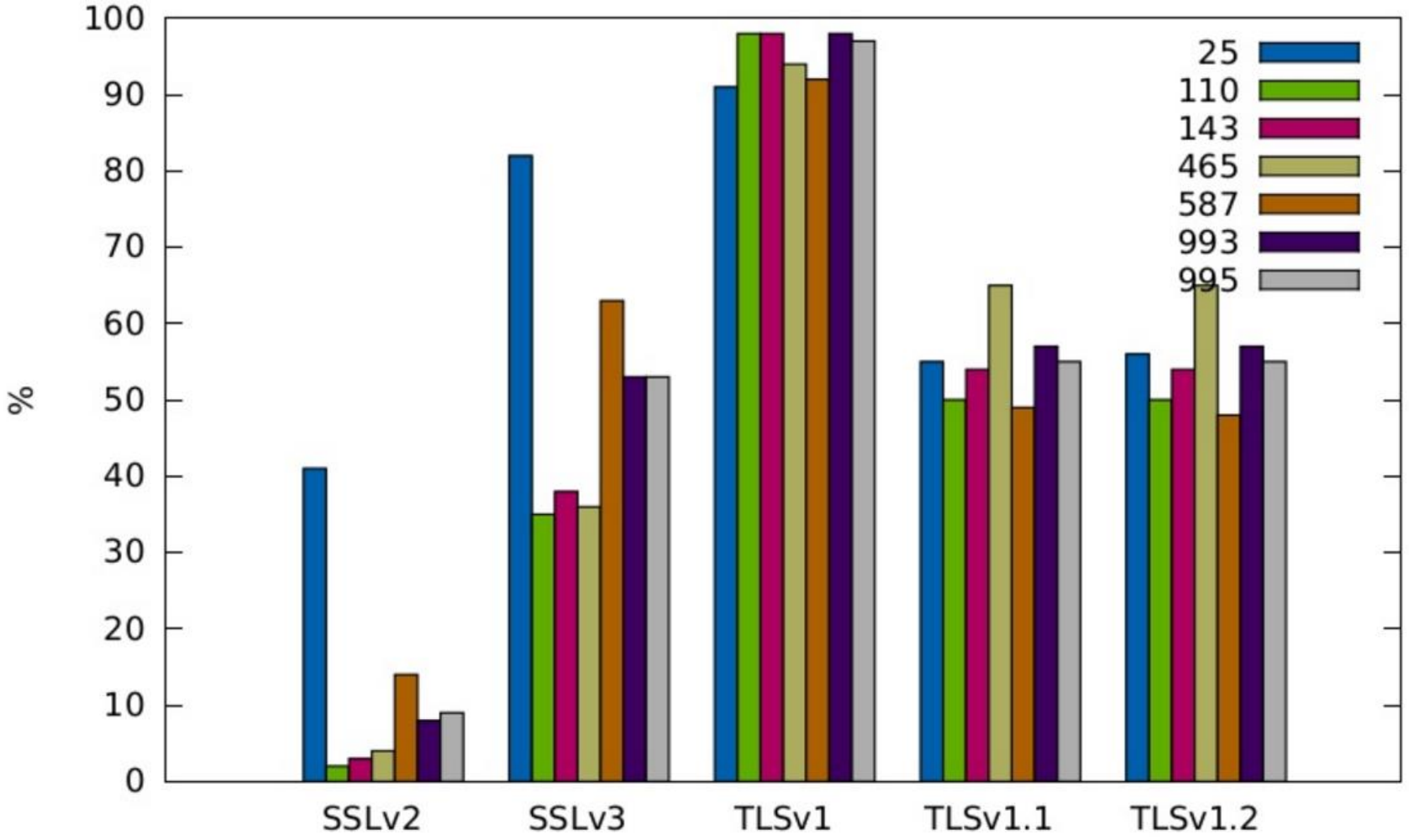
```
root@Sec-NS2:/etc/postfix# postconf -e "smtp_dns_support_level=dnssec"
root@Sec-NS2:/etc/postfix# postconf -e "smtp_tls_security_level=dane"
```

Verbreitung von TLS und DANE bei MTA‘s

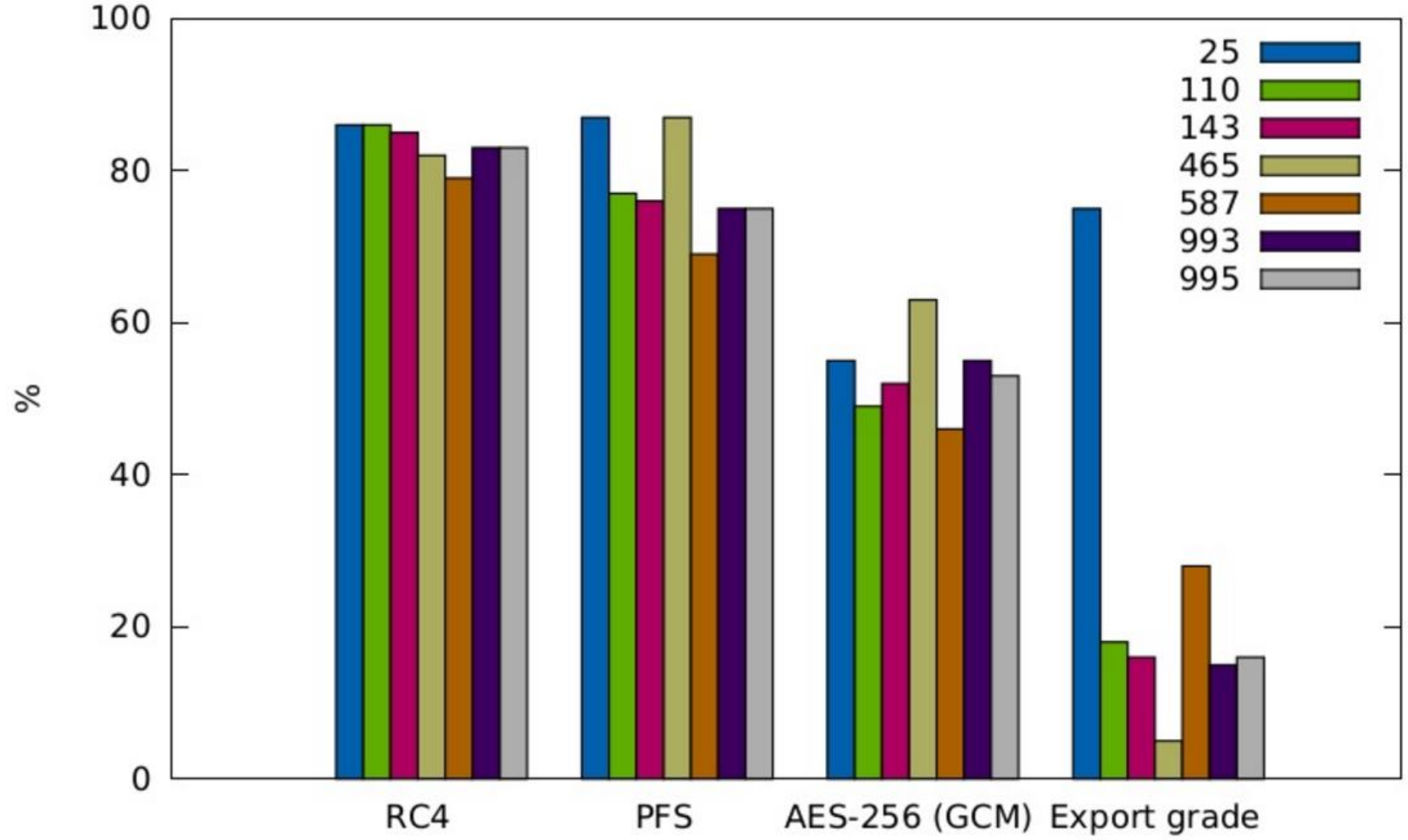
- TLS: siehe z.B.:
  Google Transparency Report
- DANE:
  Starker Trend in .de
  Dzt. aber nur vereinzelt
- Mail.de, posteo.de
  + viele Ankündigungen!



Mailserver-Studie: SSL / TLS-Protokollversionen

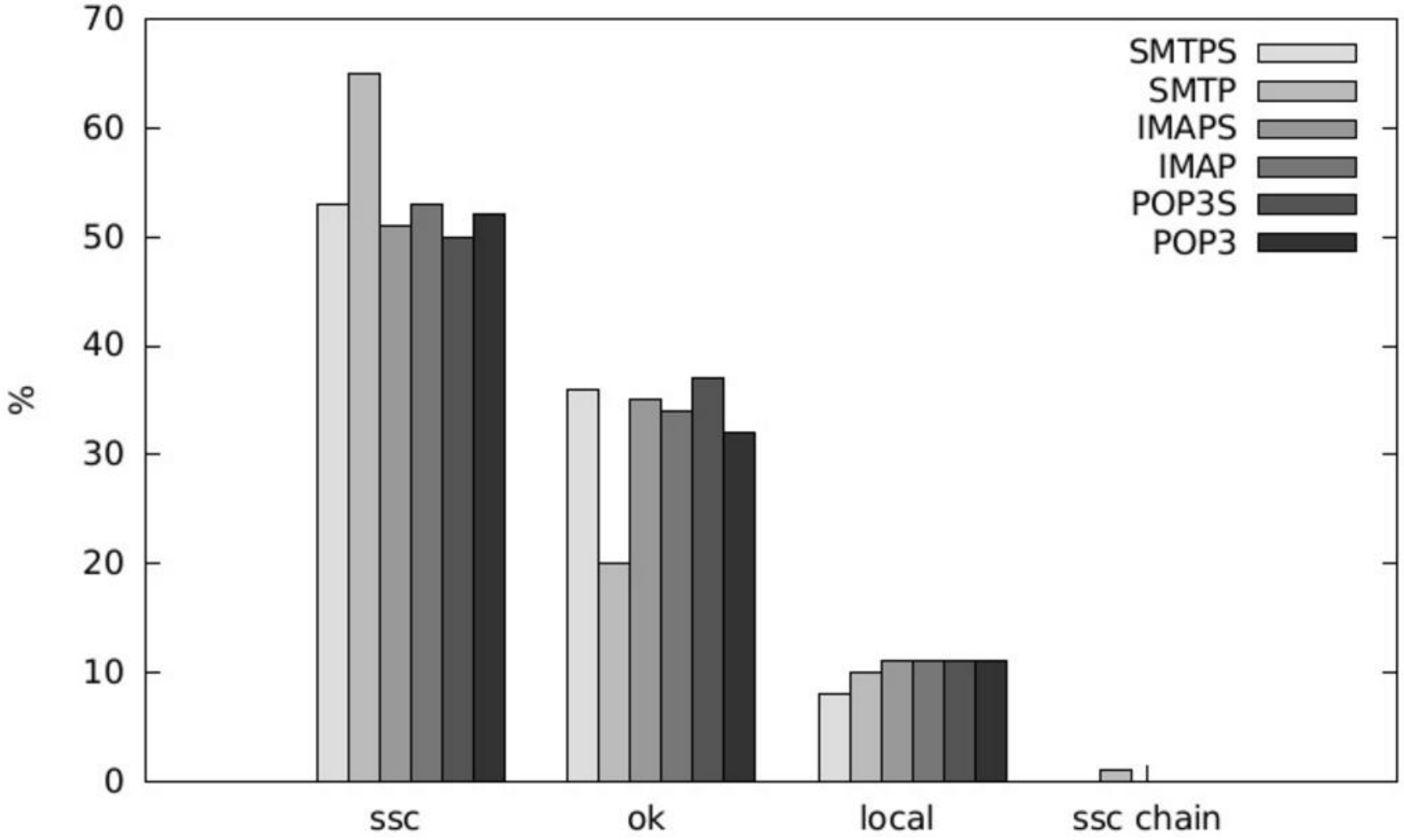


Mailserver-Studie: Cipher-Suite Unterstützung



Mailserver-Studie: eingesetzte Zertifikate

- ssc = self signed Cert
- local = unbekannte CA
- ssc chain = CertChain fehlt

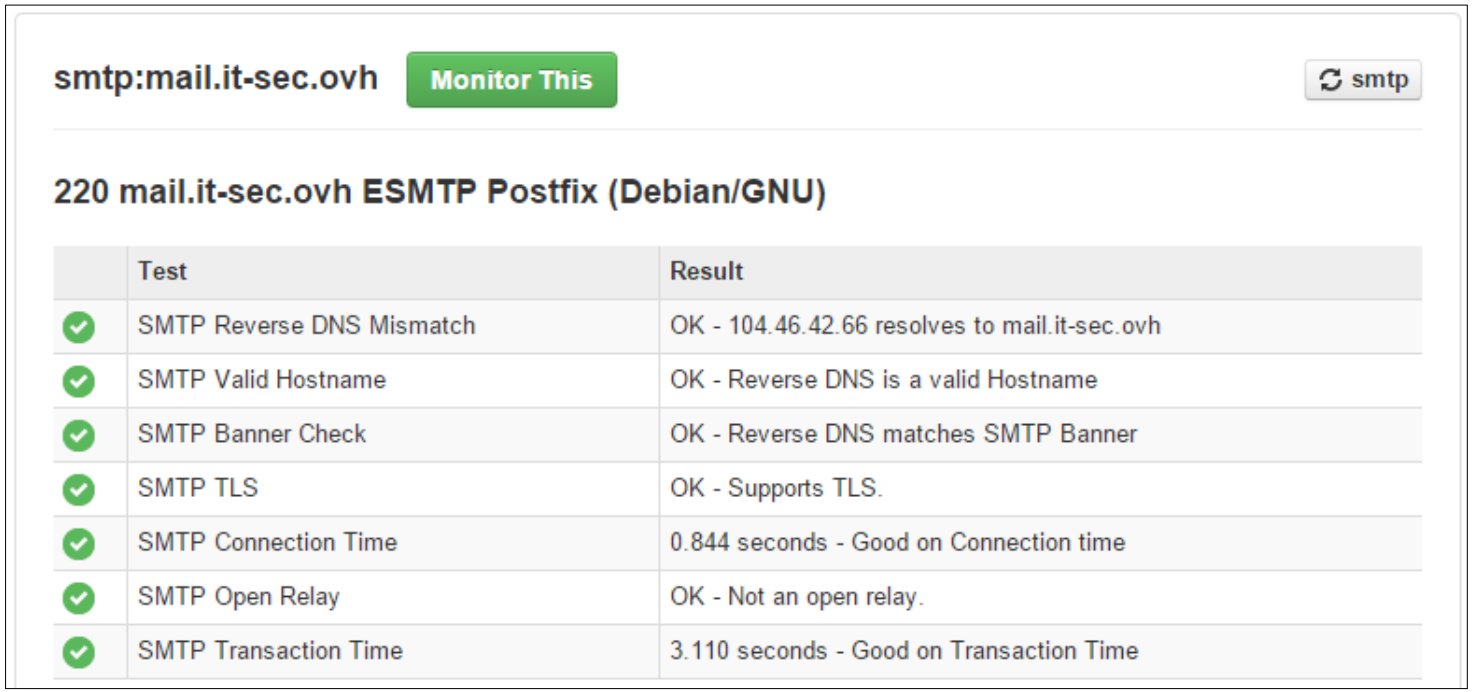


Dovecot: POP3 & IMAP

- Setup straight forward
- Zertifikat konfigurieren
- Nur TLS zulassen, Cipher-String gemäß BetterCrypto.org „CipherString B“
- Dovecot stellt SASL (Simple Authentication and Security Layer) für Postfix bereit

Mailserver-Checks

- Basis-Check: MxToolbox.com



- Versand & Empfang: CheckTLS.com

```
root@Sec-NS2:~# echo Test |
mail --subject=ncgyrmpfbizs4 -r root@it-sec.ovh test@TestSender.CheckTLS.com
```

- Detailierte Analyse per Reply-Mail

CheckTLS.com

Mail-Empfang Check

```
Trying TLS on mail.it-sec.ovh[104.46.42.66] (10):
 seconds    test stage and result
[000.106]   Connected to server
[000.212]<--220 mail.it-sec.ovh ESMTP Postfix (Debian/GNU)
[000.213]   We are allowed to connect
[000.213]-->EHLO checktls.com
[000.318]<--250-mail.it-sec.ovh
            250-PIPELINING
            250-SIZE 10240000
            250-VRFY
            250-ETRN
            250-STARTTLS
            250-ENHANCEDSTATUSCODES
            250-8BITMIME
            250 DSN
[000.319]   We can use this server
[000.319]   TLS is an option on this server
[000.319]-->STARTTLS
[000.424]<--220 2.0.0 Ready to start TLS
[000.425]   STARTTLS command works on this server
[000.687]   Cipher in use: ECDHE-RSA-AES256-GCM-SHA384
[000.687]   Connection converted to SSL
[000.707]   Certificate 1 of 3 in chain:
            subject= /C=AT/CN=mail.it-sec.ovh/emailAddress=domain.admin@hitco.at
            issuer= /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server CA
[000.726]   Certificate 2 of 3 in chain:
            subject= /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server CA
            issuer= /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority
[000.745]   Certificate 3 of 3 in chain:
            subject= /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority
            issuer= /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority
[000.745]   Cert VALIDATED: ok
[000.745]   Cert Hostname VERIFIED (mail.it-sec.ovh = mail.it-sec.ovh)
[000.745]~~>EHLO checktls.com
[000.852]<~~250-mail.it-sec.ovh
            250-PIPELINING
            250-SIZE 10240000
            250-VRFY
            250-ETRN
            250-ENHANCEDSTATUSCODES
            250-8BITMIME
            250 DSN
[000.853]   TLS successfully started on this server
[000.853]~~>MAIL FROM:<test@checktls.com>
[000.959]<~~250 2.1.0 Ok
[000.959]   Sender is OK
[000.959]~~>RCPT TO:<root@it-sec.ovh>
[001.066]<~~250 2.1.5 Ok
[001.066]   Recipient OK - E-mail address proofed
```

OpenSSL
s_client -starttls

```
root@Sec-NS2:/etc/postfix# echo |
openssl s_client -starttls smtp -connect mail.it-sec.ovh:25 -CApath /etc/ssl/certs
CONNECTED(00000003)
depth=2 C = IL, O = StartCom Ltd., OU = Secure Digital Certificate Signing, CN = StartCom Certification Authority
verify return:1
depth=1 C = IL, O = StartCom Ltd., OU = Secure Digital Certificate Signing, CN = StartCom Class 1 Primary
Intermediate Server CA
verify return:1
depth=0 C = AT, CN = mail.it-sec.ovh, emailAddress = domain.admin@hitco.at
verify return:1
---
Certificate chain
 0 s:/C=AT/CN=mail.it-sec.ovh/emailAddress=domain.admin@hitco.at
   i:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server CA
 1 s:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server CA
   i:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIHPTCCBiWgAwIBAgIHBmgq6WqV/jANBgkqhkiG9w0BAQsFADCBjDELMAkGA1UE
…
Q9T7Zmpt4uSbajHzQPpqH/WHOumRbxCXbAqxHel4YgwB
-----END CERTIFICATE-----
subject=/C=AT/CN=mail.it-sec.ovh/emailAddress=domain.admin@hitco.at
issuer=/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1
Primary Intermediate Server CA
---
No client certificate CA names sent
---
SSL handshake has read 4492 bytes and written 456 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: A36A301FF84C195F70497772A05DE8587530B05BC9AAE487B9F5A5D42D1E8764
    Session-ID-ctx:
    Master-Key: 5A34269B28D311A5566EED55BEC533DDB75DBD75EC84FDAED0B33FC32DFFDBB41884C36E4E5C97CDE8228CAE7349F50F
    Key-Arg   : None
```

Prüfung: DH-Parameter, 2048bit ?

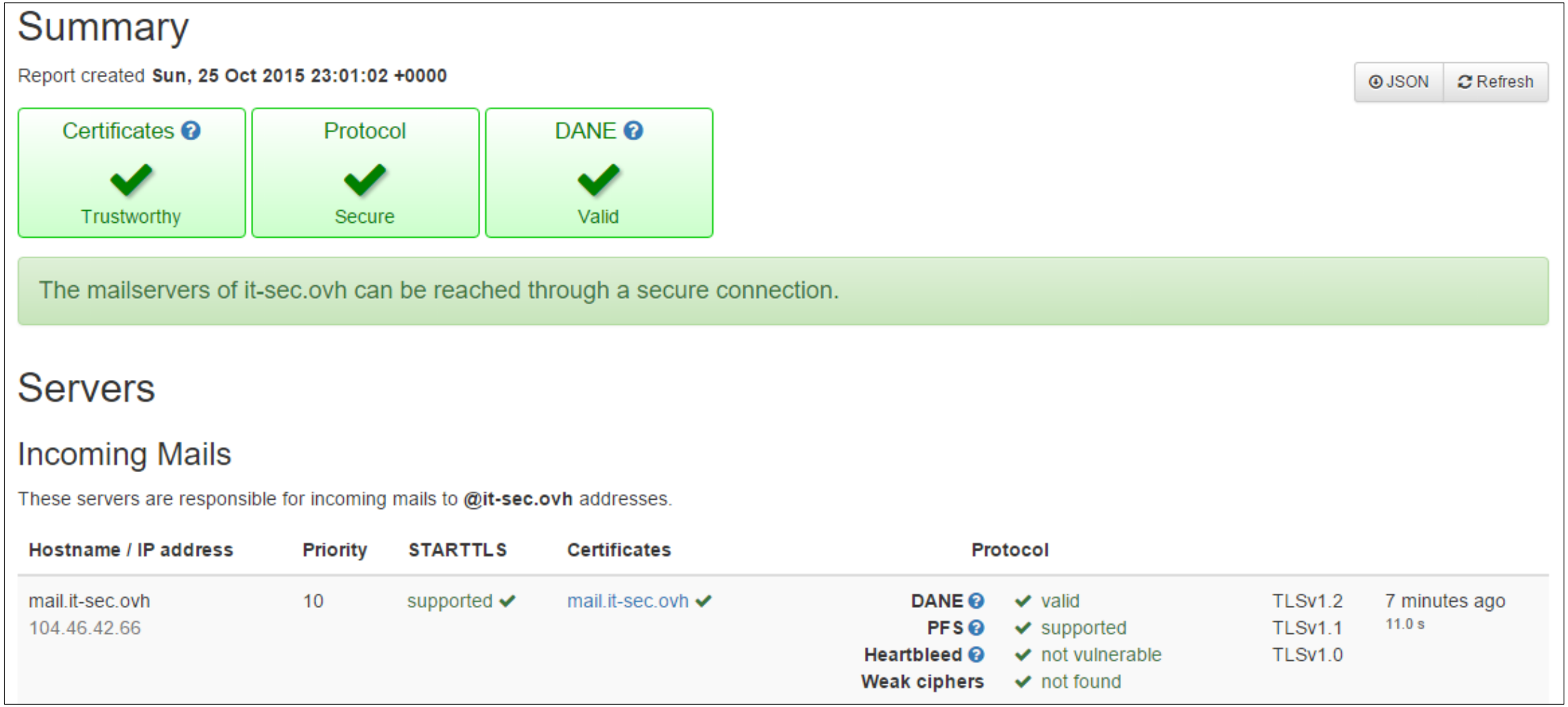
```
C:\OpenSSL-Win64>openssl version
OpenSSL 1.0.2d 9 Jul 2015

C:\OpenSSL-Win64>echo |  ↵
openssl s_client -starttls smtp -cipher "EDH" -connect mail.it-sec.ovh:25
…
Peer signing digest: SHA512
Server Temp Key: DH, 2048 bits
…
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : DHE-RSA-AES256-GCM-SHA384
…
```

DANE-Check

- PostTLS-Finger
- Mail-Empfangs-Check

```
root@Sec-NS2:~# posttls-finger -f -l dane -L summary it-sec.ovh
posttls-finger: Connected to mail.it-sec.ovh[104.46.42.66]:25
posttls-finger: < 220 mail.it-sec.ovh ESMTP Postfix (Debian/GNU)
posttls-finger: > EHLO mail.it-sec.ovh
posttls-finger: < 250-mail.it-sec.ovh
posttls-finger: < 250-PIPELINING
posttls-finger: < 250-SIZE 10240000
posttls-finger: < 250-VRFY
posttls-finger: < 250-ETRN
posttls-finger: < 250-STARTTLS
posttls-finger: < 250-ENHANCEDSTATUSCODES
posttls-finger: < 250-8BITMIME
posttls-finger: < 250 DSN
posttls-finger: > STARTTLS
posttls-finger: < 220 2.0.0 Ready to start TLS
posttls-finger: Verified TLS connection established to mail.it-sec.ovh[104.46.42.66]:25:
TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
posttls-finger: > EHLO mail.it-sec.ovh
posttls-finger: < 250-mail.it-sec.ovh
posttls-finger: < 250-PIPELINING
posttls-finger: < 250-SIZE 10240000
posttls-finger: < 250-VRFY
posttls-finger: < 250-ETRN
posttls-finger: < 250-ENHANCEDSTATUSCODES
posttls-finger: < 250-8BITMIME
posttls-finger: < 250 DSN
posttls-finger: > QUIT
posttls-finger: < 221 2.0.0 Bye
```

DANE-Empfangs-Check: dane.sys4.de



Summary

Report created **Sun, 25 Oct 2015 23:01:02 +0000**

JSON | Refresh

Certificates	Protocol	DANE
✔ Trustworthy	✔ Secure	✔ Valid

The mailservers of it-sec.ovh can be reached through a secure connection.

Servers

Incoming Mails

These servers are responsible for incoming mails to **@it-sec.ovh** addresses.

Hostname / IP address	Priority	STARTTLS	Certificates	Protocol			
mail.it-sec.ovh 104.46.42.66	10	supported ✔	mail.it-sec.ovh ✔	**DANE** ✔ valid **PFS** ✔ supported **Heartbleed** ✔ not vulnerable **Weak ciphers** ✔ not found		TLSv1.2 TLSv1.1 TLSv1.0	7 minutes ago 11.0 s

weitere Details
dane.sys4.de

Host	TLS Version & Cipher	
mail.it-sec.ovh (104.46.42.66)	TLSv1.2 AECDH-AES256-SHA ✔	vor 13 Stunden

Zertifikate

mail.it-sec.ovh — Zuerst gesehen: vor 12 Stunden

Zertifikatskette

mail.it-sec.ovh ✔
348 Tagen verbleibend 4096 bit sha256WithRSAEncryption

↳ StartCom Class 1 Primary Intermediate Server CA ✔
2546 Tagen verbleibend 2048 bit sha256WithRSAEncryption

↳ StartCom Certification Authority (Zertifikat ist selbst signiert.) ✔
7632 Tagen verbleibend 4096 bit sha256WithRSAEncryption

Subjekt

Land (C)	AT
Common Name (CN)	mail.it-sec.ovh
E-Mail	domain.admin@hitco.at
Alternative Namen	mail.it-sec.ovh it-sec.ovh

+ mehr anzeigen

DANE

DNS-based Authentication of Named Entities (DANE) ist ein Protokoll um X.509-Zertifikate mit TLSA-Einträgen im DNS zu verknüpfen und per DNSSEC abzusichern.

Name	Options	DNSSEC	Matches
_25._tcp.mail.it-sec.ovh	DANE-EE: Domain Issued Certificate Use subject public key SHA-256 Hash	✔ gültig	✔ gültig

Mailserver Check: Versand mit DANE

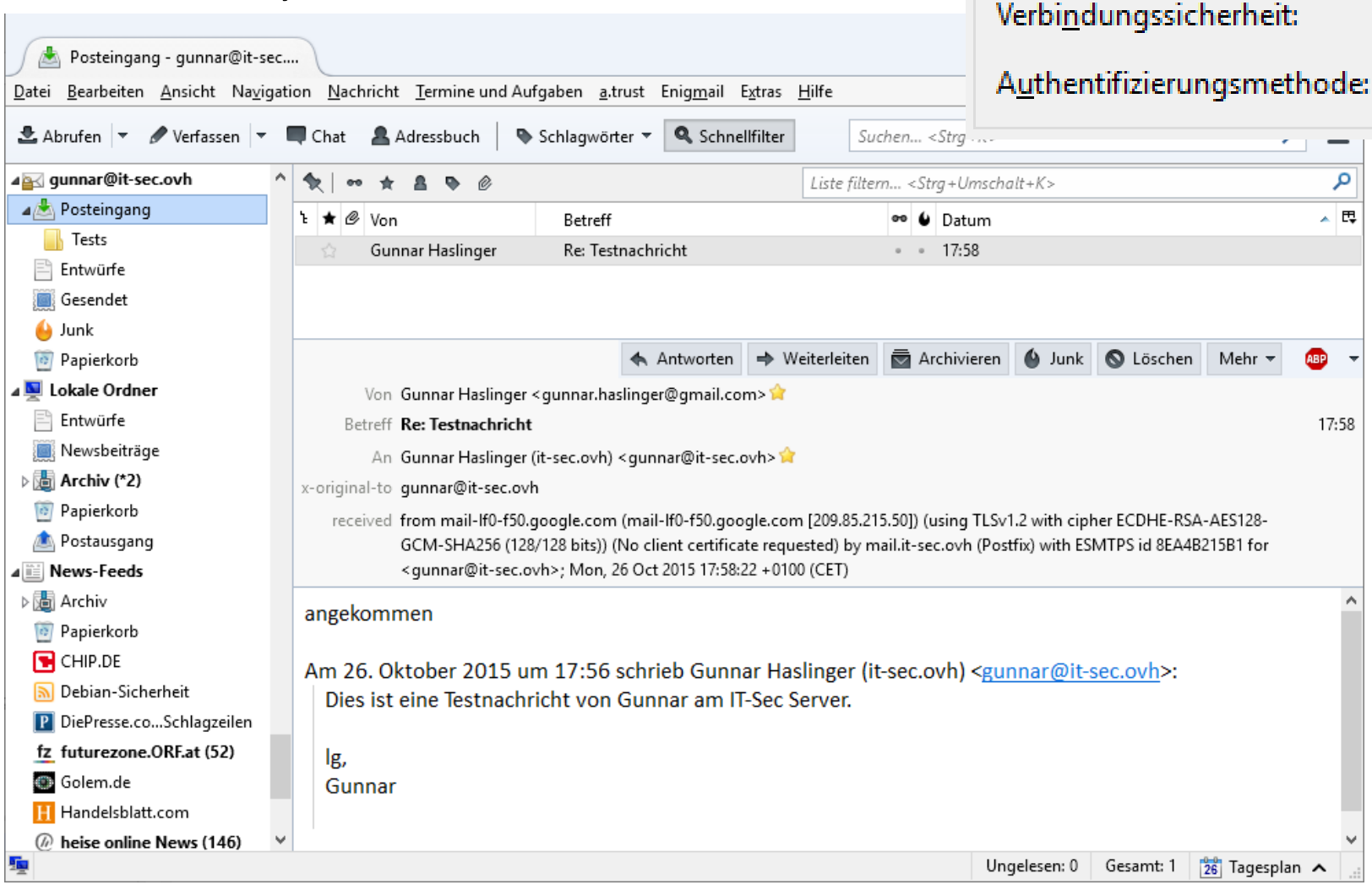
- Gegenstelle mit DANE Unterstützung erforderlich, z.B.: posteo.de

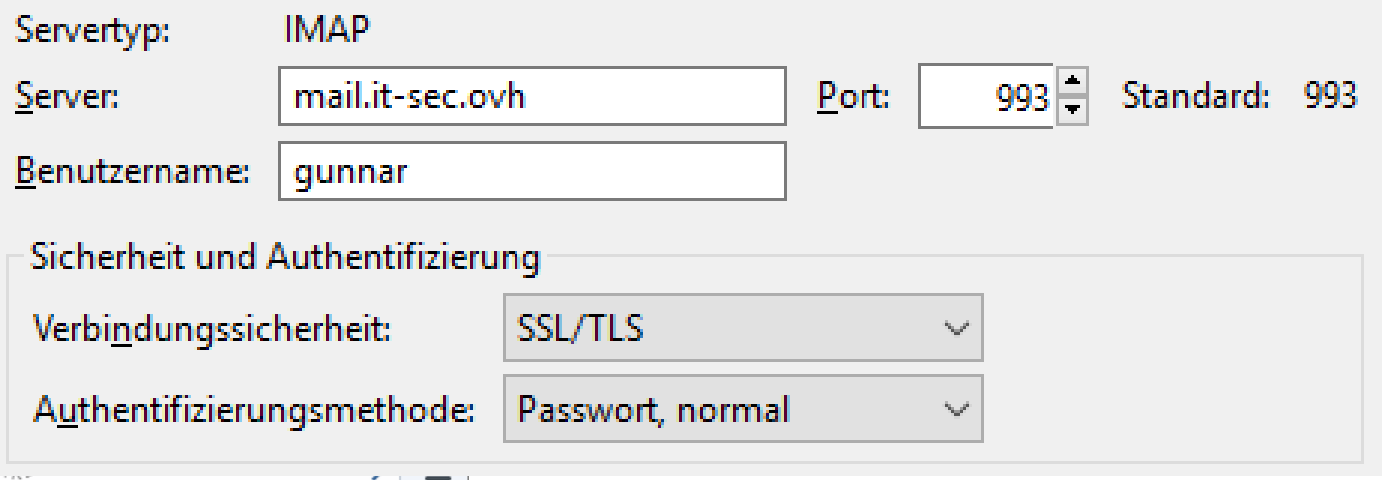
```
root@Sec-NS2:~# echo Testmail | sendmail Testmail-test@posteo.de
root@Sec-NS2:~# tail -f /var/log/mail.log
Oct 26 12:30:10 Sec-NS2 postfix/smtp[2086]:
Verified TLS connection established to mx02.posteo.de[89.146.194.165]:25: TLSv1.2 with
cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
Oct 26 12:30:12 Sec-NS2 postfix/smtp[2086]:
1601920723: host mx02.posteo.de[89.146.194.165] said:
450 4.1.1 <Testmail-test@posteo.de>: Recipient address rejected: unverified address:
Recipient address lookup failed (in reply to RCPT TO command)
```

```
Trusted TLS connection established to mx00.emig.gmx.net[212.227.15.9]:25: TLSv1.2 with
cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)
```

```
Anonymous TLS connection established to mx1.bmlv.gv.at[193.171.152.59]:25: TLSv1.2 with
cipher ADH-AES256-GCM-SHA384 (256/256 bits)
```

IMAPS, POP3S Test





TestSSL.sh Script

```
root@Sec-NS2:/tmp# wget -q https://testssl.sh/testssl.sh
root@Sec-NS2:/tmp# wget -q https://testssl.sh/mapping-rfc.txt
root@Sec-NS2:/tmp# chmod 755 ./testssl.sh
```

```
root@Sec-NS2:/tmp# ./testssl.sh mail.it-sec.ovh:993
root@Sec-NS2:/tmp# ./testssl.sh mail.it-sec.ovh:995
```

sec-ns2.cloudapp.net - PuTTY

```
--> Testing protocols (via sockets except TLS 1.2 and SPDY/NPN)

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      offered
TLS 1.1    offered
TLS 1.2    offered (OK)
SPDY/NPN   not offered
```

sec-ns2.cloudapp.net - PuTTY

```
--> Testing server defaults (Server Hello)

TLS server extensions          server name, renegotiation info, EC point formats, session ticket, heartbeat
Session Tickets RFC 5077       300 seconds
Server key size                4096 bit
Signature Algorithm            SHA256 with RSA
Fingerprint / Serial           SHA1 F046CC9
                               SHA256 91BA2
Common Name (CN)               mail.it-sec.
subjectAltName (SAN)           mail.it-sec.
Issuer                         StartCom Cla
EV cert (experimental)         no
Certificate Expiration         >= 60 days (
# of certificates provided     2
Certificate Revocation List    http://crl.s
OCSP URI                       http://ocsp.
OCSP stapling                  not offered
TLS timestamp                  random value
```

sec-ns2.cloudapp.net - PuTTY

```
--> Testing server preferences

Has server cipher order?     yes (OK)
Negotiated protocol          TLSv1.2
Negotiated cipher            ECDHE-RSA-AES128-GCM-SHA256
Cipher order
    TLSv1:     ECDHE-RSA-AES128-SHA DHE-RSA-AES128-SHA AES128-SHA ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA AES256-SHA
    TLSv1.1:   ECDHE-RSA-AES128-SHA DHE-RSA-AES128-SHA AES128-SHA ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA AES256-SHA
    TLSv1.2:   ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-
RSA-AES128-SHA256 DHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-A
ES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA AES256-GCM-SHA384
AES256-SHA256 AES256-SHA
```

Web-Mail

Apache, PHP, MySQL, RoundCube WebMail

Plattform: LAMP-Stack auf Debian 8.2

- Apache 2.4.10
  - Mod SSL
  - Mod Headers
  - Mod Rewrite
  - …
- PHP 5.6.13
- MySQL 5.5.46

Apache: SSL-Konfiguration

- Cipher-String: Anlehnung an BetterCrypto.org, jedoch selbst gebaut
- Inkonsistenzen im BetterCrypto-Guide „CipherString B“ aufgedeckt
- Zertifikat + Chain konfiguriert
- OCSP-Stapling aktiviert
- HTTP Strict Transport Security (HSTS)
- HTTP Public Key Pinning (HPKP) – Kapitel (von mir) nun in BetterCrypto enthalten

Apache

vHost SSL Config

```
SSLEngine on
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
SSLCompression off
SSLUseStapling on

# 1/2 Jahr HSTS header (60*60*24*182=15724800sek), inklusive Subdomains
Header always set Strict-Transport-Security "max-age=15724800 ; includeSubDomains"

# HTTP Public Key Pinning für Zertifikat (HPKP), 90 Tage (60*60*24*90=7776000)
# mail.it-sec.ovh.crt PubKey = pG3WsstDsfMkRdF3hBClXRKYxxKUJIOu8DwabG8MFrU=
# StartCom Certification Authority: "5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU="
# zweiter Backup-Key: "i89r5g0BAe/9ubBIuTxrW5phVO8lv7cBvXxK/evFhXw="
Header always set Public-Key-Pins
    "pin-sha256=\"pG3WsstDsfMkRdF3hBClXRKYxxKUJIOu8DwabG8MFrU=\";
     pin-sha256=\"5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU=\";
     pin-sha256=\"i89r5g0BAe/9ubBIuTxrW5phVO8lv7cBvXxK/evFhXw=\";
     max-age=7776000;
     report-uri=\"https://report-uri.io/report/866c4f253035d817119b9401f6116434\""

SSLCipherSuite '-ALL:ECDH+aRSA+AES:DH+aRSA+AES:aRSA+kRSA+AES:+AES256'

SSLCertificateFile      /etc/ssl/certs/mail.it-sec.ovh.crt
SSLCertificateKeyFile   /etc/ssl/private/it-sec.ovh.key
SSLCertificateChainFile /etc/ssl/certs/startssl.chain.class1.server.crt
```

Cipher-Suite: BetterCrypto „CipherString B“

- Enthält Camellia
- Priorisiert DH gegenüber ECDH
- Präferiert AES256 gegenüber AES128
- Unterstützt keine Java 1.7 Clients
- Ist sehr lang:

```
root@Sec-NS2:~# openssl ciphers -v 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:
EECDH+aRSA+SHA256:EECDH:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:
!EXP:!PSK:!DSS:!RC4:!SEED:!IDEA:!ECDSA:kEDH:CAMELLIA128-SHA:AES128-SHA'
```

- Mein Cipher-String:

Resultat: `'-ALL:ECDH+aRSA+AES:DH+aRSA+AES:aRSA+kRSA+AES:+AES256'`

```
root@Sec-NS2:~# openssl ciphers -v '-ALL:ECDH+aRSA+AES:DH+aRSA+AES:aRSA+kRSA+AES:+AES256'
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA  Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256     TLSv1.2 Kx=ECDH Au=RSA  Enc=AES(128)    Mac=SHA256
ECDHE-RSA-AES128-SHA        SSLv3   Kx=ECDH Au=RSA  Enc=AES(128)    Mac=SHA1
DHE-RSA-AES128-GCM-SHA256   TLSv1.2 Kx=DH   Au=RSA  Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256       TLSv1.2 Kx=DH   Au=RSA  Enc=AES(128)    Mac=SHA256
DHE-RSA-AES128-SHA          SSLv3   Kx=DH   Au=RSA  Enc=AES(128)    Mac=SHA1
AES128-GCM-SHA256           TLSv1.2 Kx=RSA  Au=RSA  Enc=AESGCM(128) Mac=AEAD
AES128-SHA256               TLSv1.2 Kx=RSA  Au=RSA  Enc=AES(128)    Mac=SHA256
AES128-SHA                  SSLv3   Kx=RSA  Au=RSA  Enc=AES(128)    Mac=SHA1
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA  Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384     TLSv1.2 Kx=ECDH Au=RSA  Enc=AES(256)    Mac=SHA384
ECDHE-RSA-AES256-SHA        SSLv3   Kx=ECDH Au=RSA  Enc=AES(256)    Mac=SHA1
DHE-RSA-AES256-GCM-SHA384   TLSv1.2 Kx=DH   Au=RSA  Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256       TLSv1.2 Kx=DH   Au=RSA  Enc=AES(256)    Mac=SHA256
DHE-RSA-AES256-SHA          SSLv3   Kx=DH   Au=RSA  Enc=AES(256)    Mac=SHA1
AES256-GCM-SHA384           TLSv1.2 Kx=RSA  Au=RSA  Enc=AESGCM(256) Mac=AEAD
AES256-SHA256               TLSv1.2 Kx=RSA  Au=RSA  Enc=AES(256)    Mac=SHA256
AES256-SHA                  SSLv3   Kx=RSA  Au=RSA  Enc=AES(256)    Mac=SHA1

ECDH = Ephemeral Elliptic curve Diffie-Hellman
EDH  = Ephemeral Diffie-Hellman
GCM  = Galois-Counter-Mode realisiert AEAD = Authenticated Encryption with Associated Data
```

Client Kompatibilität

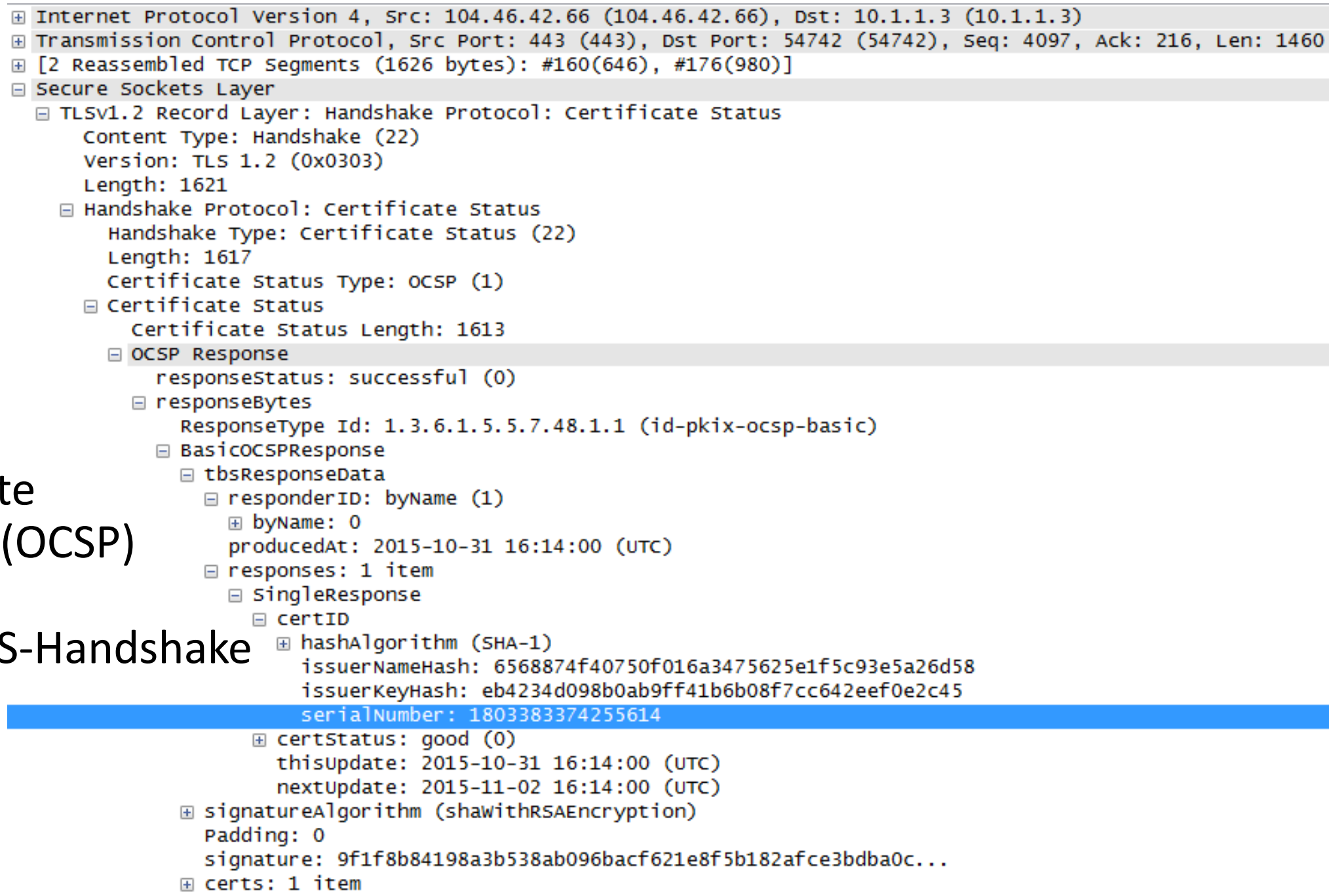
Test mit Qualys SSL Labs

Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Chrome 43 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Firefox 39 / OS X	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
IE 6 / XP	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
IE 8 / XP	Incorrect certificate because this client doesn't support SNI		Fail[2]
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
IE 11 / Win 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
IE 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
IE 11 / Win Phone 8.1 Update	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
Edge 12 / Win 10 (Build 10130)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Java 6u45	Incorrect certificate because this client doesn't support SNI		Fail[2]
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
Java 8u31	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
Safari 6 / iOS 6.0.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA FS	128
Safari 7 / iOS 7.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
Safari 7 / OS X 10.9	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
Safari 8 / iOS 8.4	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128
Safari 8 / OS X 10.10	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 FS	128

OCSP Stapling

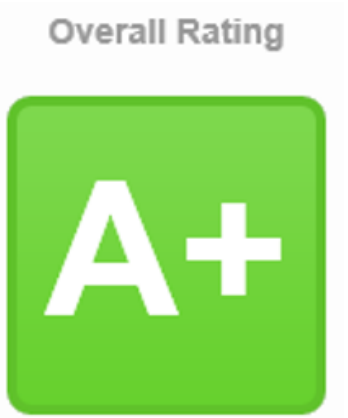
Online Certificate Status Protocol (OCSP)

Response im TLS-Handshake



HTTP Strict Transport Security (HSTS)

- Sorgt für das „+“ beim SSLLabs.com WebServer TLS-Check




```
root@Sec-NS2:/etc/apache2/mods-available# a2enmod headers

root@Sec-NS2:/etc/apache2/sites-available# vi mail.it-sec.ovh_ssl.conf
…
# 1/2 Jahr HSTS header (60*60*24*182=15724800sek), inklusive Subdomains
Header always set Strict-Transport-Security "max-age=15724800 ; includeSubDomains"
…
```

HTTP Public Key Pinning (HPKP) als Ergänzung zu DANE

- DANE für WebSites (HTTPS) möglich aber nicht gebräuchlich
- Trust on First Use (TOFU) Prinzip
- Base64 encodierter Hash des Public-Key des Zertifikates

- Cert PubKey-Pinning
- CA PubKey Pinning
- Reserve-Key!

```
root@Sec-NS2:/etc/apache2/mods-available# a2enmod headers

root@Sec-NS2:/etc/apache2/sites-available# vi mail.it-sec.ovh_ssl.conf
…
# HTTP Public Key Pinning für Zertifikat (HPKP), 90 Tage (60*60*24*90=7776000)
# mail.it-sec.ovh.crt PubKey = pG3WsstDsfMkRdF3hBClXRKYxxKUJIOu8DwabG8MFrU=
# StartCom Certification Authority: "5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU="
# zweiter Backup-Key: "i89r5g0BAe/9ubBIuTxrW5phVO8lv7cBvXxK/evFhXw="
Header always set Public-Key-Pins   ↵
"pin-sha256=\"pG3WsstDsfMkRdF3hBClXRKYxxKUJIOu8DwabG8MFrU=\";     ↵
 pin-sha256=\"5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU=\";     ↵
 pin-sha256=\"i89r5g0BAe/9ubBIuTxrW5phVO8lv7cBvXxK/evFhXw=\";     ↵
 max-age=7776000;
 report-uri=\"https://report-uri.io/report/866c4f253035d817119b9401f6116434\";"
…
```

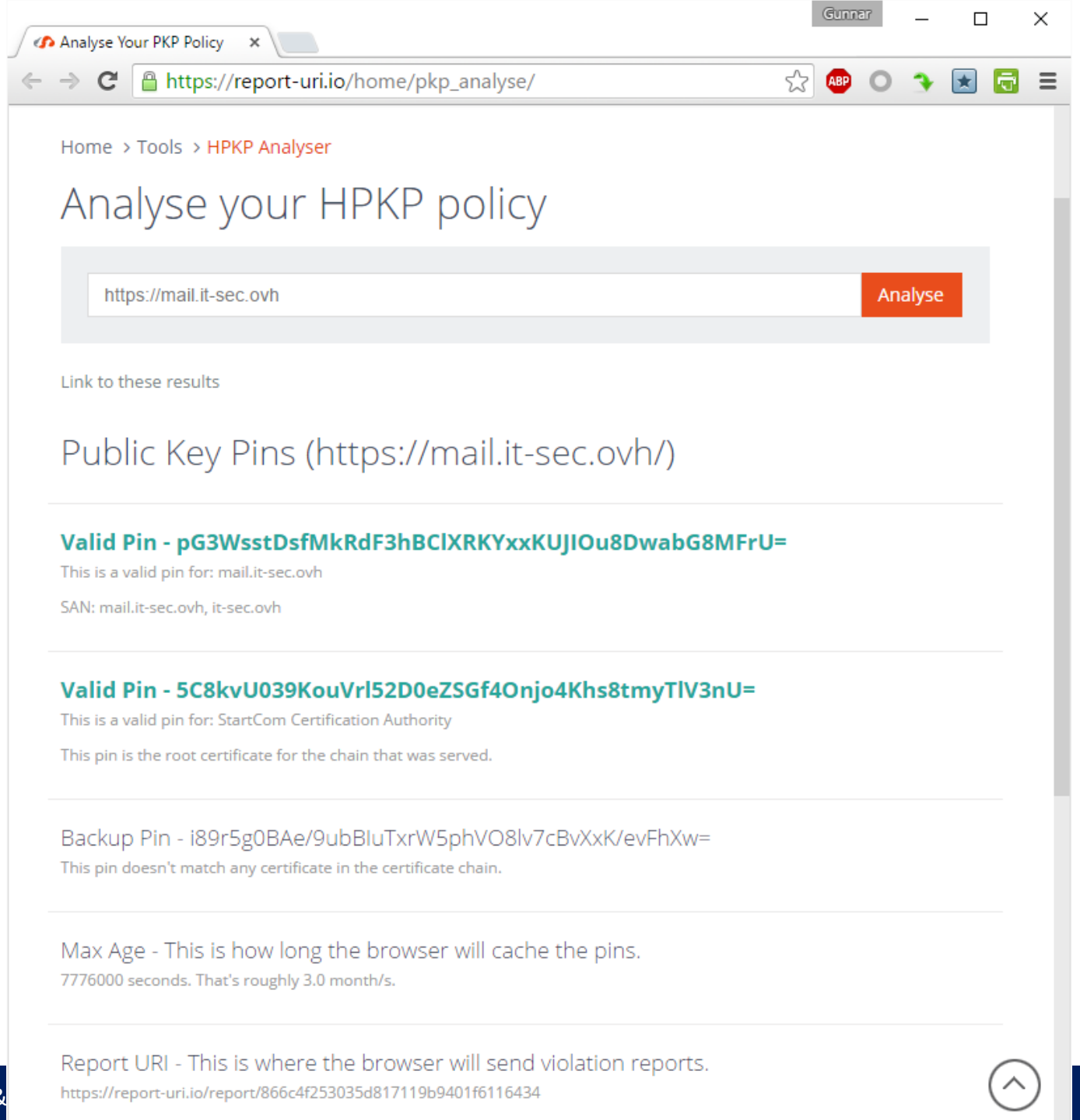
HTTP Public Key Pinning – Hash erzeugen

- OpenSSL

```
root@Sec-NS2:/etc/ssl/private# openssl x509 -in mail.it-sec.ovh.crt -pubkey -noout |
 openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64
writing RSA key
pG3WsstDsfMkRdF3hBClXRKYxxKUJIOu8DwabG8MFrU=

root@Sec-NS2:/etc/ssl/private# openssl rsa -in it-sec.ovh.backup.key -pubout -outform der
 | openssl dgst -sha256 -binary | openssl enc -base64
writing RSA key
i89r5g0BAe/9ubBIuTxrW5phVO8lv7cBvXxK/evFhXw=
```

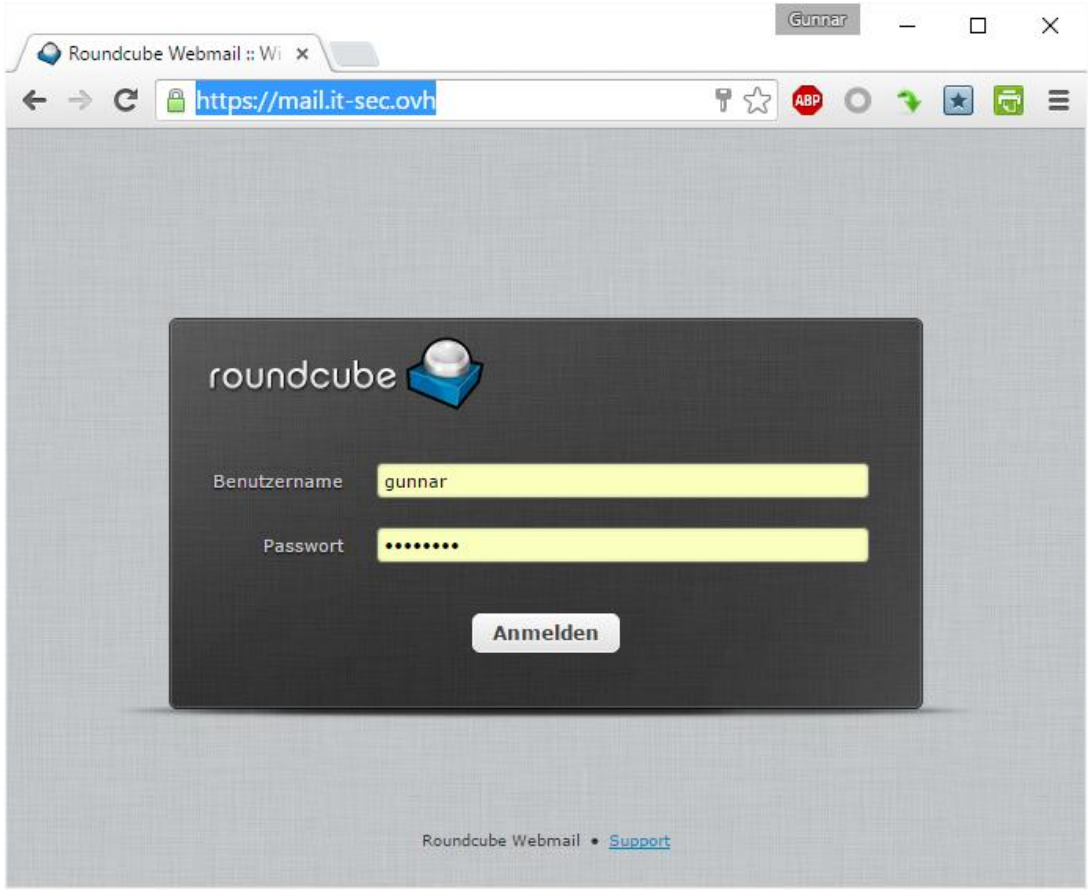
- WebService https://report-uri.io

Prüfung:
HTTP Key Pinning

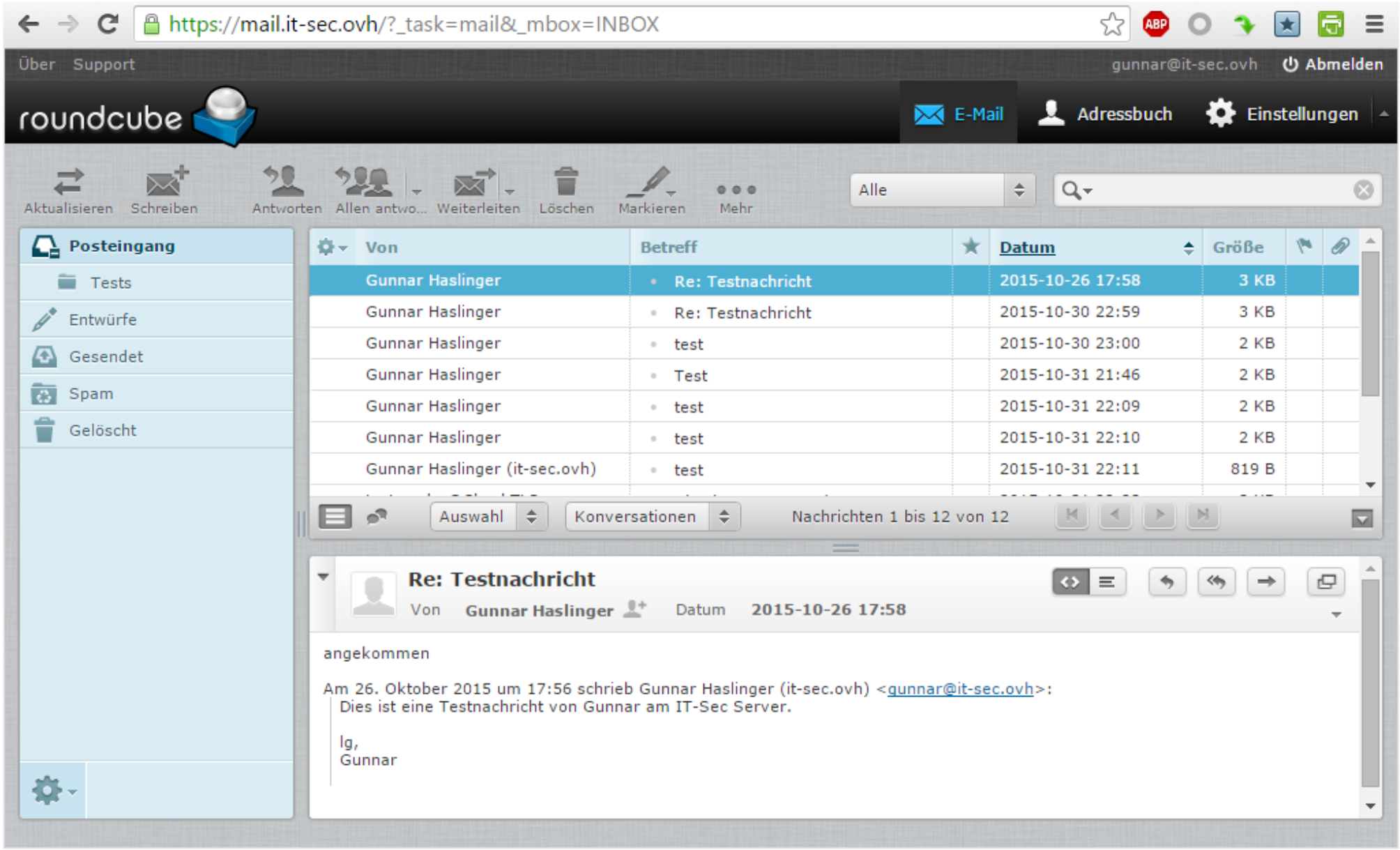


RoundCube Webmail

- Download (Sourcen) von SourceForce (kein Paket für Debian 8.2 im Repo)
- Einrichtung mit Web-Installer gemäß Doku
- Greift über LocalHost auf IMAP zu
- Versand: Nutzt Postfix über LocalHost
- Adressbuch & User-Settings: mySQL-DB
- Straight Forward, siehe Doku

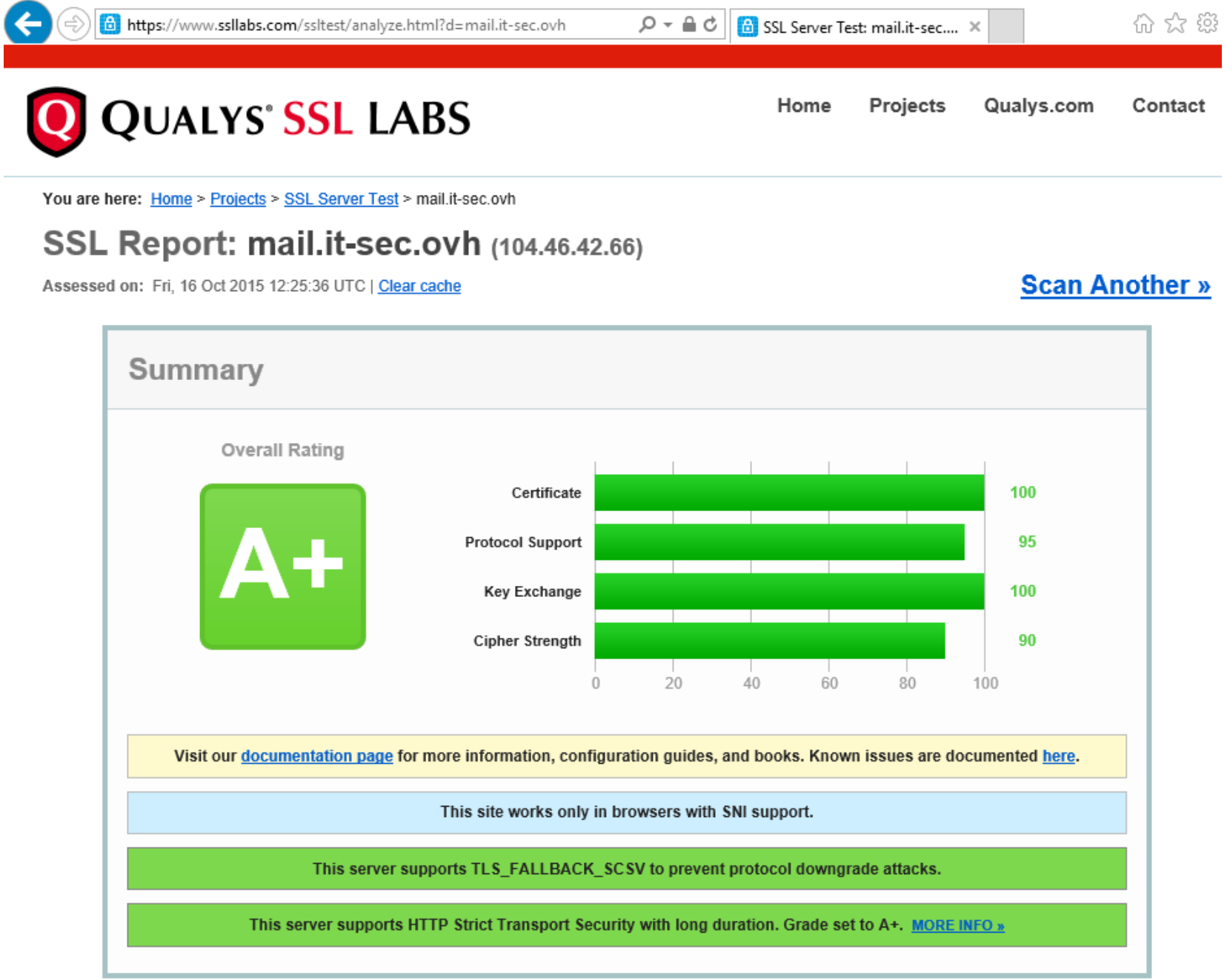


RoundCube WebMail



Checks:

Qualys SSL Labs
SSLLabs.com



Qualys SSL Labs

- Server-Zertifikat
- 4096bit RSA
- SHA256
- OCSP verfügbar

Server Key and Certificate #1

Common names	mail.it-sec.ovh
Alternative names	mail.it-sec.ovh it-sec.ovh
Prefix handling	Not required for subdomains
Valid from	Thu, 08 Oct 2015 13:25:42 UTC
Valid until	Sat, 08 Oct 2016 11:48:46 UTC (expires in 11 months and 29 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	StartCom Class 1 Primary Intermediate Server CA
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Qualys SSL Labs

- Protokolle
- Cipher Suites

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 4096 bits (p: 512, g: 1, Ys: 511) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Qualys SSL Labs

- Protokoll Details

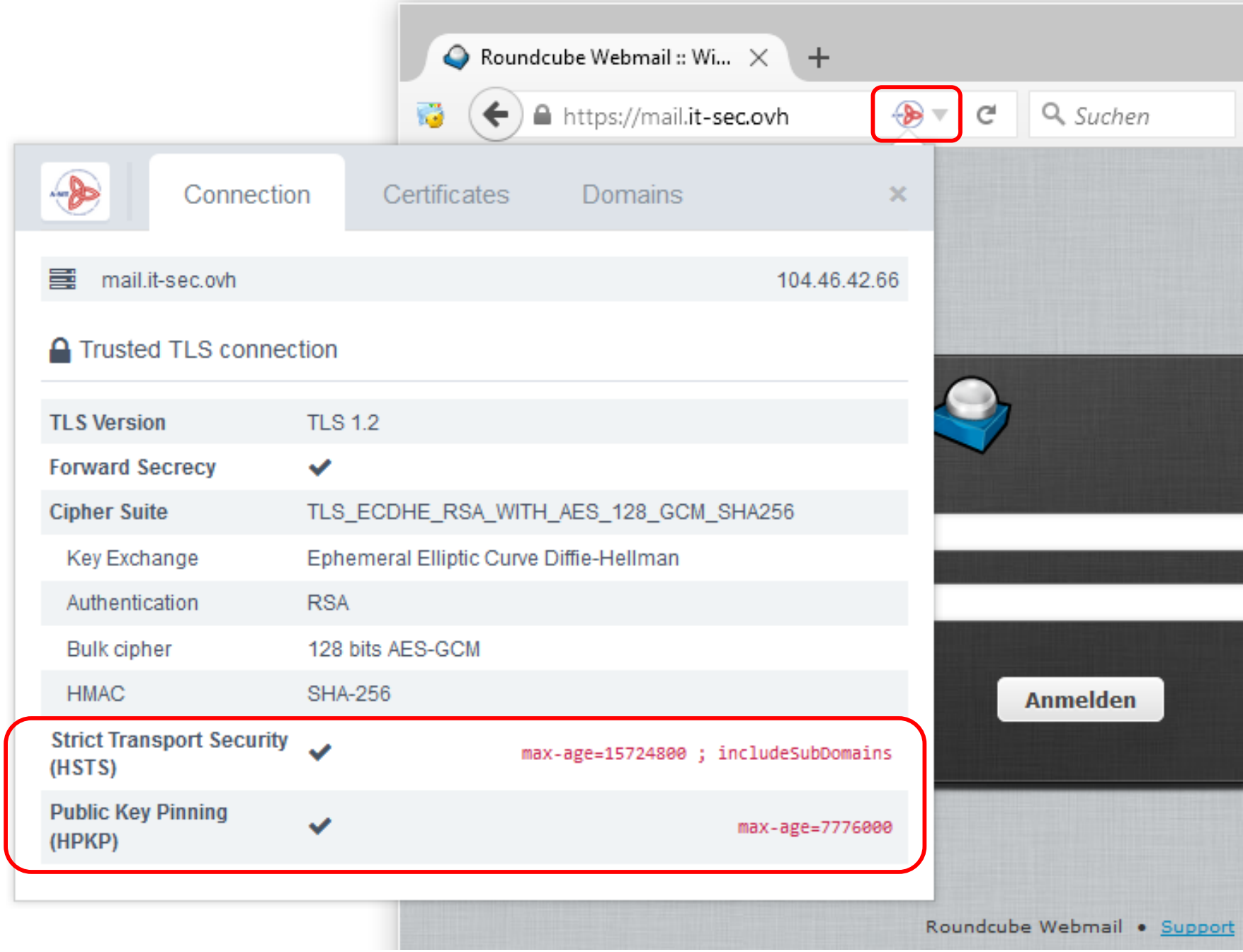
- OCSP Stapling aktiviert
- HTTP Strict Transport Security
- HTTP Public Key Pinning

- Sichere Cipher-Suiten
- Nur TLS, kein SSL aktiv
- …

Protocol Details

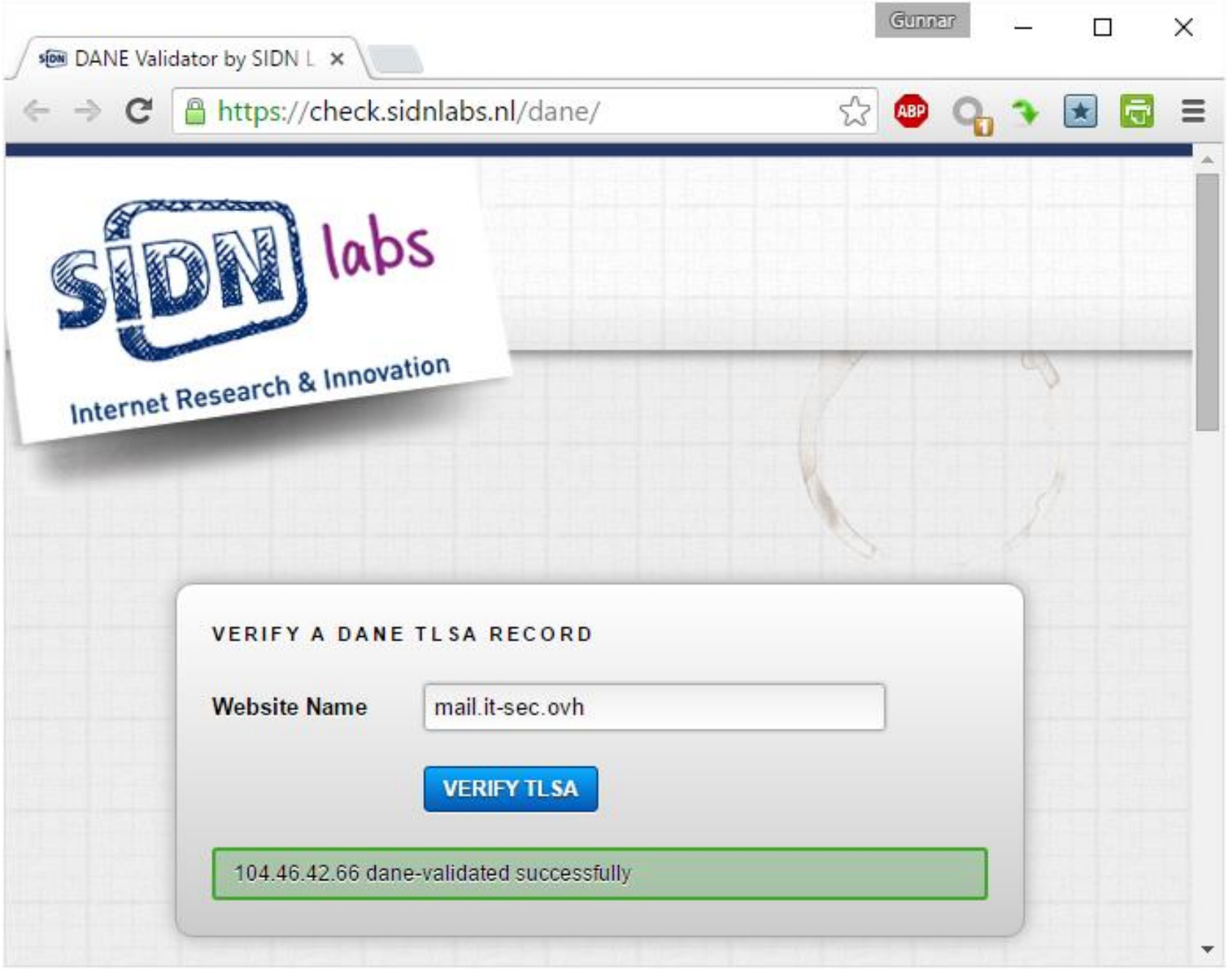
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=15724800 ; includeSubDomains
Public Key Pinning (HPKP)	**Yes** pin-sha256="pG3WsstDsfMkRdF3hBCIXRKYxxKUJIOu8DwabG8MFrU="; pin-sha256="5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU="; max-age=7776000; report-uri="https://report-uri.io/report/866c4f253035d817119b9401f8116434"; includeSubDomains
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

A-Sit
Firefox PlugIn



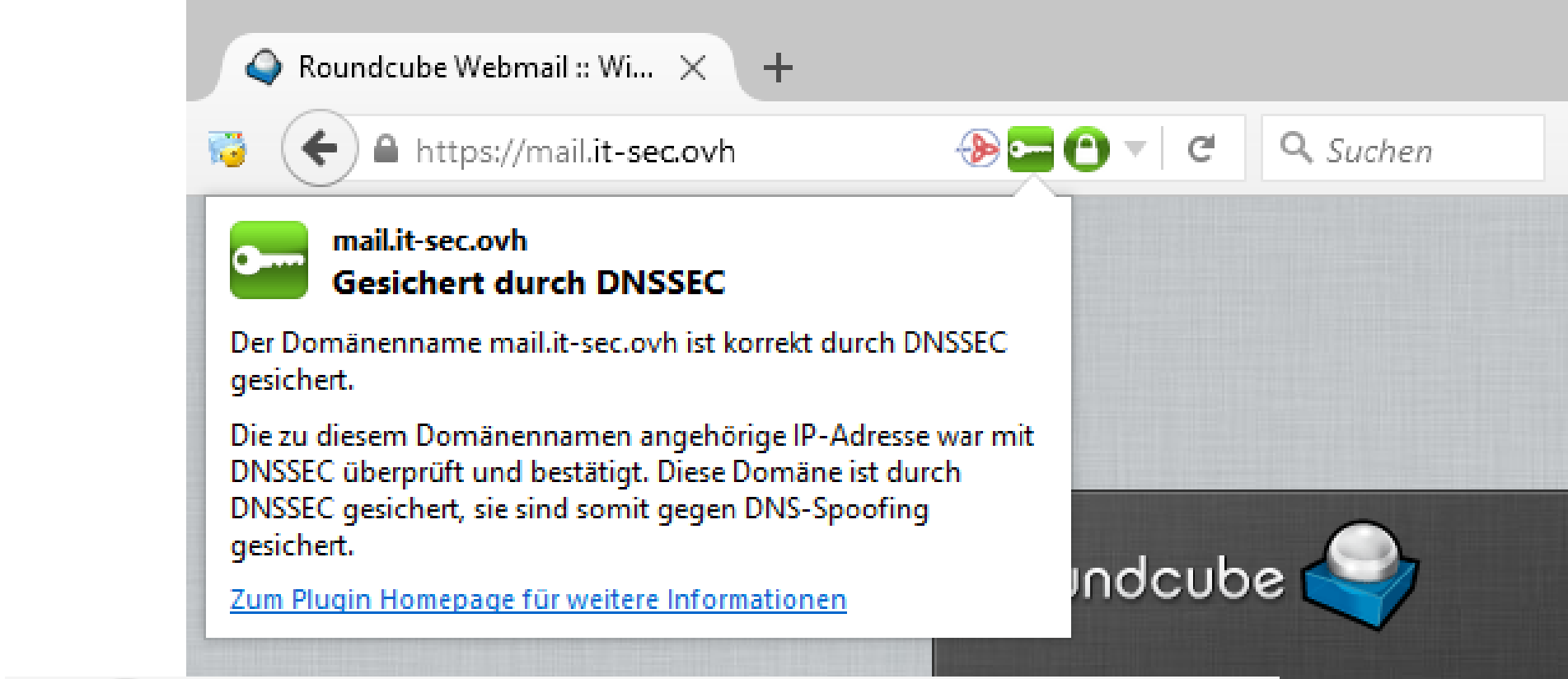
SIDN Labs

HTTPS
DANE Check



DNSSec & DANE

Validator PlugIn



Sicherer E-Mail-Dienste-Anbieter

basierend auf

Domain Name System Security Extension (DNSSec)
&
DNS-based Authentication of Named Entities (DANE)

Paper als Download (PDF): https://hitco.at/blog

https://hitco.at/blog/sicherer-e-mail-dienste-anbieter-dnssec-dane/

Quellen

- Abbildungen siehe Abbildungsverzeichnis sowie Literaturverzeichnis im zugehörigen Dokument:
  „Sicherer E-Mail-Dienste-Anbieter (DNSSec+DANE) HowTo.pdf“

Besonderer Dank an:

- SBA Research, insbesondere Aaron Zauner
- Heise-Verlag
- BetterCrypto.org
- Acidx‘s Blog – Markus Klein
- University Amsterdam
- Und allen anderen Quellen (siehe o.a. Dokument)