CIA Lab Assignment: DNS Security Extensions (DNSSEC)

Question 1. What does a validating resolver do?

First, “DNSSEC adds resource records and message header bits which can be used to verify that the requested data matches what the zone administrator put in the zone and has not been altered in transit.” These resource records types are : RRSIG (for digital signature), DNSKEY (the public key), DS (Delegation Signer), and NSEC (pointer to next secure record). The new message header bits are: AD (for authenticated data) and CD (checking disabled). So the A “DNSSEC validating resolver uses these records and public key (asymmetric) cryptography to prove the integrity of the DNS data. A private key (specific to a zone) is used to encrypt a hash of a set of resource records — this is the digital signature stored in a RRSIG record.”

Source:

1- https://www.isc.org/downloads/bind/dnssec/

Question 2. Add support for DNSSEC to your BIND or Unbound configuration.

Before, I changed my configuration file I ran the unbound-anchor command in order to create the root.key file in the root of unbound.

```
kotaiba@bristol:/usr/local/etc/unbound$sudo unbound-anchor
```

root.key

```
kotaiba@bristol:/usr/local/etc/unbound$ cat root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1508240939 ;;Tue Oct 17 13:48:59 2017
;;last_success: 1508240939 ;;Tue Oct 17 13:48:59 2017
;;next_probe_time: 1508279956 ;;Wed Oct 18 00:39:16 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
.   172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b} ;;state=1 [ ADDPEND ] ;;count=1 ;;lastchange=1508240939 ;;Tue Oct 17
13:48:59 2017
.   172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b} ;;state=2 [  VALID  ] ;;count=0 ;;lastchange=1508240939 ;;Tue Oct 17
13:48:59 2017
```

(a) What changes do you have to make to your configuration?

Now, I need to add in my unbound configuration file the following:

```
# root key file, automatically updated
        auto-trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

Then, we restart unbound:

```
kotaiba@bristol:/usr/local/etc/unbound$ sudo unbound-control stop
kotaiba@bristol:/usr/local/etc/unbound$ sudo unbound-control start
```

Test it:

```
kotaiba@bristol:/usr/local/etc/unbound$ dig com. SOA +dnssec

; <<>> DiG 9.10.6 <<>> com. SOA +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11181
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 14, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;com.                IN    SOA

;; ANSWER SECTION:
com.            900    IN    SOA    a.gtld-servers.net. nstld.verisign-
grs.com. 1508241806 1800 900 604800 86400
com.            900    IN    RRSIG    SOA 8 1 900 20171024120326
20171017105326 11324 com.
ktO8HR2kNhWtVfflKZKErUUoghjkNRarArK/wiZ9LPqrhHRph80jIWAd
rp0T+Nqn6QEQ4b77ZO9ynwSWjQgNtiWju+q6MZyQR81vtAHkD6ZM0CEE
OEzc3Q1Jt5IDq9YZDi2icXUicVUevfTIRpoa6yZUa0BpKo6GxOv7PG7E vng=

;; AUTHORITY SECTION:
com.            167719    IN    NS    j.gtld-servers.net.
com.            167719    IN    NS    b.gtld-servers.net.
com.            167719    IN    NS    i.gtld-servers.net.
com.            167719    IN    NS    a.gtld-servers.net.
com.            167719    IN    NS    g.gtld-servers.net.
com.            167719    IN    NS    e.gtld-servers.net.
com.            167719    IN    NS    k.gtld-servers.net.
com.            167719    IN    NS    d.gtld-servers.net.
com.            167719    IN    NS    c.gtld-servers.net.
com.            167719    IN    NS    f.gtld-servers.net.
com.            167719    IN    NS    l.gtld-servers.net.
com.            167719    IN    NS    h.gtld-servers.net.
com.            167719    IN    NS    m.gtld-servers.net.
com.            167719    IN    RRSIG    NS 8 1 172800 20171024045212
```

```
20171017034212 11324 com.
q2IeKLKI3MMe+CyRKSyGZk8TQGUYVmAAVywOlRFbhxveyK2yBt5wJPKw
v1BqPpd65WMIb7Y44Q+glc+QvSWzOkvRigy4joM112jAdXHSE7fPulZL
hUK+BhtGvHFFHf6YTAz2FSqEPXDp3hlvE3niP9UDVbMEFPq+zB8d8+A9 rqI=

;; ADDITIONAL SECTION:
a.gtld-servers.net. 167718    IN    A    192.5.6.30
a.gtld-servers.net. 167718    IN    AAAA    2001:503:a83e::2:30
b.gtld-servers.net. 167718    IN    A    192.33.14.30
b.gtld-servers.net. 167718    IN    AAAA    2001:503:231d::2:30
c.gtld-servers.net. 167718    IN    A    192.26.92.30
c.gtld-servers.net. 167718    IN    AAAA    2001:503:83eb::30
d.gtld-servers.net. 167718    IN    A    192.31.80.30
d.gtld-servers.net. 167718    IN    AAAA    2001:500:856e::30
e.gtld-servers.net. 167718    IN    A    192.12.94.30
e.gtld-servers.net. 167718    IN    AAAA    2001:502:1ca1::30
f.gtld-servers.net. 167718    IN    A    192.35.51.30
f.gtld-servers.net. 167718    IN    AAAA    2001:503:d414::30
g.gtld-servers.net. 167718    IN    A    192.42.93.30
g.gtld-servers.net. 167718    IN    AAAA    2001:503:eea3::30
h.gtld-servers.net. 167718    IN    A    192.54.112.30
h.gtld-servers.net. 167718    IN    AAAA    2001:502:8cc::30
i.gtld-servers.net. 167718    IN    A    192.43.172.30
i.gtld-servers.net. 167718    IN    AAAA    2001:503:39c1::30
j.gtld-servers.net. 81728    IN    A    192.48.79.30
j.gtld-servers.net. 167718    IN    AAAA    2001:502:7094::30
k.gtld-servers.net. 167718    IN    A    192.52.178.30
k.gtld-servers.net. 167718    IN    AAAA    2001:503:d2d::30
l.gtld-servers.net. 167718    IN    A    192.41.162.30
l.gtld-servers.net. 167718    IN    AAAA    2001:500:d937::30
m.gtld-servers.net. 85328    IN    A    192.55.83.30
m.gtld-servers.net. 167718    IN    AAAA    2001:501:b1f9::30

;; Query time: 1 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Oct 17 14:03:39 CEST 2017
;; MSG SIZE  rcvd: 1209
```

(b) Verify the root key used against a trusted source.

From IANA website I got:

Root Zone Trust Anchor

root-anchors.xml DNS Root Trust Anchors Includes KSK-2010 and pre-published KSK-2017.

root-anchors.p7s Signature to verify the DNS Root Trust Anchors file (S/MIME)

icannbundle.pem Additional ICANN certificates for validating S/MIME signature

I downloaded these files on my server in order to verify the root key using openssl:

```
kotaiba@bristol:~/DNSSEC$ openssl smime -verify -in ./root-anchors.p7s -
inform DER -content ./root-anchors.xml -CAfile ./icannbundle.pem

<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor id="0AF79DEA-A7CD-43DC-9EDD-AD241CA63AE2"
source="http://data.iana.org/root-anchors/root-anchors.xml">
<Zone>.</Zone>
<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5</Di
gest>
</KeyDigest>
<KeyDigest id="Klajeyz" validFrom="2017-02-02T00:00:00+00:00">
<KeyTag>20326</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D</Di
gest>
</KeyDigest>
</TrustAnchor>
Verification successful
```

Source:

1- https://www.unbound.net/documentation/howto_anchor.html

2- https://www.iana.org/dnssec/files

Question 3. Use dig or drill to verify the validity of DNS records for isc.org and os3.nl. Show the results.

I will use dig and drill.

isc.org:

```
kotaiba@bristol:~/DNSSEC$ dig isc.org +dnssec +multi

; <<>> DiG 9.10.6 <<>> isc.org +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3841
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 13

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

;; ANSWER SECTION:
```

```
isc.org.        60 IN A    149.20.64.69
isc.org.        60 IN RRSIG A 5 2 60 (
                20171115233305 20171016233305 60321 isc.org.
                aYgQ5YEeoGMw+3G8iorvDUXb3rvUSsP8GBARoeed1/tS
                09MR4WaDY+Ot0dhMMIJgt5WWa64MPW2Jn09LHmn+THhx
                GhghzI9M4lu1FeWWPTKkt+9uIhRNN34ZLH6qXyVqUT6P
                h2/Gpp3cLijPTS35UwkwlTSw2ulQ0RZXBwE3a4k= )

;; AUTHORITY SECTION:
isc.org.        3795 IN    NS ams.sns-pb.isc.org.
isc.org.        3795 IN    NS ord.sns-pb.isc.org.
isc.org.        3795 IN    NS ns.isc.afilias-nst.info.
isc.org.        3795 IN    NS sfba.sns-pb.isc.org.
isc.org.        3795 IN    RRSIG NS 5 2 7200 (
                20171115233305 20171016233305 60321 isc.org.
                Za526KsJHnpc3vLBbyj92jNmNeqGIzxjiy0TAW+9TYnY
                YBctt51H+lUVPkBhuGk5ZLSm2hEsYffwj93+kzf/swDm
                k4wbJeNtQ9J8vPoO/SVSDsnMHSm66Ai5iCDqNpQCq9SM
                bc2CaIrFLcW2Pe42YZ3Dy6VmVPI0pGdZh87tloc= )

;; ADDITIONAL SECTION:
ams.sns-pb.isc.org. 82995 IN A 199.6.1.30
ams.sns-pb.isc.org. 82995 IN AAAA 2001:500:60::30
ord.sns-pb.isc.org. 82995 IN A 199.6.0.30
ord.sns-pb.isc.org. 82995 IN AAAA 2001:500:71::30
sfba.sns-pb.isc.org.    82995 IN A 149.20.64.3
sfba.sns-pb.isc.org.    82995 IN AAAA 2001:4f8:0:2::19
ams.sns-pb.isc.org. 7200 IN    RRSIG A 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                KQ901pCsa3SijpFZ1g/al5v8xeHF8OG7PYPfcFpFcbce
                1FAE9Em67CrKB5wtJWKCPjVMDoIe67ADzCHTycn3jMF9
                HSAJvqLCnuvtjZRDjI44y+TvvOIdazaZUd0FUXwCAiY3
                38GNE7QhpvCZrZmn402fi4R7kh94ysuGo5nbwxE= )
ams.sns-pb.isc.org. 7200 IN    RRSIG AAAA 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                BLZ4dHCTOrNsRsvYSjjnvLT7EAsKhiY8nsJh1Efsmily
                nTE+yQ+ocjY4u8A4IoJOWr7eitSrF7LwazflnS5s+kvt
                79m4p0i8Bk9lfIK7ek2YVtk1mry9Ngxu9+lHJbR6BTR0
                BxM7tjOelVFrxga2KHV9aELsode6FkeklMtDt8E= )
ord.sns-pb.isc.org. 7200 IN    RRSIG A 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                da4A3jFstuoyCu3THw5LY7pYEYoUwfzFOn0LJ/1dM3JT
                nlpqHrSXakzVaoqBL+fQAycVWpd3ygF7OsQOaPQBkIN4
                fekgq0wPAYdV3sIjAAzZfi8TbYcMMT1L4BavOqgnuWPe
                hNP0bxNe4y4UI5Pia2M+lhhEqrHCxkU6EgAXVgU= )
ord.sns-pb.isc.org. 7200 IN    RRSIG AAAA 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                QEFoI/lUEHG0OtSs9AEdbBviJsRqoufRfH3X8qeOQkb0
                vL5keOi/TPdcjcUUAaKlNMFo4vXQ0Fb7b7DIG3FGwpz2
                PBuosc51eODXiQubdgD6aZCDwyXnS4W30o6c8QV0rhhy
                YNhwlqfD595diQrph3/2DsEH4gxQxrTasZ/cdR8= )
```

```
sfba.sns-pb.isc.org.    7200 IN    RRSIG A 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                fsRKjUZT9kc6Qxm+uA+4FzFGRN7Z2p9LDZ1RFeaoPDhP
                M2dbcAU2g4GYnjzPbSnLeZ9Qcyw9hSA3tEbyeKRm3QeY
                K90bBnKb6FcTTLpp4Ji74+uaGmk67OFCKXdnnO+XuDt+
                +F9Gs0iqH3J1IiSLesAQ/t5SoXEwSrq5aBFG6ls= )
sfba.sns-pb.isc.org.    7200 IN    RRSIG AAAA 5 4 7200 (
                20171115233305 20171016233305 60321 isc.org.
                OJ7+V2KjpxF4XzSjT2zCp+/Uk30ism3OxUlDzaAxVC8V
                sdftmn9VcG/wE0YBLNRaYuEHzHBk2hNnNidjtaTciJ9v
                u0WFFGJXwPwSJ+zbn3yse57V5wFU+MXbHUkMnYdWKHyU
                saOVQhRr5YptMTbvwgxYUoLU26JUUOGD3doqJTQ= )

;; Query time: 2 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Oct 17 14:15:26 CEST 2017
;; MSG SIZE  rcvd: 1619
```

os3.nl. :

```
kotaiba@bristol:~/DNSSEC$ dig os3.nl. +dnssec +multi

; <<>> DiG 9.10.6 <<>> os3.nl. +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34928
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;os3.nl.            IN A

;; ANSWER SECTION:
os3.nl.         18669 IN A 145.100.96.70
os3.nl.         18669 IN RRSIG A 5 2 21600 (
                20171116093852 20171017093852 42048 os3.nl.
                Gh2XGRDbKejtqEYMTQbJwzbhPi/sKLdtG/DKENbt7G6H
                Dy5eosFWTc1aRpX6IfkF5bxtIH89RBUJzySIUymhYovZ
                O2f07QnsTF4FLJYuA0IELHqJPHQqLUoI3xfGQOlfHuh0
                1VBz8iR2XdOzWYGG1yRw09FkpalMkPIbLjAPOlE= )

;; AUTHORITY SECTION:
os3.nl.         15704 IN NS ns1.os3.nl.
os3.nl.         15704 IN NS ns2.os3.nl.
os3.nl.         15704 IN NS ns1.zurich.surf.net.
os3.nl.         15704 IN RRSIG NS 5 2 21600 (
                20171116093852 20171017093852 42048 os3.nl.
                iTLJsPdz76xNn4NfZjyk4QBBX0Sg1q7MGWX8Hv8TnATN
                CQiCRi3tMjaDfW82u3F53+57EwX0zUo5uKd/U8TdISnE
                RYWKEfvrUfOElxcBnFnT/SVYooNz/UPZpNsJd1qZ25sh
```

```
                UxEsTp1plOWNRs/zh4HDOmgydlMtEN5T78pj0c4= )

;; ADDITIONAL SECTION:
ns1.zurich.surf.net.    166904 IN A 195.176.255.9
ns1.zurich.surf.net.    170455 IN AAAA 2001:620:0:9::1103
ns2.os3.nl.     800 IN A 145.100.96.99
ns2.os3.nl.     800 IN AAAA 2001:610:158:960::99
ns2.os3.nl.     15704 IN RRSIG A 5 3 21600 (
                20171116093852 20171017093852 42048 os3.nl.
                rg4qZkfO2Z2f9d3Y1/zuCw9TFPcNIyza8yoUwiBnb4GK
                4yPV0WzFWcjUrl49XivnpmI8RQ7x8i5PjIjVzSILPOyQ
                Ln8hPlOYTouwAeaY5x49dosaGzlrSv6gmfHZzUTVgG+N
                RDEHfW9li2WlF7FVvVTbAz94K7w/4h/DZDEGu0o= )
ns2.os3.nl.     15704 IN RRSIG AAAA 5 3 21600 (
                20171116093852 20171017093852 42048 os3.nl.
                D9A7rRyRAS4V88GOLk2625jsz6XkRYd6XXkzmO/PWzTZ
                x2FgObvH0BE+w0dLwD+N/2isUYMrhYeiXF64MaVxH3J7
                tACYThEfMDCFL++xtZ/22Rnoawocjmzaf2gS/VenFBGa
                dw3zdDF0TJ9cvAZi/iFHXg4VteZmlTjjYr5tl3Y= )

;; Query time: 0 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Oct 17 14:17:13 CEST 2017
;; MSG SIZE  rcvd: 872
```

USING DRILL:

os3.nl.

```
kotaiba@bristol:~$ drill -k /usr/local/etc/unbound/root.key -TD os3.nl. SOA
@ns1.surfnet.nl
;; Number of trusted keys: 2
;; Domain: .
[T] . 172800 IN DNSKEY 256 3 8 ;{id = 46809 (zsk), size = 2048b}
. 172800 IN DNSKEY 257 3 8 ;{id = 19036 (ksk), size = 2048b}
. 172800 IN DNSKEY 257 3 8 ;{id = 20326 (ksk), size = 2048b}
Checking if signing key is trusted:
New key: .  172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
```

```
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
Key is now trusted!
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
[T] nl. 86400 IN DS 34112 8 2
3c5b5f9b3557455c50751a9be9ebe9238c88e19f5f07f930976917b51b95cd22
;; Domain: nl.
[T] nl. 3600 IN DNSKEY 256 3 8 ;{id = 6178 (zsk), size = 1024b}
nl. 3600 IN DNSKEY 257 3 8 ;{id = 34112 (ksk), size = 2048b}
nl. 3600 IN DNSKEY 256 3 8 ;{id = 33304 (zsk), size = 1024b}
Checking if signing key is trusted:
New key: nl.    3600    IN    DNSKEY    256 3 8
AwEAAa66+xtJGp1Cj3I3/kuy1q7IsAUobRtiAwlydr6XAOZpIBXiKbrhu1Dz6oWUv4F+cuId0kUy
CjWH6EYzjv/Ai5K7wSND0pznqEKwJMa5Ulm1qfASB9m11CR5xf5fOpn0U5ZKH0ZNMQ6gl5SP9Pnr
+XsKecdb/CoPsNcA3m3R01OJ ;{id = 6178 (zsk), size = 1024b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
```

```
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: nl.    3600    IN    DNSKEY    256 3 8
AwEAAa66+xtJGp1Cj3I3/kuy1q7IsAUobRtiAwlydr6XAOZpIBXiKbrhu1Dz6oWUv4F+cuId0kUy
CjWH6EYzjv/Ai5K7wSND0pznqEKwJMa5Ulm1qfASB9m11CR5xf5fOpn0U5ZKH0ZNMQ6gl5SP9Pnr
+XsKecdb/CoPsNcA3m3R01OJ ;{id = 6178 (zsk), size = 1024b}
Key is now trusted!
    Trusted key: nl.    3600    IN    DNSKEY    257 3 8
AwEAAcb+4kIsKoZM+3ZZpU9kzxrzw30e3b+L0KZeX+aAS3eM+Q+q27Jw0NZ3dqsPSif61GjRW6ap
jDZ9Ciab3oyEu7IpihVrw94DTjWZTVViZAijAIHwKUzY0YjkT3RvN+xgpw4uZs1SnqCZxYko+15e
steKXW/nJpde0d9OeFFBaS2WTCycK+A6gd9DsOw91Y7Z2vrR/2g9N9dMIVq9neB1/KXXm4MttLqJ
yxRWZNAFTyLGQKzPpQDp9s3qowV2+pcHOh6lUTEeOWiAtotJ/5WyO91viZ5tBfClsyGpggBTaeUQ
7T5adhAtX6nRkhePyAtQgCCf63ZpHyoyxvbkDM7yuA0= ;{id = 34112 (ksk), size =
2048b}
    Trusted key: nl.    3600    IN    DNSKEY    256 3 8
AwEAAbbOFCvOz+LOeHF/B2iADJgiqPMdsoi+D7PSFbU+fd/XYXj/bxlIJr4LbXWjp9Mzmh/S0zp8
qqMkZ8WZLjI57ncT77uE3d3filLySUUKRFIn30eIl2fkXzWxJjLcewVTz5V2tmoL4o1etVk4y2oy
5C8BXaNgt1WbZNmy/R1G6VOP ;{id = 33304 (zsk), size = 1024b}
[T] os3.nl. 3600 IN DS 64426 5 2
28c5e04fc87d47bd9bbd2e27091a372768c3560795f26ebe097432578e86a6de
;; Domain: os3.nl.
[T] os3.nl. 21600 IN DNSKEY 256 3 5 ;{id = 42048 (zsk), size = 1024b}
os3.nl. 21600 IN DNSKEY 257 3 5 ;{id = 64426 (ksk), size = 2048b}
[T] os3.nl. 21600    IN    SOA    ns1.os3.nl. hostmaster.os3.nl. 1508236732
3600 1800 21600 3600
;;[S] self sig OK; [B] bogus; [T] trusted
```

```
kotaiba@bristol:~$ drill -k /usr/local/etc/unbound/root.key -TD isc.org SOA
@ns1.surfnet.nl
;; Number of trusted keys: 2
;; Domain: .
[T] . 172800 IN DNSKEY 257 3 8 ;{id = 19036 (ksk), size = 2048b}
. 172800 IN DNSKEY 257 3 8 ;{id = 20326 (ksk), size = 2048b}
. 172800 IN DNSKEY 256 3 8 ;{id = 46809 (zsk), size = 2048b}
Checking if signing key is trusted:
New key: .  172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
Key is now trusted!
```

```
[T] org. 86400 IN DS 9795 7 1 364dfab3daf254cab477b5675b10766ddaa24982
org. 86400 IN DS 9795 7 2
3922b31b6f3a4ea92b19eb7b52120f031fd8e05ff0b03bafcf9f891bfe7ff8e5
;; Domain: org.
[T] org. 900 IN DNSKEY 257 3 7 ;{id = 17883 (ksk), size = 2048b}
org. 900 IN DNSKEY 257 3 7 ;{id = 9795 (ksk), size = 2048b}
org. 900 IN DNSKEY 256 3 7 ;{id = 3947 (zsk), size = 1024b}
org. 900 IN DNSKEY 256 3 7 ;{id = 1862 (zsk), size = 1024b}
Checking if signing key is trusted:
New key: org.   900    IN    DNSKEY    256 3 7
AwEAAayiVbuM+ehlsKsuAL1CI3mA+5JM7ti3VeY8ysmogElVMuSLNsX7HFyq9O6qhZVJz54Teuzf
2EGjO8cbK/fUbyzFW+4i4BRk+pVx673NRgQqDiB2oJDmQRK918Rmoxi/Sf8S7k9FB1XzxspIi9AJ
mn5tz4ACVsD2xTc1wZtAKVjr ;{id = 3947 (zsk), size = 1024b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
    Trusted key: org.    900    IN    DNSKEY    257 3 7
AwEAAcMnWBKLuvG/LwnPVykcmpvnntwxfshHlHRhlY0F3oz8AMcuF8gw9McCw+BoC2YxWaiTpNPu
xjSNhUlBtcJmcdkz3/r7PIn0oDf14ept1Y9pdPh8SbIBIWx50ZPfVRlj8oQXv2Y6yKiQik7bi3MT
```

```
37zMRU2kw2oy3cgrsGAzGN4s/C6SFYon5N1Q2O4hGDbeOq538kATOy0GFELjuauV9guX/431msYu
4Rgb5lLuQ3Mx5FSIxXpI/RaAn2mhM4nEZ/5IeRPKZVGydcuLBS8GZlxW4qbb8MgRZ8bwMg0pqWRH
mhirGmJIt3UuzvN1pSFBfX7ysI9PPhSnwXCNDXk0kk0= ;{id = 17883 (ksk), size =
2048b}
    Trusted key: org.    900    IN    DNSKEY    257 3 7
AwEAAZTjbIO5kIpxWUtyXc8avsKyHIIZ+LjC2Dv8naO+Tz6X2fqzDC1bdq7HlZwtkaqTkMVVJ+8g
E9FIreGJ4c8G1GdbjQgbP1OyYIG7OHTc4hv5T2NlyWr6k6QFz98Q4zwFIGTFVvwBhmrMDYsOTtXa
kK6QwHovA1+83BsUACxlidpwB0hQacbD6x+I2RCDzYuTzj64Jv0/9XsX6AYV3ebcgn4hL1jIR2eJ
YyXlrAoWxdzxcW//5yeL5RVWuhRxejmnSVnCuxkfS4AQ485KH2tpdbWcCopLJZs6tw8q3jWcpTGz
dh/v3xdYfNpQNcPImFlxAun3BtORPA2r8ti6MNoJEHU= ;{id = 9795 (ksk), size =
2048b}
    Trusted key: org.    900    IN    DNSKEY    256 3 7
AwEAAayiVbuM+ehlsKsuAL1CI3mA+5JM7ti3VeY8ysmogElVMuSLNsX7HFyq9O6qhZVJz54Teuzf
2EGjO8cbK/fUbyzFW+4i4BRk+pVx673NRgQqDiB2oJDmQRK918Rmoxi/Sf8S7k9FB1XzxspIi9AJ
mn5tz4ACVsD2xTc1wZtAKVjr ;{id = 3947 (zsk), size = 1024b}
Key is now trusted!
    Trusted key: org.    900    IN    DNSKEY    256 3 7
AwEAAXxsMmN/JgpEE9Y4uFNRJm7Q9GBwmEYUCsCxuKlgBU9WrQEFRrvAeMamUBeX4SE8s3V/TEk/
TgGmPPp0pMkKD7mseluK6Ard2HZ6O3nPAzL4i8py/UDRUmYNSCxwfdfjUWRmcB9H+NKWMsJoDhAk
LFqg5HS7f0j4Vb99Wac24Fk7 ;{id = 1862 (zsk), size = 1024b}
[T] isc.org. 86400 IN DS 12892 5 2
f1e184c0e1d615d20eb3c223aced3b03c773dd952d5f0eb5c777586de18da6b5
isc.org. 86400 IN DS 12892 5 1 982113d08b4c6a1d9f6aee1e2237aef69f3f9759
;; Domain: isc.org.
[T] isc.org. 7200 IN DNSKEY 256 3 5 ;{id = 60321 (zsk), size = 1024b}
isc.org. 7200 IN DNSKEY 257 3 5 ;{id = 12892 (ksk), size = 2048b}
[T] isc.org.    7200    IN    SOA    ns-int.isc.org. hostmaster.isc.org.
2017101700 7200 3600 24796800 3600
;;[S] self sig OK; [B] bogus; [T] trusted
```

Question 4. How does dig/drill show whether DNSSEC validation was successful or not?

By showing the AD (authentic data) bit in the query. This requests the server to return whether all of the answer and authority sections have all been validated as secure according to the security policy of the server. AD=1 indicates that all records have been validated as secure and the answer is not from a OPT-OUT range. AD=0 indicate that some part of the answer was insecure or not validated. This bit is set by default.

But since I added also the drill command now (for next questions)

[S] self sig OK; [B] bogus; [T] trusted

As we see above the chain of trust fully verified by following these legend.

Source:

1- https://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/man.dig.html

Question 5. Where does BIND/Unbound store the DNSSEC root key?

Unbound: The root key is stored in a file, /usr/local/etc/unbound/root.key

Question 6. How do “managed keys” differ from “trusted keys”? Which RFC describes the mechanisms for managed keys?

managed keys: allows automatic tracking of the key using a protocol known as **RFC-5011**. So for the root zone or “dnssec-validation auto”, there is low risk. because with managed-keys, BIND will self-update when the root key changes.

trusted keys: you will need to update your configuration prior to October, 2017, to avoid a potentially serious service impact. So for the root zone, you need to update your configuration.

Source:

1- https://www.isc.org/blogs/using-the-root-dnssec-key-in-bind-9-resolvers/

2- https://www.isc.org/blogs/2017-root-key-rollover-what-does-it-mean-for-bind-users/

Question 7. How did you modify the DNSSEC root key?

First lets make a copy of it before we try anything.

So the original file is :

```
.       172800  IN      DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyB$
.       172800  IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efuc$
```

Modified file is:

```
.       172800  IN      DNSKEY  257 3 8
XwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyB$
.       172800  IN      DNSKEY  257 3 8
PwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efuc$
```

As you see I just changed tow first letters of the keys.

Question 8. What problems did your server encounter, and how did it react?

The problem now if we drill the same way as above.

```
kotaiba@bristol:/usr/local/etc/unbound$ drill -k
/usr/local/etc/unbound/root.key -TD isc.org SOA
;; Number of trusted keys: 2
;; Domain: .
```

```
;; Signature ok but no chain to a trusted key or ds record
[S] . 172800 IN DNSKEY 257 3 8 ;{id = 19036 (ksk), size = 2048b}
. 172800 IN DNSKEY 256 3 8 ;{id = 46809 (zsk), size = 2048b}
. 172800 IN DNSKEY 257 3 8 ;{id = 20326 (ksk), size = 2048b}
Checking if signing key is trusted:
New key: .  172800    IN    DNSKEY    256 3 8
AwEAAcRIZfxskdElMKgjwvWQO2bQe7EGAvX6zgIaqmbsaMqmMrIpd1+bP7nyULLuL8jWnKAqcaVf
al2yJD50gg5zFl5yW/F9dKNXXEFI7VEcGrPyG6/OrA9RBU8pGWm0qxpsNm5UIgTU5IX7pb/0rBj6
7c/R7qln8sjH1ylsr4f1Y3R6p/druiEalKasEjGKA9L2w9jzUQusWxM7fQx/T8c/3x3bsjveD1dl
eQ6MJaCx4bpPXYZpqXmSvGn+T2v5350cBVAFqVKhGbjxEyXAweem8cTU4L1p+DV7Ua11a1tMf0Tl
u8pkpLwh7NQIggIEhJwEhPeXE3E4C6Q2/PFENcoFERc= ;{id = 46809 (zsk), size =
2048b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
XwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 43878 (ksk), size =
1312b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
PwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 34396 (ksk), size =
1568b}
[S] org. 86400 IN DS 9795 7 2
3922b31b6f3a4ea92b19eb7b52120f031fd8e05ff0b03bafcf9f891bfe7ff8e5
org. 86400 IN DS 9795 7 1 364dfab3daf254cab477b5675b10766ddaa24982
;; Domain: org.
;; Signature ok but no chain to a trusted key or ds record
[S] org. 900 IN DNSKEY 257 3 7 ;{id = 9795 (ksk), size = 2048b}
org. 900 IN DNSKEY 256 3 7 ;{id = 3947 (zsk), size = 1024b}
org. 900 IN DNSKEY 257 3 7 ;{id = 17883 (ksk), size = 2048b}
org. 900 IN DNSKEY 256 3 7 ;{id = 1862 (zsk), size = 1024b}
Checking if signing key is trusted:
New key: org.   900    IN    DNSKEY    256 3 7
AwEAAayiVbuM+ehlsKsuAL1CI3mA+5JM7ti3VeY8ysmogElVMuSLNsX7HFyq9O6qhZVJz54Teuzf
2EGjO8cbK/fUbyzFW+4i4BRk+pVx673NRgQqDiB2oJDmQRK918Rmoxi/Sf8S7k9FB1XzxspIi9AJ
mn5tz4ACVsD2xTc1wZtAKVjr ;{id = 3947 (zsk), size = 1024b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
XwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlE
xOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgC
mr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+
SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnX
GXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 43878 (ksk), size =
1312b}
    Trusted key: .    172800    IN    DNSKEY    257 3 8
PwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0
EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q
Zxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hO
```

```
A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8
ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 34396 (ksk), size =
1568b}
[S] isc.org. 86400 IN DS 12892 5 1 982113d08b4c6a1d9f6aee1e2237aef69f3f9759
isc.org. 86400 IN DS 12892 5 2
f1e184c0e1d615d20eb3c223aced3b03c773dd952d5f0eb5c777586de18da6b5
;; Domain: isc.org.
;; Signature ok but no chain to a trusted key or ds record
[S] isc.org. 7200 IN DNSKEY 256 3 5 ;{id = 60321 (zsk), size = 1024b}
isc.org. 7200 IN DNSKEY 257 3 5 ;{id = 12892 (ksk), size = 2048b}
[S] isc.org.    7200    IN    SOA    ns-int.isc.org. hostmaster.isc.org.
2017101700 7200 3600 24796800 3600
;;[S] self sig OK; [B] bogus; [T] trusted
```

as we see we will get “;; Signature ok but no chain to a trusted key or ds record”

CREDITS FOR PETER PARKER :D TO HELP ME IN THIS.

Question 9. Look up which cryptographic algorithms are available for use in DNSSEC. Which one do you prefer, and why?

DNSSEC was designed to be extensible so that as attacks are discovered against existing algorithms, new ones can be introduced in a backward-compatible fashion.

Some of these algorithms are:

Algorithm field Algorithm 1 RSA/MD5 3 DSA/SHA-1 5 RSA/SHA-1 (RFC 3110) 7 RSASHA1-NSEC3-SHA1 (RFC 5155) 8 RSA/SHA-256 (RFC 5702) 10 RSA/SHA-512

In my opinion RSA/SHA-256 (RFC 5702) is enough and good for DNSSEC because cryptographic operations are computationally expensive. They are robust algorithms and not broken yet (as we know). However if we choose weaker algorithms for speed we take a risk about the security part. In contrast, longer key lengths in cryptographic algorithms are associated with significantly greater computational expense and memory consumption. The uses the SHA-256 algorithm, which produces a 256-bit hash so that even the easiest attack (a so-called birthday attack) would take an an incredible amount of computing power — beyond the limits of what is believed to be practical for many years to come.That's why I choose RSA/SHA-256.

Source:

1- https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions#Algorithms

2- https://technet.microsoft.com/en-us/library/dn593667(v=ws.11).aspx

Question 10. In practice, different algorithms, key sizes and key lifetimes are chosen for KSKs and ZSKs. Discuss what are these differences in:

Before we list the differences, what are these 2 keys ? A KSK stands for Key Signing Key. A KSK is a public/private key pair. The KSK private key is used to generate a digital signature for the ZSK. The KSK public key is stored in the DNS to be used to authenticate the ZSK.

(a) algorithms

The idea behind this separation is that there are only a few signatures to validate that were made with a KSK, so it can have a higher security qualification than the ZSK. Having a longer KSK means less rollover of these keys, and thus less of the complicated interactions with the parent zone. The result of a lower-grade ZSK is that it can help to quickly resolve quite a few DNS records, but the disadvantage is that it cannot be safely used for long periods. This means that the ZSK must be replaced periodically.

The KSK is a different matter altogether; its validity is stated by the parent zone, which signs and publishes secure hashes of the KSK(s). The mere fact that other parties are involved in setting up or tearing down a KSK, thus making it more complicated to change, means that it is better to design that key for a higher level of security.

(b) key sizes

Lengths are 1024 bit for a one-month ZSK and “longer” for the KSK. Note that “longer” need not mean the double length: The search space doubles with every few bits added to a key, and in general the cracking effort grows exponentially with key size. Longer keys however, also waste resources on resolvers, which is preferred to keep as fast as possible. For a one-year period currently length consider 1280 to be a good KSK key size.

© key lifetimes

The Zone Signing Key can be used to sign all the data in a zone on a regular basis. When a Zone Signing Key is to be rolled, no interaction with the parent is needed. This allows for signature validity periods on the order of days.

The Key Signing Key is only to be used to sign the DNSKEY RRs in a zone. If a Key Signing Key is to be rolled over, there will be interactions with parties other than the zone administrator. These can include the registry of the parent zone or administrators of verifying resolvers that have the particular key configured as secure entry points. Hence, the key effectivity period of these keys can and should be made much longer.

and give the motivation for the difference.

According to RFC 4641 the motivation for the difference between the KSK and ZSK has several advantages:

1 - No parent/child interaction is required when ZSKs are updated.

2- The KSK can be made stronger. This has little operational impact since it is only used to sign a small fraction of the zone data. Also, the KSK is only used to verify the zone's key set, not for other RRSets in the zone.

3- As the KSK is only used to sign a key set, which is most probably updated less frequently than other data in the zone, it can be stored separately from and in a safer location than the ZSK.

4- A KSK can have a longer key effectivity period.

Source:

1- https://auda.zendesk.com/hc/en-us/articles/201442880-What-is-a-KSK-ZSK-RRSIG-

2- https://www.dnssec.nl/wat-is-dnssec/faq.html#KSK_ZSK_sleutels

3- https://tools.ietf.org/html/rfc4641#section-3.1

NOTE THAT THE ANSWERS FOR THESE QUESTIONS ARE FROM **RFC 4641**.

4- https://blog.surf.nl/en/cryptographic-sanity-key-sizes/

Question 11. Choose appropriate algorithms, key sizes and key lifetimes for your KSK and ZSK.

Based on what I answered above. I choose the following setup:

RSA/SHA-256 for KSK with key length of 2048 bits RSA/SHA-256 for ZSK with key length of 1024 bits

I will change the ZSK every 3 month, and the KSK every 1 year.

Question 12. Show the signed version of your zone file. How does it differ from the unsigned version? Any unexpected differences?

Generating KSK:

```
kotaiba@bristol:~$ dnssec-keygen -f KSK -r /dev/urandom -a RSASHA256 -b 2048
-n ZONE bristol.prac.os3.nl
Generating key pair.............+++
.........................................+++
Kbristol.prac.os3.nl.+008+35677
```

Generating ZSK:

```
kotaiba@bristol:~$ dnssec-keygen -3 -a RSASHA256 -b 1024 -r /dev/urandom -n
ZONE bristol.prac.os3.nl
Generating key pair.....................................++++++
.........++++++
Kbristol.prac.os3.nl.+008+23385
```

Now, sign the zone:

```
kotaiba@bristol:/usr/local/etc/nsd$sudo dnssec-signzone -S -K
/usr/local/etc/nsd/keys/ -g -a -r /dev/random -o bristol.prac.os3.nl.
bristol.prac.os3.nl

Fetching KSK 35677/RSASHA256 from key repository.
Fetching ZSK 23385/RSASHA256 from key repository.
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
bristol.prac.os3.nl.signed
```

Now, we need to check the signed zone:

```
kotaiba@bristol:/usr/local/etc/nsd$ cat bristol.prac.os3.nl.signed
; File written on Tue Oct 17 17:54:23 2017
; dnssec_signzone version 9.10.6
```

```
bristol.prac.os3.nl.    300    IN SOA    ns1.bristol.prac.os3.nl.
admin.bristol.prac.os3.nl. (
                    2017092411 ; serial
                    300        ; refresh (5 minutes)
                    300        ; retry (5 minutes)
                    300        ; expire (5 minutes)
                    300        ; minimum (5 minutes)
                    )
            300    RRSIG    SOA 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    Hp1z3+Vp9a/jWrtJMlpSK8haZY9YUgLgD7HC
                    BXaXR5zlEYKBpR2BMHQKhsZzjqr3XL6gzstA
                    fyLpFymnDeOyvXpADI+8I5EY1aV0XBcydyhC
                    rDv5Gci7GD66pu2z7SjCF5cfFVk5vXA8uc6z
                    z8WaeHoRHb3qney/cvn5Y3/ppCM= )
            300    NS    ns1.bristol.prac.os3.nl.
            300    RRSIG    NS 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    lvwmZkOXa2ucxHZIB4Xpg2r6VJImPuknSDJd
                    2/JdLsH33QZU+6DygAOuaH+qbJtgF8wmFj3p
                    zU98or/t3KgYwNqHk2jLcM0e/fd2odAsg4Yz
                    vKW/a4z4A9lclh+KofWgnGeo33BoiJX4ADyW
                    7M4kBpZkS1b6ZwPIAFrOu8Ygv1k= )
            300    A    145.100.104.163
            300    RRSIG    A 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    jE0FajdEnkt0GiZX6Qv5Nm3y1VilpRf7Kdvu
                    w5WO6t503nwvp0ApTDqBdiaf421SqkJaDHIw
                    6kZhHlBfLNYoeiktuZ4srDcMT8KJb1lRedsO
                    s0o1NBhBajmthS7hW4cr29veFPmCQmiHWgo9
                    kw2qfstnG6ZIpyBU93FHceqHY68= )
            300    MX    10 mail.bristol.prac.os3.nl.
            300    MX    20 mail.foix.prac.os3.nl.
            300    MX    20 mail.brest.prac.os3.nl.
            300    MX    20 mail.grenoble.prac.os3.nl.
            300    RRSIG    MX 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    V6GL5bNaYMoJdBZSVMHgzX85kzZENFOLfbHi
                    t8qVjBpdVBQAccdXqL/b35hSx8r/YG1hPLNQ
                    OwO4k3YevD+bLfr6MPYMMR8qU5RZ4Dor8v4p
                    b2TLDsg/a419DZiVoWEG3UVdWA55hfjapQC0
                    K5fO5R/gs+qvM6EkpFhEjxCUAZg= )
            300    TXT    "v=spf1 a mx -all"
            300    RRSIG    TXT 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    sV8sPQ3EPSh7ZsLEOXWY6nn8ItA+9wVE2QaI
                    DymB4F3bDNl8t2H3gABzLseBMfnQLF4Qi5lY
                    2RHnjizMoS/nA74zyvnQJdGY5r423f9Y2wSs
                    DzSwOXBcHTh00r0A16TRK1lCtKc0jOzfDCZ3
                    HHvxPPzTZibBwH9wT31tmzZ1Gds= )
            300    NSEC    201710._domainkey.bristol.prac.os3.nl. A NS SOA
```

```
MX TXT RRSIG NSEC DNSKEY
            300    RRSIG    NSEC 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    TTd2Bo04qr6XX2wBpCZ9XqMSIzDp4xaJwWde
                    j7w2IlbSLGjd1fCUtUttwjfEAwPnAB08hT5t
                    TBWszN+rO+nbTub+SINvkdHGXZvHJroxHy68
                    1R4Ixd6mNXp/dzl9voyJnW3wYSKEptXrSY+W
                    SqhthCsSm+3vP2024X4tRNcK2Uc= )
            300    DNSKEY    256 3 8 (
                    AwEAAct9g2aQqUrtiJh2ha+qUbQ+9iOVuBgN
                    chd0aE3LVUFa45i9fXhRtDuIo4wSoInyiSp2
                    Y9x0cyTypSflNGzzrUuMmNko35Ulxknf7fFK
                    KTkCdRw5HrSVRHHfAwD9ISoCpMGlrzfirY2Y
                    Ux8q3L7OSd2/UQkzrOrlWpf8qbVw1+zD
                    ) ; ZSK; alg = RSASHA256 ; key id = 23385
            300    DNSKEY    257 3 8 (
                    AwEAAcC4LwbH55G2W6/qR/G41ge/edFW1CZu
                    HIpVvF1uDN1uWP2xfXa9zirJH3CF7YMZw1Hj
                    g5/cU8EFQP5NNUgQi55jtpSB5KuUlLnoi768
                    y3yM/QDPZS0h2wxCL2z801/MrnM3pxytq/B0
                    T9Hnf3zAGLITZDMMbHIybgl7tPCqBmzjRLCO
                    Jnpz8xyKnHwhAHpKBbGeZPZAvD5qaiGu6oH6
                    VXT49LuVfCy0WWOcVsi9SczrbrMpvrjER1Xa
                    wb/XaPa/bK4JtP0e+12E7nNRtL50D3Po8c9r
                    vjD4VqeC4eg7XDdvYNz1UxBfT02nRX6KHfSM
                    /OdrDiKL//Rq5NhgeNmE/Zc=
                    ) ; KSK; alg = RSASHA256 ; key id = 35677
            300    RRSIG    DNSKEY 8 4 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    vAJbaAXV9pW+I38RtnPCUXgS4lf/ansq4dl5
                    P6gCchn3Ey4ZpbQyJAIz0ZgNfvy9C9d94ifG
                    DDVeh2tBA/VXWSIYB5Xf5A4JSeMh+iu5LPis
                    k1udoeI9pG6sq6Ec5rtQDKxag6IAoYw6gtA4
                    lgKSMsFmL4Ng20m4GwJLxnnB9Us= )
            300    RRSIG    DNSKEY 8 4 300 (
                    20171116145423 20171017145423 35677 bristol.prac.os3.nl.
                    N58pqK/bH9NBZiNTzmV+ZLrNZBQRkeXMxfpK
                    LWTg4uh1K6TNHw9lXVOvAgSwOB8aOnR1N5bg
                    ju2GRTcpJ0kUQlavaYD8J3OJTFm8eQb3YZd1
                    dBP5out4SZeWCbev5uJt/OgjeottdOQCbabK
                    kcXk5M1PlGm5GPWJ/2jAet5QuxELXd2R+ZBx
                    r4cT4psRlEHjSrL7VB07GP+PN5KyFXlekbGu
                    5Oevwy8pdfBEgt7AeWfKCWwJoRHXX/aE6cdc
                    Lz1aNqMIV3C9Fv3HyZVWFRkkDL7OWGQU2kW9
                    q6EHMXqihDBdY6KF9U6awf0Ctp7o3OI45xVA
                    26HSdFCAplO7Q+8cXA== )
201710._domainkey.bristol.prac.os3.nl. 300 IN TXT "v=DKIM1; k=rsa-sha256;
s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ySql41pk2fMBeKC+JVdxMcq80rc8
pn76B/HYi4yMYt6fYIvB5iwpYaiLfCJ6t7hl7aP9zgSNQtPY0zLIRp7+EbjP5qQ07NRvnXNvqVmo
5PX0IwqFlunOJNWqrKImC3K9k9sr2oax1Yc6VCfk1hbZ2YtX/YVC1DH0Bp0A9O3J+2taCmcMe3hR
```

```
KsbaR9yqSTUhdKQfgMjBESFV3"
"znqBfgnrQ4V5fywDeOldz/yirj3KktcoDyksdifbndqSmbU/64rcK5xmP60wXj3FnW05B4Bs0H9
LnURngO9py35Z5NQXXEhRAG/KJkMgS3i1Fa9hvWjjew+D2zUq4Vcu5Yj1oHjQIDAQAB"
            300    RRSIG    TXT 8 6 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    BtoRGSqbD3hLOhhmWgTQ6u1wRTI1vNKpUyqF
                    VFlD5U/oBdkR5l4Gv1CzlIftuRCwgYapvs4I
                    7q9qAXOd9osRvYgyQf5rnZZRWnPMGRs2l9Ec
                    cEn21dQzBskcsJDtkf28NPXpW4ZZTgM7h1pc
                    fFZ8RDwIjMaM3zaO0Yz6/FQEXu4= )
            300    NSEC    mail.bristol.prac.os3.nl. TXT RRSIG NSEC
            300    RRSIG    NSEC 8 6 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    HHw3hfbUz337jtttYq5Ozd6Cwet7PC5EmgQz
                    DYzd/bHHXHEn9Mb6FsnH/EYQ+IgguXoXdiRO
                    5rrjRHHAYw4Va8Yu4cLi8dcOqwnAGcMeZ5pD
                    RoSS12gwK9Lhw1XzxXQ8Bjq2EBZvfTqT5FVF
                    PQnvMJC5IjAnUG026Ygvs+QwhYk= )
www.bristol.prac.os3.nl. 300    IN CNAME bristol.prac.os3.nl.
            300    RRSIG    CNAME 8 5 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    dr0lGYYt+veuz2bCM4Asa03Ly+Ao7qTzda5A
                    lF4TwQf4Whf02TDj4vSjd/yTgU4UqhwTbWLS
                    M/8JvXst3ANavUx/b2rKaS/XRIV0tNnRW3iK
                    p5rGQSfj80rjgei9ebBLFXFJ6BYAI7kikqP8
                    RfCsG21p71LWX1Zy8BnRsA6APx8= )
            300    NSEC    bristol.prac.os3.nl. CNAME RRSIG NSEC
            300    RRSIG    NSEC 8 5 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    d+WvCEiQNNhGxJuZtTrWey5lEL2gsyt1Xwq9
                    BZpZUpK1Udr7pU4jwJiTIcnecH0kRbxykuZ4
                    NCGlwkiWr0Pf/+5vcPXU3AO1vnmIc9oQHOwf
                    PisT4FZ46LKz+9Sdl3Enq94qd78L2oi6e+eB
                    Wy6w6ybFbC1RYSC7FD82YGVRsL8= )
ns1.bristol.prac.os3.nl. 300    IN A    145.100.104.163
            300    RRSIG    A 8 5 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    NDGx3gRoWTXBfm88XxjCH7dfKHAiSPxoUjHm
                    Omp3n1XASdDYc4moy+T0WW+SMIje+wcMBf7Z
                    Q1Q/Xogh2N5dGRo76fzngG7AJQoWgHt8A22c
                    EgyA5zbSB3T7IbJHROcB/74YSbpNCuTIjIzF
                    1oQPxP0gjB4UM7ArUMLTfg08WPA= )
            300    AAAA    2001:610:158:1046:145:100:104:163
            300    RRSIG    AAAA 8 5 300 (
                    20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                    O3ETaHIS0QmTeNH4gXvkwFhNXhuQf6g3cqe1
                    u6OlzWXWm3p/HF3z2lwG2Gv9qB5SXr2bSEFH
                    NWPrPU9/1WsERrf0Lm1s96DMLPKom5wuJLzT
                    MNV75/IgPO4uuXhIFxgLp+EdV7J8Wqyt8ddk
                    ABOyMe1R50h7vyVyi/WYJ/p+D6k= )
            300    NSEC    nsreim.bristol.prac.os3.nl. A AAAA RRSIG NSEC
```

```
            300    RRSIG    NSEC 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   kWRQoE8xZXX2Ez2whWOxWabAoR0GCdddt/uJ
                   rO4FQ9V9Tbki/Z8+ePlhZfczXQaILxxNkQGD
                   EWOLYnICQwOlaO4qF9YmHnDhUSQz/ZPj7OjX
                   xWqdcK/t9owpUdWXLbC5EdYFGrEgkt2BXl+9
                   Pia4jKA65aXXxP0kzjP84utcJ/4= )
sub.bristol.prac.os3.nl. 300    IN A    145.100.104.163
            300    RRSIG    A 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   Dm2aH3YeiohBIfc3E0ZhTMNkLtAjqzjG36tQ
                   huxriWvDH7nGIU73US84cKzo61FGB9WJ3+P7
                   4W46Pjkp24t8eF/zpCVaqug1gCkb5PLwu8O1
                   YMZxql1PBSNsCiuBkrdjbL+J6zYeGEVU3RWH
                   5l9tvJ1hEcoVzQIDU8373G4ank0= )
            300    MX    15 mail.bristol.prac.os3.nl.
            300    RRSIG    MX 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   mo8lJUD1c6+3tr0RZRnbS2h3Cj9pZKcymj2W
                   Qy+K24MfTcTYLgzS5hbM2iLW7YNZqnT0z3wJ
                   CxXxcrQgVzsXsEobAra7E9NXP36Ekp0bglUH
                   nVkoScCqxJqwKzdiJCbT4noLd8aVEzz0oRk9
                   VG6lp7UcD/BIFZV7wFQeMwGNOYw= )
            300    NSEC    www.bristol.prac.os3.nl. A MX RRSIG NSEC
            300    RRSIG    NSEC 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   chsP6bnIDbKolr82ExsCKf9Dd7/gYPCeN4tD
                   uiEJL+Nse6fM/ajfy8tn2liQKrIIa8RXaffW
                   zLZG4d7dHnSJvRvqKCkuHTb0JDF99NDvRDmv
                   CXXgOrQZhIT/ggexcOtf4ag3T8NxpRnDnSTp
                   2N0Vh2nIK7pKMckzMOLFGaethf0= )
nsreim.bristol.prac.os3.nl. 300 IN A    145.100.104.122
            300    RRSIG    A 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   TVkNc1NnbYjTk9uYJ7mdN34oYUxkHQPjle1n
                   yBb7U0j2dhphgjovNf0vsUgz9o7dcJaWFw4V
                   xxBJFXYcKK04YhVFvmXUbCSGnUmL6Cq3Qn3f
                   PW/3dOPPdOFeE1z9O79jhxu9/0NAxK2isA3k
                   cStMHU9rjMQtGP7tX71feS5FKLA= )
            300    NSEC    sub.bristol.prac.os3.nl. A RRSIG NSEC
            300    RRSIG    NSEC 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   nFMEWCKT7VdxOGxkCO1+VrNo/R5AaCspR8EB
                   SQEHL94lY/bS8culiIdO018y/DxRkroPaHOM
                   +YlSRD7hm9sK7eaMynnC8ssmShDXTBBjIbXh
                   LBFUA5lcSr2edpMZVy8Kw5DiBxXARZcX1isc
                   U7/2S1NDPgr1Y4aHyM7/89DYawI= )
mail.bristol.prac.os3.nl. 300   IN A    145.100.104.163
            300    RRSIG    A 8 5 300 (
                   20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                   KwHlDCXifXeJwaa7iwobY2U4O8iqwgIAUSHU
```

```
                 Lj2bfApLJS7R7pjygBIWwSifZ88jYK/6zFvP
                 FBGJ1QOAu7kVwN7XR7qkFElXr8tRXI0UJVN7
                 qAKrE6FpWYbpKcjOjp92MLhpHaxV2a+RKASb
                 XxDHFDBloKaA06f4LM9ynq3lCm0= )
        300    AAAA    2001:610:158:1046:145:100:104:163
        300    RRSIG    AAAA 8 5 300 (
                 20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                 UO86mSSkUpz5JvU31YYNSmMz3DBvle4XfAYm
                 0OgR09ok/jjFYpp6DIBcsHQcPOIedKV18bsK
                 rqKCn6otbxipvnu9NJPCmJaNq3iChuofa7EP
                 EgcLgMRYHZHLG/DVJ62zqulxG5XLnmAAd5Wj
                 c3JWAZODKZDUKyRlB2DK5HjeneM= )
        300    NSEC    ns1.bristol.prac.os3.nl. A AAAA RRSIG NSEC
        300    RRSIG    NSEC 8 5 300 (
                 20171116145423 20171017145423 23385 bristol.prac.os3.nl.
                 TlZrmoesni8gJ/dcXrn5eX0wBJ6f2MlqbtJX
                 IZHW+7eyTTacNPI529p7aXvFYzLt0G559cNb
                 mhhL02NHaz8FxjEseN51oxvIO+7FTTzb076R
                 75DrXtXR3sts3Kta0LecVrfumnVqM5SKO5ln
                 USOpqI9ngvJLXWdibu1bGv6GfWk= )
```

As, we see in the singed zone we have more records suck as NSEC, RRSIG and DNSKEY.

Source:

1- https://www.dnssec.nl/cases/dnssec-en-bind-named-deel-i-het-ondertekenen-van-de-zones.html

Edit the BIND/NSD configuration to include the signed version of your zone file.

I edited my nsd.conf file, I added:

```
zone:
        name: "bristol.prac.os3.nl"
        zonefile: "bristol.prac.os3.nl.signed"
```

Restart the authoritative server and look at the syslog for errors.

```
kotaiba@bristol:/usr/local/etc/nsd$ sudo nsd-control stop
ok
kotaiba@bristol:/usr/local/etc/nsd$ sudo nsd-control start
[2017-10-17 18:00:19.034] nsd[30706]: notice: nsd starting (NSD 4.1.17)
[2017-10-17 18:00:19.037] nsd[30706]: info: setup SSL certificates
kotaiba@bristol:/usr/local/etc/nsd$ echo $?
0
```

If the server appears to be up and running, test DNSSEC by querying your server for the DNSKEY of bristol.prac.os3.nl.

```
kotaiba@bristol:/usr/local/etc/nsd$ dig DNSKEY bristol.prac.os3.nl +dnssec
; <<>> DiG 9.10.6 <<>> DNSKEY bristol.prac.os3.nl +dnssec
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10627
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;bristol.prac.os3.nl.       IN    DNSKEY

;; ANSWER SECTION:
bristol.prac.os3.nl.    300    IN    DNSKEY    257 3 8
AwEAAcC4LwbH55G2W6/qR/G41ge/edFW1CZuHIpVvF1uDN1uWP2xfXa9
zirJH3CF7YMZw1Hjg5/cU8EFQP5NNUgQi55jtpSB5KuUlLnoi768y3yM
/QDPZS0h2wxCL2z801/MrnM3pxytq/B0T9Hnf3zAGLITZDMMbHIybgl7
tPCqBmzjRLCOJnpz8xyKnHwhAHpKBbGeZPZAvD5qaiGu6oH6VXT49LuV
fCy0WWOcVsi9SczrbrMpvrjER1Xawb/XaPa/bK4JtP0e+12E7nNRtL50
D3Po8c9rvjD4VqeC4eg7XDdvYNz1UxBfT02nRX6KHfSM/OdrDiKL//Rq 5NhgeNmE/Zc=
bristol.prac.os3.nl.    300    IN    DNSKEY    256 3 8
AwEAAct9g2aQqUrtiJh2ha+qUbQ+9iOVuBgNchd0aE3LVUFa45i9fXhR
tDuIo4wSoInyiSp2Y9x0cyTypSflNGzzrUuMmNko35Ulxknf7fFKKTkC
dRw5HrSVRHHfAwD9ISoCpMGlrzfirY2YUx8q3L7OSd2/UQkzrOrlWpf8 qbVw1+zD
bristol.prac.os3.nl.    300    IN    RRSIG    DNSKEY 8 4 300 20171116145423
20171017145423 23385 bristol.prac.os3.nl.
vAJbaAXV9pW+I38RtnPCUXgS4lf/ansq4dl5P6gCchn3Ey4ZpbQyJAIz
0ZgNfvy9C9d94ifGDDVeh2tBA/VXWSIYB5Xf5A4JSeMh+iu5LPisk1ud
oeI9pG6sq6Ec5rtQDKxag6IAoYw6gtA4lgKSMsFmL4Ng20m4GwJLxnnB 9Us=
bristol.prac.os3.nl.    300    IN    RRSIG    DNSKEY 8 4 300 20171116145423
20171017145423 35677 bristol.prac.os3.nl.
N58pqK/bH9NBZiNTzmV+ZLrNZBQRkeXMxfpKLWTg4uh1K6TNHw9lXVOv
AgSwOB8aOnR1N5bgju2GRTcpJ0kUQlavaYD8J3OJTFm8eQb3YZd1dBP5
out4SZeWCbev5uJt/OgjeottdOQCbabKkcXk5M1PlGm5GPWJ/2jAet5Q
uxELXd2R+ZBxr4cT4psRlEHjSrL7VB07GP+PN5KyFXlekbGu5Oevwy8p
dfBEgt7AeWfKCWwJoRHXX/aE6cdcLz1aNqMIV3C9Fv3HyZVWFRkkDL7O
WGQU2kW9q6EHMXqihDBdY6KF9U6awf0Ctp7o3OI45xVA26HSdFCAplO7 Q+8cXA==

;; Query time: 9 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Oct 17 18:02:54 CEST 2017
;; MSG SIZE  rcvd: 958
```

It Works :D

Question 13. Which DS record do you need to send to Niels, and why that one?

In addition to the signed zone file, there is a file named dsset-bristol.prac.os3.nl. (due to the '-g' option). generated. That contains the DS records (extracts of keys) that should be included in the parent zone in the domain name hierarchy.

```
kotaiba@bristol:/usr/local/etc/nsd$ cat dsset-bristol.prac.os3.nl.
bristol.prac.os3.nl.    IN DS 35677 8 1
056A74991A027B43B106877A06E315C1B36A9580
```

```
bristol.prac.os3.nl.    IN DS 35677 8 2
5411547461493C090408F47A8766E4FE49736E1963F6B16B495D887A 804F8254
```

I will send the DS-2 record to Niels:


```
bristol.prac.os3.nl.    IN DS 35677 8 2
5411547461493C090408F47A8766E4FE49736E1963F6B16B495D887A 804F8254
```


The last one, with “Digest type” 2, is the KSK extract to be uploaded to the registrar.

Question 14. Show the results of the examination of your secured domain.

Using the link that you provided for the DNSSEC examination, here is a screenshot of the result:

Source:

1- http://dnssec-debugger.verisignlabs.com/bristol.prac.os3.nl

Question 15. Describe the DS and DNSKEY records from os3.nl down that are important for your domain. Which keys are used to sign them?

the DS and DNSKEY records from os3.nl down that are important for my domain are below:

```
os3.nl.         15284 IN DNSKEY    257 3 5 (
                AwEAAbyzpi3ynVCs9Zcd2tAuYekjk3Vp894JH8KaxVyX
                zVfmqURWgT4ddimAuTtl91r5ajWI+9zteNVRu+9taVkq
                O1PP8kTRmN2zxlMUbGZ6e18zPk099Pdmz1brxwsSCOSH
                k7jWJR3ohjCYjrHkl2keFD/uViPj98ZFr1SnW7PiIpdl
                0w18eT547r+ng8Fffnn82erLPxdS15U14SrYjyqbA4rS
                XM4ntOsrQelRJ+6YGQcdNLmWyLyKIn9jtzcR56pS4S/r
                G5Rz8IF59Ol4cxsjhukPyixMyexL1O2c64wKmLgpJEcM
                0eifm0MzaHeSP1voYn8gajpA+3fln5cUTV5RPBM=
                ) ; KSK; alg = RSASHA1 ; key id = 64426
os3.nl.         15284 IN DNSKEY    256 3 5 (
                AwEAAcDCrv6e/KXaBjqvqld3brtldPsvHBoTQDO5YGKy
                +ELfO3owjsdapdHSxlmbcsNc1Obczwu53yqlDRTPnGNu
                2fvQ6FzeLdlv9LEe3kwFWnlDDb8tmENtXlu792gPs3x1
                d0a2G77Sd/J9ihpUsy4jnlVfWScuoBDVrXm5P9d9q77z
                ) ; ZSK; alg = RSASHA1 ; key id = 42048
```

Those keys “KSK” and “ZKS” are important for signing my domain. Since the ZSK of os3.nl is signing the DS records of my domain that I sent to Niels to sign.

The figure below will show a same case for our case.

Source:

1- https://blog.resellerspanel.com/wp-content/uploads/2017/02/dnssec-ds-records.jpg

Question 16. Start planning for a Zone Signing Key rollover.

(a) Describe the options for doing a ZSK rollover, make a motivated choice for one procedure.

There are two methods for doing a ZSK rollover: 1- a Pre-Publishing method, where the DNSKEY record is already announced. 2- Double Signature method, where the zone is signed using both keys temporarily.

I will choose Double Signature method because it is straightforward to implement. This method means that my zone doubles in size temporarily, and the new key can be generated when you want to do the rollover.

(b) How do you implement this procedure with the tools for signing your zone?

1- Generate new ZSK (ZSK-1) (as we did above) 2- Move ZSK-1 to the zone keys folder 3- Sign with ZSK-1 / ZSK-0 / KSK 4- Remove ZSK-0 DNSKEY record and sign again with ZSK-1 / KSK 5- Reload your zone (nsd-control).

© Which timers are important for this procedure?

1- Signature validity period 2- Maximum/Minimum Zone Time to Live (TTL)

(d) Implement the procedure and use a DNSSEC debugger to verify each step. Don’t forget to show the results of each verification.

1- First generate new ZSK key

```
kotaiba@bristol:~$ dnssec-keygen -3 -a RSASHA256 -b 1024 -r /dev/urandom -n
ZONE bristol.prac.os3.nl
Generating key pair.....++++++ .....++++++
Kbristol.prac.os3.nl.+008+05940
```

2- Move the ZSK key to the keys folder

```
kotaiba@bristol:~$ sudo mv Kbristol.prac.os3.nl.+008+05940.private
/usr/local/etc/nsd/keys/
```

3- Sign zone with all three keys:

```
kotaiba@bristol:/usr/local/etc/nsd$ sudo dnssec-signzone -t -S -K
/usr/local/etc/nsd/keys/ -g -a -r /dev/random -o bristol.prac.os3.nl.
bristol.prac.os3.nl
Fetching ZSK 5940/RSASHA256 from key repository.
Fetching KSK 35677/RSASHA256 from key repository.
Fetching ZSK 23385/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 2 active, 0 stand-by, 0 revoked
bristol.prac.os3.nl.signed
Signatures generated:                       45
Signatures retained:                         0
```

```
Signatures dropped:                              0
Signatures successfully verified:               45
Signatures unsuccessfully verified:              0
Signing time in seconds:                     0.019
Signatures per second:                    2366.552
Runtime in seconds:                          0.026
```

4- Reload signed zone and wait until the key expiry date, then remove first ZSK and resign zone.

Remove the ZSK key from the file (I just moved it to the home):

```
kotaiba@bristol:/usr/local/etc/nsd/keys$ sudo mv
Kbristol.prac.os3.nl.+008+23385.* /home/kotaiba/
```

Sign it again:

```
kotaiba@bristol:/usr/local/etc/nsd$ sudo dnssec-signzone -t -S -K
/usr/local/etc/nsd/keys/ -g -a -r /dev/random -o bristol.prac.os3.nl.
bristol.prac.os3.nl
Fetching ZSK 5940/RSASHA256 from key repository.
Fetching KSK 35677/RSASHA256 from key repository.
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
bristol.prac.os3.nl.signed
Signatures generated:                           23
Signatures retained:                             0
Signatures dropped:                              0
Signatures successfully verified:               23
Signatures unsuccessfully verified:              0
Signing time in seconds:                     0.011
Signatures per second:                    1959.948
Runtime in seconds:                          0.019
```

Now, lets test our implementation:

```
kotaiba@bristol:/usr/local/etc/nsd$ dig +dnssec bristol.prac.os3.nl

; <<>> DiG 9.10.6 <<>> +dnssec bristol.prac.os3.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43538
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;bristol.prac.os3.nl.       IN    A

;; ANSWER SECTION:
```

```
bristol.prac.os3.nl.    300    IN    A    145.100.104.163
bristol.prac.os3.nl.    300    IN    RRSIG    A 8 4 300 20171116161411
20171017161411 5940 bristol.prac.os3.nl.
huaTSYgZn4nHGiHQm83sJEwOTXmkyX+c9K/zmEklWolsOnovwZtpe5wh
4iI3OVO1l6tdftGIqtUVGkD3X3PkLhtWT2DqdgX7NIoFV1fTFB8V1zlS
TGQf3yXBchiXZAJGeXTa1+NPUmKXQJp40COpc5YufPwvVQe3YlsR+im3 HUE=

;; Query time: 4 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Oct 17 19:16:13 CEST 2017
;; MSG SIZE  rcvd: 243
```

IT WORKS :D

Source:

1- https://1sand0s.nl/2014/08/dnssec-key-rollovers-explained/

2- I got help from Peter and his Wiki.

Question 17. Can you use the same procedure for a KSK rollover? What does this depend on?

Yes, The DS-record must be given to the parent in order to set-up the chain of trust again also It depends on the delegation responsible, or authority.