

# DNSSEC - Zonen mit BIND 9 DNSSEC signieren

Patrick Koetter und Carsten Strotmann, sys4 AG

# Agenda

---

1. Eine Zone manuell signieren
2. Automatisches Signieren einer dynamischen Zone
3. Automatisches Signieren per 'in-line' Signing
4. DNSSEC Automatisierung in BIND 9.16 und 9.18

# Zone manuell signieren

---

Seit BIND 9.6 können Zonen mit den BIND 9 Tools manuell signiert werden

- Vorteile:
  - Das Signieren kann vollständig offline und ohne laufenden BIND 9 DNS-Server erfolgen
  - Die privaten Schlüssel können auf sicheren Geräten gespeichert werden, ggf. verschlüsselt
  - Die erstellen Zonen-Dateien sind unabhängig von der DNS-Server Software
  - Die Parameter des Signatur-Vorgangs können optimal eingestellt werden
- Nachteile:
  - Die Zonen müssen regelmäßig manuell aufgefrischt werden, damit die Signaturen nicht ablaufen
  - Automatisierung muss durch eigene Skripte erfolgen

# Manuelles Signieren mit BIND 9 (1)

- DNSSEC in der BIND 9 Konfigurationsdatei `named.conf` anschalten

```
options {  
    directory "/var/named";  
    dnssec-enable yes;  
};
```

# Manuelles Signieren mit BIND 9 (2)

- Erstellen des Zone-Signing-Keys (ZSK)
  - Hierzu wird genügend echter Zufall auf dem System benötigt. Ggf. muss ein Hardware-Zufallszahlen-Generator oder ein Software-Entropy-Gathering-Daemon (z.B. Haveged) installiert werden.

```
% dnssec-keygen -a RSASHA256 -b 1536 -n ZONE zone0x.dnslab.org
Generating key pair.....++++ .....
Kzone0x.dnslab.org.+008+16239
```

```
% more Kzone0x.dnslab.org.+008+16239.key
; This is a zone-signing key, keyid 16239, for zone0x.dnslab.org.
; Created: 20160202121320 (Tue Feb  2 13:13:20 2016)
; Publish: 20160202121320 (Tue Feb  2 13:13:20 2016)
; Activate: 20160202121320 (Tue Feb  2 13:13:20 2016)
zone0x.dnslab.org. IN DNSKEY 256 3 8 AwEAAc1xFtt40wPEx4TVB7h8Ac7HvMZuF1LIqESU/0HUUzDT2rkujM
z0fgJJQVStYIbb1fXN0/PmKayEpj5ScbT7WU9Bef6b49uG1PwhsaftRr
/udr3DEA6MTedRqkl8K+E3P9hFj4XKxus45MYVSPaXZg3TcIQK3xpXC8
sKISny43cQaJpm12oBtKsANlA25KRJC8soPls/GqLSnArWDMN/YGqvs0
QECulpm2Nh1uULZfzwga8515xizyx5yAl/sgWQ==
```

# Manuelles Signieren mit BIND 9 (3)

- Erstellen des Key-Signing-Keys (KSK)

```
% dnssec-keygen -a RSASHA256 -b 2048 -f KSK -n ZONE zone0x.dnslab.org
Generating key pair.....
Kzone0x.dnslab.org.+008+04351
```

```
% more Kzone0x.dnslab.org.+008+04351.key
; This is a key-signing key, keyid 4351, for zone0x.dnslab.org.
; Created: 20160202121714 (Tue Feb  2 13:17:14 2016)
; Publish: 20160202121714 (Tue Feb  2 13:17:14 2016)
; Activate: 20160202121714 (Tue Feb  2 13:17:14 2016)
zone0x.dnslab.org. IN DNSKEY 257 3 8 AwEAAcmn/QkiCne922gBBBuJJOnq9jnG2yYbB10zBS2SgUCUx1Z
PAyubB2V+QhFsKf0VKUsVGl28JWAMcG1NGitj+nna4sGwvmeumj70DbG
ZzynwcFknEZG1Swn2bM/OFmlMS2WV3luzDYKnLeZgvN5geB6ZetONlpP
H9am3MRmExNIxoFb5NEcUlCzxSUI5GzjPZtGmCtDoNkrGE5nsssCgrjw
ec6hbeXLOjp9JiQ3egF3+PJHLUOjuqXKwSofHw4jV4Rqc3eP+uAHk5Wp
iH/BNW7c7lJ9IP+jZYZ3dp3SkO2qU8BOVV4fcm1L+IVcA9jwuPaOV53
j9L8fCTL/Uk=
```

# Manuelles Signieren mit BIND 9 (4)

- Die unsignierte Zone

```
$TTL 3600
$ORIGIN zone0x.dnslab.org.
@           IN SOA server0x.dnslab.org.  hostmaster.zone0x.dnslab.org
                        1001 ; serial
                        1d   ; refreh
                        2h   ; retry
                        4w   ; expire
                        30m  ; negTTL
                        )
                IN NS  server0x.dnslab.org.
                IN MX  10 mail.zone0x.dnslab.org.
www            IN A   192.168.53.199
mail          IN A   192.168.53.199
```

## Manuelles Signieren mit BIND 9 (5)

- Die öffentlichen Schlüssel (ZSK und KSK) der Zone hinzufügen

```
% cat Kzone0x.dnslab.org.+008+*.key >> zone0x.dnslab.org
```



# Manuelles Signieren mit BIND 9 (6)

- Die Zonen-Datei signieren

```
% dnssec-signzone -o zone0x.dnslab.org -k Kzone0x.dnslab.org.+008+04351.private \
  zone0x.dnslab.org Kzone0x.dnslab.org.+008+16239.private
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                  ZSKs: 1 active, 0 stand-by, 0 revoked
zone0x.dnslab.org.signed
```

- Syntax:

```
dnssec-signzone -o <origin> -k <KSK-privat> <Zonendatei> <ZSK-privat>
```

- Wird die Fehlermeldung *dnssec-signzone: fatal: SOA is not signed (keys offline or inactive?)* angezeigt, dann sind der KSK und der ZSK in der falschen Reihenfolge angegeben worden

# Manuelles Signieren mit BIND 9 (7)

- Weitere Optionen zu *dnssec-signzone*
  - `-j sec` Jitter, Variation in Sekunden der Signatur-Gültigkeit
  - `-M maxttl` - die maximale TTL in der Zone festlegen. Höhere TTL-Werte werden auf diesem Wert gesetzt.
  - `-s starttime` - Gültigkeits-Beginn der Signaturen
  - `-e endtime` - Gültigkeits-Ende der Signaturen
  - `-N SOA-format` - Format der SOA-Seriennummer
    - `increment` SOA-Serial um eins erhöhen
    - `unixtime` Unixtime (Sekunden seit dem 1.1.1970) als SOA-Serial benutzen
  - `-x` DNSKEY Record-Set nur mit dem KSK signieren (keine Signatur mit dem ZSK)
  - `-n numcpus` Anzahl CPU-Kerne für die Signierung
  - `-t` Ausgabe von Statistiken zur Geschwindigkeitsmessung

# Manuelles Signieren mit BIND 9 (8)

- Signierte Zone anzeigen

[illegible]

# Manuelles Signieren mit BIND 9 (9)

- Dateigröße vergleichen

```
% wc zone0x.dnslab.org*
  23      133      1554 zone0x.dnslab.org
 130      314      5178 zone0x.dnslab.org.signed
 153      447      6732 total
```

# Manuelles Signieren mit BIND 9 (10)

- BIND 9 Zonen-Konfiguration anpassen, so dass nun die signierte Zone geladen wird

```
zone "zone0x.dnslab.org" IN {  
    type master;  
    file "zone0x.dnslab.org.signed";  
};
```

- Konfiguration prüfen

```
% named-checkconf -z  
zone zone0x.dnslab.org/IN: loaded serial 1001 (DNSSEC signed)
```

- BIND 9 Zone neu laden

```
% rndc reload zone0x.dnslab.org
```

# DS-Record

- Den DS-Record an den Betreiber der Eltern-Zone senden
  - Der DS-Record befindet sich in der Datei "dsset-". Diese Datei wird beim manuellen Signieren automatisch erstellt.
- Warten bis der DS-Record in der Eltern-Zone sichtbar ist
- DNSSEC-Validierung prüfen (AD-Flag)

```
% dig zone0x.dnslab.org SOA +dnssec +m
; <<>> DiG 9.10.3-P3 <<>> zone0x.dnslab.org soa +dnssec +m
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20294
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1
```

# DNSSEC mit dynamischen Zonen

---

Seit BIND 9.7.4 können dynamische DNS-Zonen mit DNSSEC signiert werden

- Vorteile
  - BIND 9 aktualisiert die Signaturen automatisch (RRSIG Records)
  - Die Zonen-Schlüssel werden automatisch in die Zone importiert und nach dem Austausch der Schlüssel wieder aus der Zone entfernt
  - Der Lebenszyklus eines DNSSEC-Schlüssels kann über Meta-Daten des Schlüssels gesteuert werden
  - Mit diesem Meta-Daten lassen sich die Schlüssel-Rollover automatisieren
  - Änderungen an der Zone werden sofort per DNSSEC signiert
  - Die SOA-Seriennummer wird automatisch bei jeder Änderung in der Zone aktualisiert
  - Beim Parsen von Update-Befehlen werden Syntax-Fehler in den Zonen-Daten entdeckt. Diese Fehler können nicht in die Zonen-Datei kommen
  - Das Journal der Zone erfasst alle Änderungen in der Zone über die Zeit

## DNSSEC mit dynamischen Zonen

Seit BIND 9.7.4 können dynamische DNS-Zonen mit DNSSEC signiert werden Nachteile:

- Die DNS-Master-Server muss online Zugriff auf die Privaten Schlüssel der Zone haben. Der DNS-Master sollte daher ein "Hidden-Master" sein.
- Die Zonen-Daten dürfen nicht mehr in den Zonen-Dateien verändert werden. Die Benutzung von Editoren und einigen DNS-Verwaltungs-Programmen ist nicht möglich.



# Dynamisches DNSSEC (1)

DNSSEC in der BIND 9 Konfiguration anschalten und das Verzeichnis für DNSSEC-Schlüssel angeben

```
options {  
    directory "/var/named";  
    key-directory "/var/named/keys";  
    dnssec-enable yes;  
};
```

Konfiguration testen und BIND 9 neu laden

```
% named-checkconf -z  
% rndc reconfig
```

## Dynamisches DNSSEC (2)

ZSK und KSK für die Zone erstellen.

- Wird kein Algorithmus angegeben, so ist *RSASHA1* der Default (nicht empfohlen).
- Werden keine Schlüssel-Größen angegeben, so wird ein ZSK mit 1024bit RSA und ein KSK mit 2048bit RSA erstellt
- Der Parameter `-k` gibt an, in welchem Verzeichnis die Schlüssel abgelegt werden

```
% dnssec-keygen -a RSASHA256 -b 1536 -K /var/named/keys -n ZONE dynamic0x.dnslab.org  
% dnssec-keygen -a RSASHA256 -b 2048 -K /var/named/keys -f KSK -n ZONE dynamic0x.dnslab.org
```

## Dynamisches DNSSEC (3)

Bei der Erstellung der Schlüssel können die Schlüssel-Ereignisse für den Lebenszyklus des Schlüssels angegeben werden.

Zeitpunkte können entweder im Format YYYYMMDD oder YYYYMMDDHHMMSS, oder als Offset von der aktuellen Uhrzeit (now) angegeben werden. Das Offset wird mit +/-, einer Zahl und den Einheiten y (Jahr), mo (Monat), d (Tage), h (Stunde) und mi (Minute) angegeben

- Monate haben in diesem Format 30 Tage
- Jahre haben 365 Tage

## Dynamisches DNSSEC (4)

Diese Daten können mit `dnssec-settime` angezeigt und auch nachträglich geändert werden.

- `-P` Zeitpunkt, wann der Schlüssel in der Zone sichtbar werden soll (Publish)
- `-A` Zeitpunkt, an dem der Schlüssel zum Erstellen von Signaturen verwendet wird (Active)
- `-I` Zeitpunkt, von dem an der Schlüssel nicht mehr zum Signieren verwendet wird (Inactive)
- `-D` Zeitpunkt, an dem der Schlüssel aus der Zone gelöscht werden soll (Delete)
- `-R` Zeitpunkt, an dem der Schlüssel widerrufen wurde (Revoke)

# Dynamisches DNSSEC (5)

Publizierte Schlüssel können mit dem Befehl `dnssec-revoke` widerrufen werden.

```
% dnssec-revoke Kzone0x.dnslab.org.+008+23689.private
Kzone0x.dnslab.org.+008+23817

% more Kzone0x.dnslab.org.+008+23817.key
; This is a revoked key-signing key, keyid 23817, for zone0x.dnslab.org.
; Revoke: 20160202164447 (Tue Feb  2 17:44:47 2016)
zone0x.dnslab.org. IN DNSKEY 385 3 8 AwEAAeHhGKk8b0lK2sI8dysod64WOBpkudNx/SNNsAcy8PWddOGau8
F7a+YZH2JAOPFshfF9GLR3yt0kWTDjUOs0TCkyFoB4uYJftkeP5o/VO1
BeDapl5O87Qij3sq+DC8AmPfxYIIT/Kl0BSl0bEhR0AxnGoEpPzsaoNH
MSgkYp3wUZjNxZrXfOslekfn2VcCdwztXfjW9FJxw6ltg4bc2HydDUKw
6YS8YntWcdkbDdTWHImcaBk2UqBcfzluL9BShedDZ7psnIqh9EmNu+BR
jaMuE64xAbuk5py2cKKY3sg9LEpT5CLEuN0HSoH+iNY/E1QV1AHMGWlj
pdnw9il5Wq0=
```

- Ein widerrufender KSK hat die Flags *385*
- Es werden nur KSK-Schlüssel widerrufen, das Widerrufen eines ZSK-Schlüssels ist nicht definiert

# Dynamisches DNSSEC (6)

Anpassen der Zonen-Definition in der Datei `named.conf`

- `update-policy local`; erlaubt Updates mit dem BIND 9 Sitzung-Schlüssel aus `/var/run/named/session.key`. Dieser Schlüssel wird von `nsupdate` benutzt, wenn `nsupdate` mit dem Parameter `-l` gestartet wird
- `auto-dnssec maintain` sorgt für das automatische Laden der Schlüssel in die Zone und das aktualisieren der DNSSEC-Signaturen

```
zone "dynamic0x.dnslab.org" IN {  
    type master;  
    file "dynamic0x.dnslab.org";  
    update-policy local;  
    auto-dnssec maintain;  
};
```

# Dynamisches DNSSEC (7)

## Konfiguration prüfen und BIND 9 neu laden

```
% named-checkconf -z  
% rndc reconfig
```

- Ab diesem Zeitpunkt darf die Zonen-Datei nicht mehr per Editor verändert werden!
- BIND 9 wird die Zone beim nächsten DNSSEC-Signatur-Intervall (max. 60 Minuten) signieren
- Das Signieren der Zone kann über `rndc sign` angestoßen werden. Der Befehl `rndc sign` liefert keine Fehlermeldung, wenn die Zone nicht signiert werden kann (weil z.B. Schlüssel fehlen). Daher immer die Log-Dateien prüfen!

```
% rndc sign dynamic0x.dnslab.org  
% dig axfr @localhost dynamic0x.dnslab.org
```

## dynamisches DNSSEC (8)

Einen neuen DNS-Record hinzufügen. Die neuen Daten werden sofort per DNSSEC signiert:

```
# nsupdate -l
> update add test.dynamic0x.dnssec.example. 3600 IN TXT "Ein neuer DNS-Record"
> send
# dig txt test.dynamic0x.dnssec.example. @localhost +dnssec
[..]
;; ANSWER SECTION:
test.dynamic0x.dnssec.example. 3600 IN TXT "Ein neuer DNS-Record"
test.dynamic0x.dnssec.example. 3600 IN RRSIG TXT 5 4 3600 20160230114919 (
    20160131104919 25032 dynamic0x.dnssec.example.
    YliG936cphhDO2nAp1V5pXVMUH8/+90DEyRMqv0YCBVWR7Tz8tqqxjmr
    5sj0hxNJSfHJlMXa8lgwx33X0D6nl3JeAQ48ivDAKDHYOkd/ogo8GxjB
    L40lyxZ900NWcWQaCW0Ly9lKHgoD8PV4t50qb0/lqpZ/AK0m0TsMWpi/ IeA=
```



## dynamisches DNSSEC (9)

Einen DNS-Record löschen. Die Daten und die Signatur wird entfernt, die SOA-Serial wird hochgezählt:

```
# nsupdate -l  
> update del test.dynamic0x.dnssec.example. IN TXT  
> send
```

## dynamisches DNSSEC (10)

Die DS-Records für die Eltern-Zone werden mit dem Befehl `dnssec-dsfromkey` erstellt. Als Eingabeparameter erwartet `dnssec-dsfromkey` die Datei mit dem öffentlichen KSK-Schlüssel:

```
% dnssec-dsfromkey Kdynamic0x.dnslab.org.+008.+12345.key
dynamic0x.dnssec.example. IN DS 12345 8 1 B7BE432A2C4A25A0C9F1DA6DD4C289C99C25B2CC
dynamic0x.dnssec.example. IN DS 12345 8 2 DCA5AFBD131982707B55A19CD33048674ADE5FDD9FFCB008A
B378B689
```

Es werden die DS-Records mit SHA1-Hash und SHA256-Hash am Terminal ausgegeben.

## dynamisches DNSSEC (11)

- Warten, dass der DS-Record in der Eltern-Zone erscheint
- DNSSEC-Validierung in der Zone testen (AD-Flag!)

# DNSSEC mit 'inline-signing'

---

## DNSSEC mit 'inline-signing'

Seit BIND 9.9 kann der BIND 9 DNS-Server eine Zone beim Laden der Zone DNSSEC-signieren:

- Beim Laden aus einer Zonen-Datei
- Beim Zonen-Transfer von einem andern DNS-Server

Die DNSSEC-Signaturen werden automatisch aktualisiert

- Wenn die Zone neu aus der Datei geladen wird und in der Datei eine höhere SOA-Serial vorkommt
- Wenn die Zonen-Daten neu per Zonen-Transfer übertragen werden

# DNSSEC mit 'inline-signing'

## Vorteile von 'inline-signing'

- Gewohnte Administrations-Arbeitsabläufe können beibehalten werden
- DNS-Verwaltungs-Programme ohne DNSSEC-Unterstützung können weiter verwendet werden
- Bestehende DNS-Infrastrukturen können durch einen BIND 9 Server als 'bump-in-the-wire' DNSSEC-Signer DNSSEC-fähig gemacht werden, ohne den bestehenden DNS-Master anpassen zu müssen
- BIND 9 lädt die DNSSEC-Schlüssel automatisch und frischt die Signaturen selbsttätig auf
- Der Lebenszyklus eines DNSSEC-Schlüssels kann über Meta-Daten des Schlüssels gesteuert werden
- Mit diesem Meta-Daten lassen sich die Schlüssel-Rollover automatisieren

## DNSSEC mit 'inline-signing'

### Nachteile von 'inline-signing'

- Die SOA-Serial in der Zone auf den DNS-Servern kann höher sein als die Nummer in der Zonen-Datei
- Die SOA-Serial in der Zonen-Datei muss weiterhin manuell erhöht werden

# DNSSEC mit 'inline-signing' (1)

DNSSEC in der BIND 9 Konfiguration anschalten und das Verzeichnis für DNSSEC-Schlüssel angeben

```
options {  
    directory "/var/named";  
    key-directory "/var/named/keys";  
    dnssec-enable yes;  
};
```

Konfiguration testen und BIND 9 neu laden

```
% named-checkconf -z  
% rndc reconfig
```



## DNSSEC mit 'inline-signing' (2)

ZSK und KSK für die Zone erstellen.

- Der Parameter `-k` gibt an, in welchem Verzeichnis die Schlüssel abgelegt werden

```
% dnssec-keygen -a RSASHA256 -b 1536 -K /var/named/keys -n ZONE inline0x.dnslab.org  
% dnssec-keygen -a RSASHA256 -b 2048 -K /var/named/keys -f KSK -n ZONE inline0x.dnslab.org
```

# DNSSEC mit 'inline-signing' (2)

## Inline-Signing in der Zone aktivieren

```
zone "inline0x.dnslab.org" IN {  
    type master;  
    file "inline0x.dnslab.org";  
    inline-signing yes;  
    auto-dnssec maintain;  
};
```

## DNSSEC mit 'inline-signing' (3)

Konfiguration prüfen, BIND 9 neu laden, Zone signieren

```
% named-checkconf -z  
% rndc reload  
% rndc sign inline0x.dnslab.org
```

In den Log-Dateien das Ergebnis prüfen (rndc sign liefert keinen Fehler zurück!):

```
% tail /var/log/named.log  
31-Jan-2016 21:58:37.945 zone inline0x.dnslab.org/IN (unsigned): loaded serial 1002  
31-Jan-2016 21:58:37.946 zone inline0x.dnslab.org/IN (signed): loaded serial 1003 (DNSSEC s
```

## DNSSEC mit 'inline-signing' (4)

- Die Daten der signierten Zone werden im Binärformat (Format "raw") in die Datei mit der Endung ".signed" geschrieben
- BIND 9 legt zusätzlich noch eine Journal-Datei (.jnl) mit den Änderungen (für IXFR-Zonen-Transfers) und ein Backup des Journals (.jbk) an
- Die Ursprungs-Datei wird nicht geändert!
- Geänderte Daten werden nach spätestens 15 Minuten nach der Änderung in die Datei geschrieben
- Mittels `rndc sync` kann die Datei sofort aktualisiert werden
- Der Befehl `named-compilezone` kann eine Zone-Datei vom Format "RAW" in das RFC 1035 Text-Format umwandeln

```
# rndc sync inline0x.dnslab.org
# named-compilezone -f RAW \
  -o inline0x.dnslab.org.txt \
    inline0x.dnslab.org inline0x.dnslab.org.signed
```

## DNSSEC mit 'inline-signing' (5)

Änderungen in den Zonen-Daten werden wie gewohnt in der Zonen-Datei durchgeführt. Die SOA-Serial muss dabei erhöht werden. Die SOA-Serial kann, muss dabei nicht höher als die SOA-Serial der Zone auf den DNS-Servern werden

# DNSSEC in BIND 9.16

---

## BIND 9.16 DNSSEC (1/2)

BIND 9.16 ist die aktuelle Version des BIND 9 DNS-Servers.  
DNSSEC Verbesserungen in BIND 9.16:

- DNSSEC Konfiguration mit einer Zeile
- Automatische Erstellung der DNSSEC Schlüssel
- Automatischer Key-Rollover des ZSK-Schlüssel
- Automatischer Algorithmus-Rollover

## BIND 9.16 DNSSEC (2/2)

DNSSEC Konfiguration in einer (zusätzlichen) Zeile:

```
zone "example.com" {  
    type master;  
    file "example.com";  
    dnssec-policy default; # <-- DNSSEC anschalten  
};
```



## BIND 9.18

In BIND 9.18 (01/2022) sind weitere DNSSEC und DNS-Sicherheit-Verbesserungen implementiert:

- Automatischer KSK Rollover
- Unterstützung von CDS/CDNSKEY zum automatischen Austausch des DS-Records in der Eltern-Zone
- DNS Transport-Verschlüsselung
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)

Fragen?

---