DNSSEC Einführung

Einführung

- 1. Begriffe
- 2. Schlüssel der Root-Zone
- 3. Schlüssel in der Parent-Zone
- 4. KSK in der Kunden-Zone
- 5. ZSK in der Kunden-Zone
- 6. Links

1.1. Begriffe

- Seit 2010 ist DNSSEC aktiv
- KSK Key-Signing Key

  Zum Signieren eines rotierenden USK
- ZSK Zone-Signing Key
  Zum Signieren der DNS Records
- CSK Combined-Signing Key
  Ein Schlüssel der alles signiert

1.2. Records

- DNSKEY

  der öffentliche Schlüssel
- DS
  eine Signatur für einen öffentliche Schlüssel
- RRSIG

  eine Signatur für einen Record
- NSEC / NSEC3
  Verkettung der Records

1.3. Key-Rollover

- Ein ZSK sollte regelmäßig erneuert werden. Damit dies störungsfrei funktioniert, wird zuerst der neue Schlüssel veröffentlicht und die Zone mit alten und neuen Schlüssel signiert.
  Nach Ablauf einer Übergangszeit wir der alte Schlüssel und die zugehörigen Signaturen entfernt. Das passiert automatisch im DNS Server.

1.3. Key-Rollover

- Bei einen KSK oder CSK Rollover muss zusätzlich auch der DS Record in der übergeordneten Zone angepasst werden. Dies muss von Hand gemacht werden.
- Das RIPE bietet eine Automatisierung diese Prozesses für die Reverse-Zonen an.
- Standards RFC7344/RFC8078

2. Schlüssel der Root-Zone

- Wird mit dem Betriebsstem verteilt und erneuert
- Automatsches update nach RFC5011
- DNSSEC root key rollover am 11. Okt. 2018
- $ host -t DNSKEY .

Root DSNKEY

$ host -t DNSKEY .

has DNSKEY record 256 3 8
AwEAAcVnO2jZFx4756Rb/yAhJnsl72eemsObU43nclmXwqdJlp+kC5WQjGYkqLT5xkaUCPhkr4NKLLrIBZXeSGazc6gx/
yrrMtUpXcQvax6kfDJPTu974OmeEbtjyyP7ZG5tUfSwNWt/
4EuxDNmZTESG8jU0ZLjYIB11pK0gSXQbMVPyIyGtFGHMPx6UxWn6zUzpECWRFbqEvkA6Y13zeJ1jG2Rki/zs7a/o13FTl/
kI9013Eh6l6Kc2zxbc14GS8fpM0/xQIrZZyeiXj/
2C4RcsPeqWuNj9m0qSQrbrCZtLHb20U8x1uue4iwSX9y7LpwZd6vjYd1d6dgBa1Xxgc/TC+m8=

has DNSKEY record **257** 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+
B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/
EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/
ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=

has DNSKEY record 256 3 8
AwEAAbF1LAxEQPtClEQno48k6u7JjCOfVfwdENOxQUrX0JbpN5DnKGMAKIfdiWa5oDeKQ3OoQ58yCC8vjtaaGFDgpJxoLwqz
hBYHPGFgins5HIERcCQPGAJKWu/
ku4XLh+Fu7UyBubDCelxKTbnj26EwbochltRqGIE8hbwSXEzRNo4g+NXkaRMq2FFbaBtEE82yTmZUgFRYAFUvfGTPWblyZGt
kepVuHyNb0w/u24dpsz+uyCZZR04cHfRrWOKvqD3lDOwC4+sqd6f7F841R0N2tqSh/
WDUZzWdvPBaBOz0FWFLb9porIeZ3Jm08tAMHa+3SGRXfK4RAmxVCmIQQypGabE=

3. Schlüssel in der Parent-Zone

- KSK der „.de“ Zone ist vom ZSK der Root Zone signiert
- $ host -t TS de.

DS .de

$ host -t DS de.

de has DS record 26755 8 2
f341357809a5954311ccb82ade114c6c1d724a7
5c0395137aa3978035425e78d

3. Schlüssel in der Parent-Zone

- KSK der „.de“ Zone signiert ZSK der „.de“ Zone
- ZSK der „.de“ Zone signiert den KSK der Kunden-Zone
- $ host -t DNSKEY de.

DNSKEY .de

$ host -t DNSKEY de.

de has DNSKEY record 256 3 8
AwEAAb2hI7MrhbnAp2dbPqfNAryacz7nx6oku0IUnu9nyipwL/r3EN1ylCmGO74P/J1xpzNL/
LfBhi5IybBgl1QisvvRSs6jxKQoc1pEYPWRORrGt4R1seMO15abyxXBsGflbpgyNQ4Syv5ElQF/
GmQ1wc1RpzNlNXG0+A5yvkhPRZwb

de has DNSKEY record **257** 3 8
AwEAAbWUSd/QN9Ae543xzdiacY6qbjwtZ21QfmdgxRdm4Z7bjjHWy249uqxCyjjjoS4LDoRDKmj7ElffMKvTW
KE1qFKu0p8TUy4wyhX0M+m5FUjvQ3CiZMi+qY7GSHA5B+Zd73cidmnTeb3e8lso6jEsXg05/
VZ2AyAqWF6FexEIFxIqiwwLk4UP0BwZ17Ur3q1qx9VSbPMyHgQ9d6nHUN1EEJsTDA2v0vKumsUyp74Zan
RZ/bB/
6IzpaaZyr5BLF5pSCNdbRNjVmkwYD0993vm79LueyOeibsoHRc16jhALrIJou1PFjdq7YQsYN0KtqRiJtaAfPpr
DBREpeamPuW/MnW0=

de has DNSKEY record 256 3 8
AwEAAcAQmKR/GoUr9GydvoraNDvuhxcpGkYccgCcP7Ck8HMQmJ7Bx2vD8MV1jvRk0KpZdCXD1J/
ovykTzu3ldoHtkRrm9fmLaP5/
qqms2e3XHfyE0kWvamPsWZ5am+rQUyILeqgcWNhdYrfw9Kl0zTc7n9AwUqTTYx8/jp7D0FeU5L7P

4. KSK in der Kunden-Zone

- In der Parent-Zone wird ein passender DS Record eingetragen
- Oft kann dieser automatisch aus dem DNSKEY Record der Kunden-Zone erzeugt werden

- $ host -t DS lug-kassel.de.

  lug-kassel.de has DS record 30120 13 2 15c4ac942517dfb3be2e03806669fd4fa5fac32ba4187764843f83fbc9acde8f

5. ZSK in der Kunden-Zone

$ host -t DNSKEY lug-kassel.de.

lug-kassel.de has DNSKEY record **257** 3 13
Yhc2uLYuMrOcMuYSHFOWt2qNylwON4nvAbayQgattaSSEA1
g27O1zic9OlQLP1nn3z5324htufiIsbd3SPJkxg==

lug-kassel.de has DNSKEY record 256 3 13
w8r+l6h5pJY6q7MEbTRuQHixQAhk9+ddMV8Eh/2diNAcAYXX
XhtvvLJUXpZmZ1cssqnSv/4KcUijZ5vjCzGrhQ==

lug-kassel.de has DNSKEY record 256 3 13
bXWdYI5NThlfIEzOCQ0/DPkliKzHXOvGHmpnH0HZjdGt6RgJG
WurKieCY2VnfCWp+cKltQ0gEl6d9YqvHp+8Ag==

6. DNS-Eintrag

```
# dig +norec +dnssec soa lug-kassel.de
[…]
;; ANSWER SECTION:
lug-kassel.de.        86400   IN      SOA     uucp.dinoex.org. abuse.dinoex.de. 2023010752 86400 18000 604800 3600
lug-kassel.de.        86400   IN      RRSIG   SOA 13 2 86400 20230419140600 20230404130600 50934 lug-kassel.de.
Zln4wMxJV8Z7c5Od1c1VTfdFFW8ggfNl+a+WNh5X9qgy3G1Ck3UJSi8J PRI4JgKMKWv3YSnF+ghIjtAAO8S9aw==
lug-kassel.de.        86400   IN      RRSIG   SOA 13 2 86400 20230419140600 20230404130600 52815 lug-kassel.de.
Se1S1EHr5kcUrHAbLowLfz0YReayy92463XqBlcYqQFaJz/K+1P9SJRA Vfnuec/GAk3OjdN7q91S6rXf7uJVRw==
;; AUTHORITY SECTION:
lug-kassel.de.        86400   IN      NS      ns3.dinoex.net.
lug-kassel.de.        86400   IN      NS      ns3.dinoex.de.
lug-kassel.de.        86400   IN      NS      uucp.dinoex.org.
lug-kassel.de.        86400   IN      NS      ns3.dinoex.org.
lug-kassel.de.        86400   IN      RRSIG   NS 13 2 86400 20230418185127 20230403182546 50934 lug-kassel.de.
u4q+zgdUQGaTKnQWOZoK7S3uF86pWOX3MO5MAl90W/KvJ5P44L0d13tk F19aTnyMUutOdTeTAZaaLY65QEj64w==
lug-kassel.de.        86400   IN      RRSIG   NS 13 2 86400 20230418185127 20230403182546 52815 lug-kassel.de.
HKP7p/pkm6v6Bv3ERs5cQoa0/7wWj4VPLHqfSFHCNxaBS8U+5e9snjS4 8R8y7qC7ou12QfyiGOypKWMXjL0V3g==
[…]
```

5.1. Links

- Prüfung der Nameserver
  https://dnsviz.net/

- Darstellung des Signatur-Baums
  https://dnssec-analyzer.verisignlabs.com/

Diagramm Teil 1

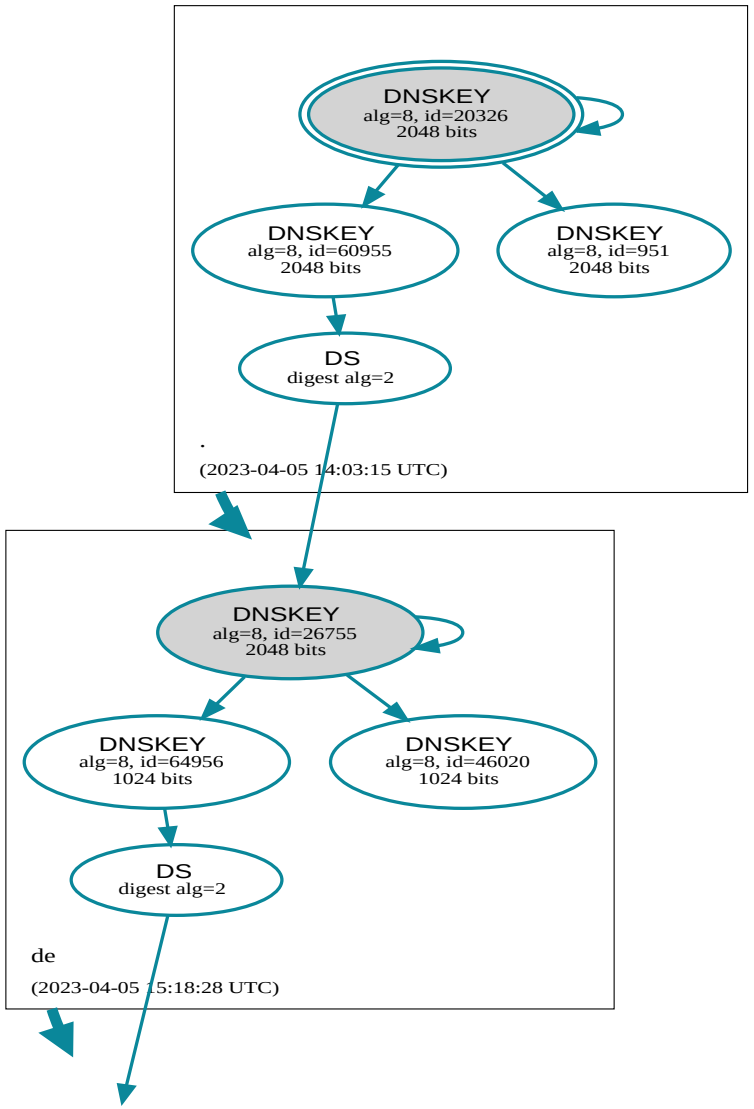

Diagramm Teil 2