

DNSSEC

Zonen Verwaltung

mit ZKT

53. DFN Betriebstagung

Berlin
26. Oktober 2010

Holger.Zuleger@hznet.de

Secure DNS

- Erweiterung des DNS Protokoll (EDNS0 DO flag)
- Erlaubt Überprüfung der Authentizität einer DNS Antwort
 - Resolver wird zum „validierendem“ Resolver (unbound, BIND 9.7)
 - Benötig „Trust Anchor“ um Validierung durchzuführen
 - Zur Installation eines validierenden Resolver siehe c't 21/2010
- Aus Skalierungsgründen ist „Chain of Trust“ bis zur Root Zone nützlich
 - Root Zone ist signiert seit 15. Juli 2010 (+ 53/42 TLDs)
 - DENIC betreibt z.Z. signierte shadow .de Zone
 - RIPE signiert reverse Zonen seit 2006
 - .arpa ist signiert aber noch kein DS in der Root Zone
- Authoritative Nameserver benötigt „signierte“ Zone
 - Zone benötigt Schlüsselmaterial zum Signieren (DNSKEY)
 - Jeder RR bekommt eine Signatur (RRSIG)
 - Zone bekommt NSEC[3] Records für authentifizierte negative Antworten
 - Zeiger auf „Key Signing Key“ muß in Parentzone hinterlegt werden (DS)

Signieren einer Zone

- Jeder Resource Record bekommt eine Signatur

```

www.zonekeytool.de.      28800 IN A 88.198.13.165
www.zonekeytool.de.      28800 IN RRSIG A 5 3 28800 20101111085030 (
                          20101012085030 41747 zonekeytool.de.
                          i6lN3IQ/XQITceSH8K5GH2psnZZ2neT9PAgo6Ggf/0QF
                          wGONtIab3pRihY6sy8FqUmmb1X1XklP9EWZ9uFfFPQ== )

www.zonekeytool.de.      28800 IN AAAA 2a01:4f8:130:1261::2
www.zonekeytool.de.      28800 IN RRSIG AAAA 5 3 28800 20101111085030 (
                          20101012085030 41747 zonekeytool.de.
                          VUBoQd64ukDiZ5X17JUePlfgipzudYvjT87RcmRNtebK
                          PRCHX1UWzk8Myy11FUTK1M0nZOeKuMwIOVjs0+JXQg== )

```

- RRSIG Record enthält (u.a.)
 - Resource Record **Typ** den der RRSIG signiert
 - Gültigkeitsdauer (**Start**, **Ende**) der Signatur
 - **KeyID** des Schlüssels
- Gültigkeitsdauer hat Auswirkungen auf Zone Management
Dauer ist einstellbar (default 30 Tage: **12 Okt 2010 8:50** – **11 Nov 2010 8:50**)
- Rechtzeitiges Re-signieren ist essenziell!
z.B. nach 20 Tagen

Schlüsselmateriale

- Für die Signaturen werden Schlüssel benötigt
 - a. Zum Signieren „normaler“ RR (**Zone Signing Key**)
 - b. Zum Signieren des Schlüsselmaterials (**Key Signing Key**)

- Öffentliche Teile der Zonenschlüssel werden veröffentlicht

```
zonekeytool.de. 7200 IN DNSKEY 256 3 5 (
    BQEAAAABnc8bnYfE1A66b/hVKX60577xeV66QG1ctnsb
    dUlh7PDR7b8lqQ/+CYF0cR0aYBBsV7xNjT1VH/pxgthr
    ZMKImw== ) ; key id = 41747
7200 IN DNSKEY 257 3 5 (
    BQEAAAABctvLS6pq9OPiiwDaN2HJTUKG7VrfF1FBrK/S
    n/xQtiwznbTwUfEkB8cvs+ETBE7OBvRr4VL3Nz3tkKT8
    lNyJ1FcIffk/+YwJV/Ovq9o72Dng5iY3uPNpNtpdo9ER
    H21Rer90kUHKTQ8vIzObDADF9kJnyGXQ/bkwt/QUIg/m
    mBvJv7Ri6yIPu0eq+YRMtHfg4tM3dxhymOE2/ITJkDrr
    L4ZHdw== ) ; key id = 45693
7200 IN RRSIG DNSKEY 5 2 7200 20101111085030 (
    20101012085030 45693 zonekeytool.de.
    BWAgPxroNhgflAe0F0 ... Mlwf3jGU6W07aqOXlTPhg== )
```

- Wie kommen die DNSKEY Records in die Zone ?
Insbesondere bei Key Rollover ?

Schlüsseltausch

Key Rollover nach RFC 4641 „DNSSEC Operational Practices“

- ZSK Rollover (pre-publish key)
 1. Generiere einen zweiten ZSK
 2. Publiziere beide Schlüssel; Nutze nur den Alten zum Signieren
 3. Warte mindestens (propagation time + TTL des DNSKEY)
 4. Signiere mit neuem Schlüssel; Publiziere nach wie vor beide
 5. Warte mindestens (propagation time + max TTL der Zone)
 6. Entferne den alten Schlüssel aus der Zone

- KSK Rollover (double signature)
 1. Generiere einen zweiten KSK
 2. Benutze beide Schlüssel zum Key Signing
 3. Warte bis Validierer neuen Schlüssel kennen (proptime + DNSKEY TTL)
 4. Sende den neuen DS-Record zum Parent
 5. Warte bis DS in der Parentzone ist + TTL des alten DS-RR
 6. Entferne den alten Schlüssel

Signieren einer Zone mit BIND (< 9.7)

- Schlüsselmateriale erzeugen

```
$ dnssec-keygen -a RSASHA1 -b 1300 -f KSK zonekeytool.de
$ dnssec-keygen -a RSASHA1 -b 1024 zonekeytool.de
```

- DNSKEY Records in die Zone aufnehmen

```
$ cat Kzonekeytool.de.*.key >> zone.db
```

- Signieren

```
$ dnssec-signzone -g -x -N unixtime -e +1814400 -o zonekeytool.de. zone.db
```

- Lebensdauer der RRSIG 1814400 Sekunden (21 Tage)
- SOA Serialnumber wird auf unixtime gesetzt (>= BIND 9.4)
- DS RR von signierten Childs automatisch in die Zone aufnehmen (-g)
- DNSKEYs werden ausschliesslich durch KSK signiert (-x) (>= BIND 9.6)

- Reload der signierten Zonendatei (zone.db.signed)

```
$ rndc reload zonekeytool.de.
```

- Prozess zum Re-signieren aufsetzen

Machen sie sich schon mal 'nen Knoten ins Taschentuch

Zone Signing mit ZKT 1.0 (Einrichtung)

- a. Separates Verzeichnis für Zone anlegen

```
$ mkdir -p de/zonekeytool.de
```

- b. Zonenfile dort ablegen (zone.db)

- c. Schlüsseldatenbank in die Zone einfügen (`$INCLUDE dnskey.db`)

Ab ZKT 1.1 durch `zkt-conf -w zone.db`

- d. Signierte Zonendatei anlegen (`touch zone.db.unsigned`)

- e. Schlüsselmaterial erzeugen und probesignieren

```
$ zkt-signer -v -v -o zonekeytool.de # (Ausgabe gekürzt)
parsing zone "zonekeytool.de." in dir "."
No active KSK found: generate new one
No active ZSK found: generate new one
Re-signing necessary: Modified zone key set
Writing key file "./dnskey.db"
Signing zone "zonekeytool.de."
Run cmd "cd ./usr/local/sbin/dnssec-signzone -C -g \
-o zonekeytool.de. -e +864000 -N unixtime zone.db K*.private 2>&1"
```

- f. Signierte Zonendatei in BIND Konfigfile eintragen und laden

```
zone "zonekeytool.de" { type "master"; file "de/zonekeytool.de/zone.db.unsigned"; };
$ rndc reload zonekeytool.de
```

Zone Signing mit ZKT 1.0 (Regelmäßig)

- Regelmässig `zkt-signer` starten

Am besten als Cron Job

```
zkt-signer -r -N /etc/named/named.conf
```

- ZKT kann `named.conf` parsen (`-N`)
- Re-Signing nur falls notwendig
 - Zone wurde verändert
 - Neues Schlüsselmaterial
 - Subzone hat modifizierten KSK (DS Record erzeugen)
 - Re-Signing Intervall erreicht
- Automatischer Reload der Zone nach dem Signieren (`-r`)
- Logfile kontrollieren

```
notice: running zkt-signer -r -N /var/named/named.conf
notice: "zonekeytool.de.": lifetime of zone signing key 41747 exceeded: ZSK rollover done
notice: "zonekeytool.de.": re-signing triggered: Modified zone key set
notice: "zonekeytool.de.": reload triggered
notice: end of run: 0 errors occurred
```

Zone Key Tool

- Eines der ersten freien Tools zur Verwaltung von DNSSEC Zonen
Erste Release (zkt-0.5) 1. Apr 2005; Aktuelle Version ist zkt-1.0
- Wrapper um die BIND dnssec Kommandos
- ZKT unterstützt alle aktuellen BIND Versionen (9.3 bis 9.7)
- Wird seit 9.6 mit BIND ausgeliefert (contrib/zkt)
- Aktuelle Version über Sourceforge oder auf der Projekt Webseite
<http://sourceforge.net/projects/zkt>, <http://www.zonekeytool.de>
- FreeBSD und OpenBSD ports verfügbar
Maintained by Frank Behrens and Jakob Schlyter
- zkt-users mailing list (low volume)
<https://lists.sourceforge.net/lists/listinfo/zkt-users>

ZKT Features

- Kommando zur Anzeige des DNSKEY Schlüsselstatus (`zkt-ls`)
- Automatische Schlüssilverwaltung (key generation and rollover)
 - Pre-Publish (RFC4641 used for ZSK rollover)
 - RFC5011 (KSK rollover)
 - Double Signature (RFC4641 for KSK rollover)
- Automatische Anpassung der Seriennummer im SOA Record der Zone
 - UNIX time (seconds since the epoch)
 - plain integer
 - date format (yyyymmddnn)
- ZKT unterstützt „full zone signing“
Inkrementelles Signieren bei dynamischen Zonen
- Datei- und syslog basierendes Logging
Separate Log-Level einstellbar; Zonenbasierte Logfiles;
- Kommando zur Verwaltung der Konfigurationsdateien (`zkt-conf`)
Zur Zeit ca. 43 Parameter konfigurierbar

References

- Allgemeine Infos
 - DNSSEC Howto Ver 1.8.2, Olaf Kolkman, NLnetlabs, Ripe NCC (http://www.nlnetlabs.nl/dnssec_howto/)
 - DNSSEC Info Seiten (<http://www.dnssec.net>, <http://www.dnssec-deployment.org>)
 - Aktuelle Liste signierter TLDs (http://stats.research.icann.org/dns/tld_report/)
- Vergleich kommerzieller und freier DNSSEC Tools
 - Tool Guide Series on DNSSEC Verisign, Feb 2010 (<http://net.educause.edu/ir/library/pdf/CSD5928.pdf>)
 - A Review of Administrative Tools for DNSSEC Certezza AB, Frühjahr 2010 (<http://www.iis.se/docs/DNSSEC-Admin-tools-review-Final.pdf>)
- DNSSEC Software & Tools
 - Idns (<http://www.nlnetlabs.nl/ldns/index.html>)
 - unbound (<http://unbound.net/>)
 - BIND (<http://www.isc.org/software/bind/>)
 - ZKT (<http://www.zonekeytool.de/>)

Fragen ?

H Z N E T

DNSsec, VoIPsec, IPsec, XMPPsec, SMTPsec, WLANsec ...

... DKIM, Kerberos, IMAP, LDAP, ENUM, SIP, ...

... NTP, DNS, DHCP, IPv6, Routing, Switching

Holger.Zuleger@hznet.de

CONTENTS

- 1
- Secure DNS 2
- Signieren einer Zone 3
- Schlüsselmaterial 4
- Schlüsseltausch 5
- Signieren einer Zone mit BIND (< 9.7) 6
- Zone Signing mit ZKT 1.0 (Einrichtung) 7
- Zone Signing mit ZKT 1.0 (Regelmäßig) 8
- Zone Key Tool 9
- ZKT Features 10
- References 11
- 12