Innopolis University

SYSTEM AND NETWORKING ENGINEERING

Classical Internet Applications

LABORATORY REPORT 5

DNS Security Extensions (DNSSEC)

Student Name	Student ID
Sergey Grebennikov	47611

Lecturer:

Rasheed Hussain

Submission Date : October 10, 2017

Contents

1 Introduction

DNS has been designed without security in mind. Since security researcher Dan Kaminsky demonstrated the ease of DNS cache poisoning, DNSSEC, a DNS security extension, has become popular. DNSSEC is an open standard, documented in various RFCs that adds cryptographic protection to DNS making it hard to forge DNS replies.

2 Setting Up A Validating Resolver

1. What does a validating resolver do?

   Answer:

   It performs DNSSEC validation of the data that it receives.

Could you please describe the step which resolver do for validating ?

To validate any domain Resource Records a Validating Resolver do the following steps:

(a) At first, we need to add a root's public KSK as a *trust-anchor* (from which the whole *chain of trust* is derived) to the unbound configuration file

(b) The process starts when a validating resolver sets the **DO** (**D**NSSEC **O**K) flag bit in a DNS query

(c) The validating resolver would start with verifying the **DS** and **DNSKEY** records at the DNS root

(d) Then it would use the **DS** records for the top level domain found at the root to verify the **DNSKEY** records in the top level domain zone

(e) From there, it would see if there is a **DS** record for the subdomain in the top level domain zone, and if there were, it would then use the **DS** record to verify a **DNSKEY** record found in the subdomain zone

(f) This would continue until we go down to the required domain

(g) Finally, validating resolver would verify the **RRSIG** record found in the answer for the Resource Records

2. Add support for DNSSEC to the Unbound configuration.

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

```
$ cd /usr/local/etc/
$ sudo chown -R unbound:unbound unbound
$ cd unbound
$ sudo -u unbound touch root.key
$ sudo -u unbound unbound-anchor
$ sudo -u unbound unbound-anchor -a root.key
```

   The next line was added to the **unbound.conf** file:

```
server:
...
        auto-trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

   (b) Verify the root key used against a trusted source.
   Answer: Figure 1

3. Use **dig** or **drill** to verify the validity of DNS records for *isc.org* and *os3.nl* (Figure 2).

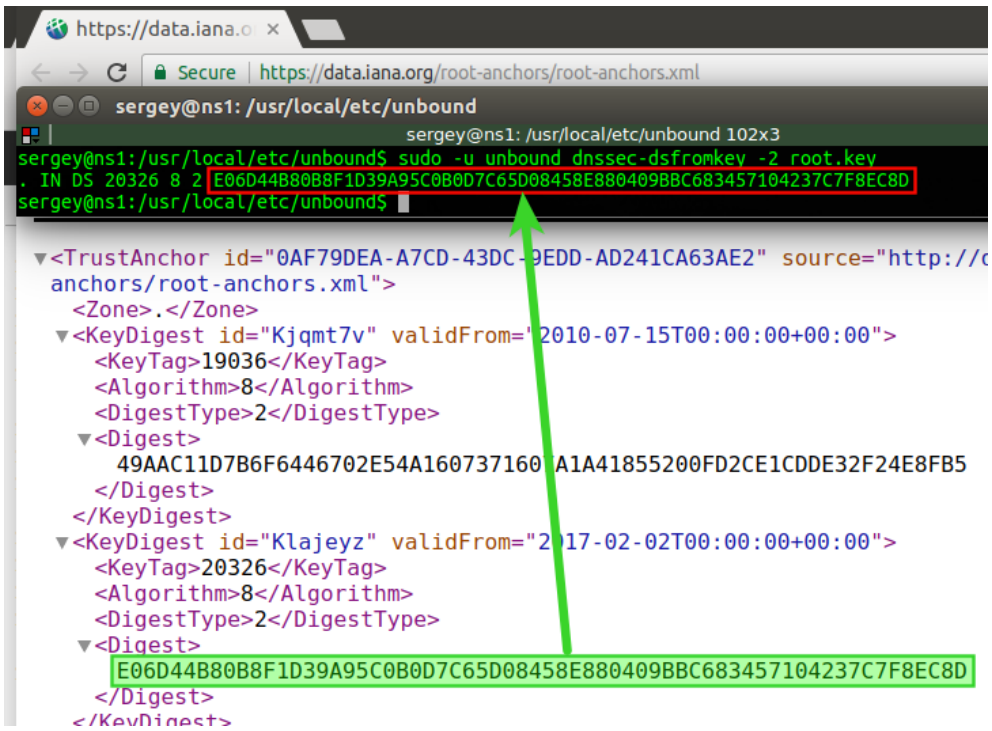

Figure 1: Verifying the root key

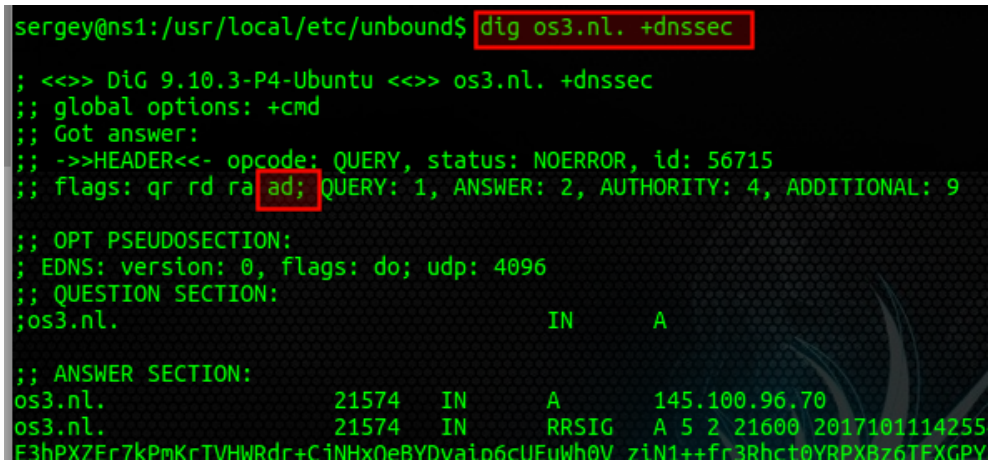

Figure 2: Validity of DNS records

4. How does **dig**/**drill** show whether DNSSEC validation was succesful or not?

   Answer:

   The response should contain AD flag that means **A**uthenticated **D**ata. It indicates that all data have been authenticated by the server. AD flag should be set only if all data in the response has been cryptographically verified or otherwise meets the server's local security policy.

ok where it is updated and maintained ?

The command **dig** allows using **+dnssec** option that requests DNSSEC records be sent by setting the **D**NSSEC **O**K bit (**DO**) in the OPT pseudo resource record in the additional section of the query.

5. Where does Unbound store the DNSSEC root key?

   Answer:

   The DNSSEC root key is stored in the file **/usr/local/etc/unbound/root.key**.

ok please add more details

The DNSSEC root key acts as the trust anchor for DNSSEC for the Domain Name System. This trust anchor is configured in DNSSEC-aware resolvers to facilitate validation of DNS data.

Output root.key file:

```
$ cat /usr/local/etc/unbound/root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1505456533 ;;Fri Sep 15 09:22:13 2017
;;last_success: 1505456533 ;;Fri Sep 15 09:22:13 2017
;;next_probe_time: 1505497275 ;;Fri Sep 15 20:41:15 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
.        172800        IN        DNSKEY        257 3 8 AwEAAaz/tAm8yTn4M
 ↪  feh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5e
 ↪  mLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8Pzg
 ↪  Cmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbu
 ↪  v7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhH
 ↪  dY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
 ↪  ;{id = 20326 (ksk), size = 2048b} ;;state=1 [ ADDPEND ] ;;count=33
 ↪  ;;lastchange=1505204858 ;;Tue Sep 12 11:27:38 2017
.        172800        IN        DNSKEY        257 3 8 AwEAAagAIKlVZrpC6
 ↪  Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqB
 ↪  GCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/
 ↪  QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6
 ↪  G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu
 ↪  +ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
 ↪  ;{id = 19036 (ksk), size = 2048b} ;;state=2 [  VALID  ] ;;count=0
 ↪  ;;lastchange=1505126662 ;;Mon Sep 11 13:44:22 2017
```

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

   Answer:

   trusted-keys are copies of DNSKEY RRs for zones that are used to form the first link in the cryptographic chain of trust.

managed-keys are trusted keys which are automatically kept up to date via **RFC 5011** trust anchor maintenance.

ok but no output is shown

trusted-keys and **managed-keys** server options use in **BIND** configuration file. **Unbound** configuration file has **auto-trust-anchor-file** server option. This file contains trusted keys for validation. Both DS and DNSKEY entries can appear in the file. The format of the file is the standard DNS Zone file format.

unbound.conf file:

```
server:
...
        auto-trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

7. How did you modify the DNSSEC root key?

   Answer:

   Changed the value of the public key in the DNSKEY record (Figure 3)

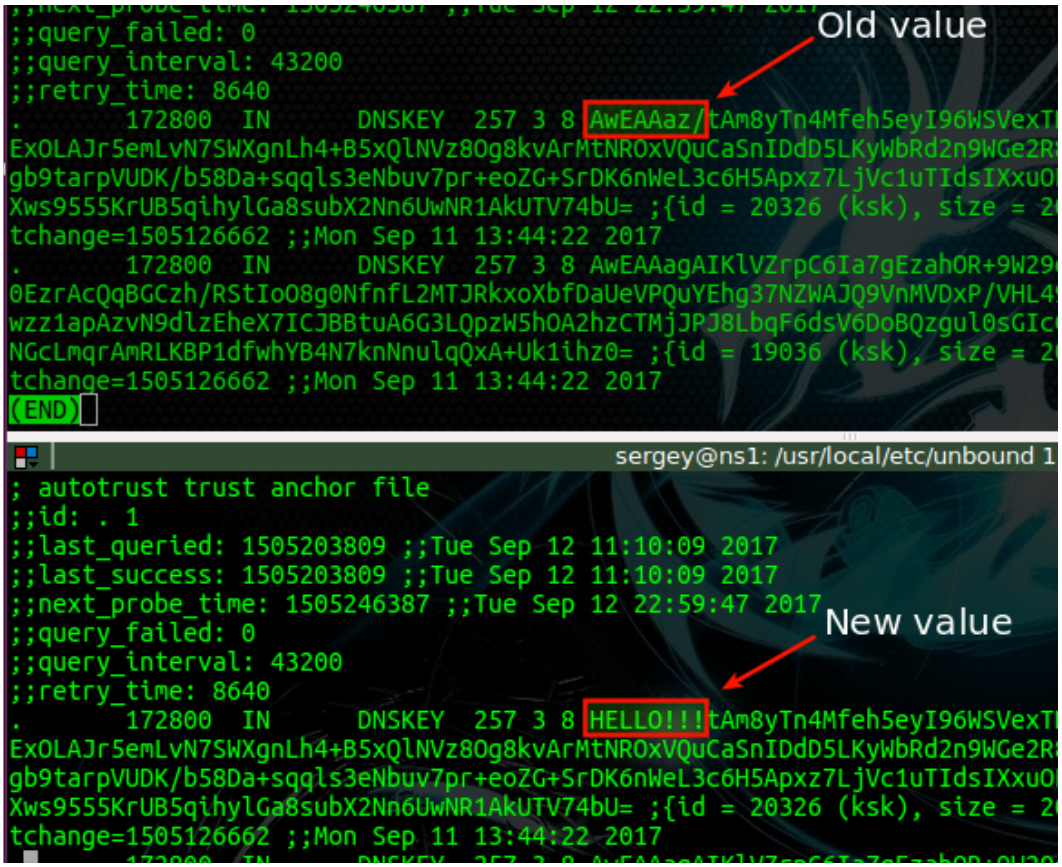

Figure 3: Modifying the root key

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

   The unbound.log file:

```
...

[1505379917] unbound[14187:0] info: 127.0.0.1 os3.nl. A IN
[1505379917] unbound[14187:0] info: 127.0.0.1 os3.nl. A IN SERVFAIL
↪  0.214435 0 35

...
```

Request DNSSEC records:

```
$ dig os3.nl +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> os3.nl +multiline +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 40961
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 214 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Sep 14 12:05:17 MSK 2017
;; MSG SIZE  rcvd: 35
```

3 Setting Up A Secure Zone

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

   Answer:

Algorithm field	Algorithm	Reference
1	RSA/MD5	[RFC3110][RFC4034]
2	Diffie-Hellman	[RFC2539]
3	DSA/SHA1	[RFC3755]
5	RSA/SHA-1	[RFC3110][RFC4034]
6	DSA-NSEC3-SHA1	[RFC5155]
7	RSASHA1-NSEC3-SHA1	[RFC5155]
8	RSA/SHA-512	[RFC5702]
10	RSA/SHA-512	[RFC 3110]
12	GOST R 34.10-2001	[RFC 3110]
13	ECDSA Curve P-256 with SHA-256	[RFC5702]
14	ECDSA Curve P-384 with SHA-384	[RFC6605]
15	Ed25519	[RFC8080]
16	Ed448	[RFC8080]

I prefer use SHA-256 or SHA-512, because it is widely believed to be more resilient to attack than SHA-1 or MD5 [5]. In addition, SHA-256 and SHA-512 are proposed for use in DNSSEC [6].

10. In practice, different algorithms, key sizes and key lifetimes are chosen for **KSK**s and **ZSK**s. Discuss what are these differences in:

    (a) algorithms

    (b) key sizes

    (c) key lifetimes

    and give the motivation for the difference.

    Answer:

    - **Algorithms:** It is recommended to use public key algorithms based on hashes that are stronger than RSASHA-1 (for example, RSASHA-256) for KSK and ZSK [7]
    - **Sizes:** KSK sizes: 1024 bits for low-value domains, 1300 bits for medium-value domains, and 2048 bits for high-value domains. ZSK size: The difference with the KSK should be limited to 100 bits. [7]
    - **Key lifetime:** For Key Signing Keys, it is reasonable to set 13 months with the intention of replacing them in 12 months. A month is reasonable for Zone Signing Keys. [7]

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

    KSK:

    - **Algorithm:** RSASHA-256
    - **Sizes:** 2048 bits
    - **Key lifetime:** 13 months

    ZSK:

    - **Algorithms:** RSASHA-256
    - **Sizes:** 1024 bits
    - **Key lifetime:** A month

There are various tools that can generate keys and sign zones. NSD+Unbound uses the **ldns** tools from NLnet labs , in particular, **ldns-keygen** and **ldns-signzone** .

Generation the KSK and ZSK for zone

ZSK

```
$ sudo -u nsd ldns-keygen -a RSASHA256 -b 1024 -r /dev/random st13.os3.su
Kst13.os3.su.+008+18969
$ ls
Kst13.os3.su.+008+18969.ds
Kst13.os3.su.+008+18969.key
Kst13.os3.su.+008+18969.private
```

KSK

```
$ sudo -u nsd ldns-keygen -a RSASHA256 -k -b 2048 -r /dev/random st13.os3.su
Kst13.os3.su.+008+15514
$ ls
Kst13.os3.su.+008+15514.ds
Kst13.os3.su.+008+15514.key
Kst13.os3.su.+008+15514.private
```

Zone signing

```
$ sudo -u nsd ldns-signzone st13.os3.su.zone Kst13.os3.su.+008+15514
 ↪  Kst13.os3.su.+008+18969
$ ls
st13.os3.su.zone.signed
```

12. Show the signed version of your zone file.

```
$ cat st13.os3.su.zone.signed
st13.os3.su.        3600        IN        SOA        ns1.st13.os3.su. vkaser.st13.os3.su. 2017090602
 ↪  86400 7200 2419200 3600
st13.os3.su.        3600        IN        RRSIG        SOA 8 3 3600 20171012110724 20170914110724
 ↪  18969 st13.os3.su.
 ↪  rOFMed/sCG+BO/w5WmgPPwlYs/M5OkjA7KgY2yApiv8/HZheErKbPRSlTSreW/wpRTs69JiNFRmDYKsm66/NnNHW2GzP4k
 ↪  TwmrtPlW82ie6Ypq22RpmQLzqi4AIia+wqzNGS4LjFfZywnfUqJF3Sv//LHPLkZZHFZ74/V3zPlTI=
st13.os3.su.        3600        IN        A        188.130.155.46
st13.os3.su.        3600        IN        RRSIG        A 8 3 3600 20171012110724 20170914110724
 ↪  18969 st13.os3.su.
 ↪  WUy2ax5YLkxP3ow3iZWV0i1lRxlRZ7SHtiM1hakh3U+72VbujFvqz0x2C01pl2icWDF1VYtVIQl7KQg22xajpNdmACl1G0
 ↪  qoq8zvSjtcL8FOHHhd+Nt516klclCe0B6/elf70w6I2KxugjFjY6+U6R47wMvA6GsfiXMJ87EZEjU=
st13.os3.su.        3600        IN        NS        ns1.st13.os3.su.
st13.os3.su.        3600        IN        NS        sub.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        NS 8 3 3600 20171012110724 20170914110724
 ↪  18969 st13.os3.su.
 ↪  zGyu/kJLms4ZB+58qLqGFPE6qrGe0jGS7d0hjEU+0pKYSZqIx0kXyq1jaEZaEi0GhM2j8TxUMwLYbwvGtKXX8LzXUBABAk
 ↪  hCjGm9DTGbWC6SmUwJ4OK42WPobzd+YHChZfJnfNy4hndCmMVCFCWVNSxPtf9zD8Vzi47byTSKKyU=
st13.os3.su.        3600        IN        MX        10 mail1.st13.os3.su.
st13.os3.su.        3600        IN        MX        50 mail2.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        MX 8 3 3600 20171012110724 20170914110724
 ↪  18969 st13.os3.su.
 ↪  wzfI3pA6HCuFNJqUZvd804yYA4AdA78p2fNsi0S+gaas1sDvQTti9XA1bGlgZpvNiB2y1C4okSyK81z912tI8+HoZjqI15
 ↪  TXvxlqzkX2zchdMed7SBltXDGHPEBPIf+Yt66hwqQ/2CyVjL/BGNAelohBj2vnAM3WYA/nuqs8zqg=
st13.os3.su.        3600        IN        DNSKEY        256 3 8
 ↪  AwEAAdYodQQ7EmyqB03dvx4Vrtg7ct5S6AG4DLePEVIUxTcb079BZNUF17Gvafvuxhw6S8tFpBIvVFNaRZSQzgAbFsfw07
 ↪  hHlP7n6WJoiYg4PwWkKh0qs2zt0STSWQupTxxgwaLY7C6IlDllFSi8J0bM0+TQYZgT/VGjgdKuxAUNjieD ;{id =
 ↪  18969 (zsk), size = 1024b}
st13.os3.su.        3600        IN        DNSKEY        257 3 8
 ↪  AwEAAcigr1cqhoUZzX1IoE4goc6XNQaX5mqYsHhzUqfar18qEPSblefB+B3zqR+GcX6W2bfpL40+vjudzQGDP9SodizXxm
 ↪  IRguSs+10YgMExPUCejNqvaAOxtUo+334LfJo8x9wu5ErWe5rKoeZpFYqAJENTQxSznWo2bFgUJnJJ91u142JOsJ5Tq2B3
 ↪  m9hGrKgXRLqcASHDntuvsFfQXhD3QNUdSNDn8l8urMQIdk+JTI4lvBsXery4BWS9ocvHvltY+ryo7dZzwBmniWEk88/Khn
 ↪  3PEcxN5QDJYQ45DIkLP7EAm7gPYWa2PqJb3lHLfdiXDye6+UjYbGY2laVtWIwv9vk= ;{id = 15514 (ksk), size =
 ↪  2048b}
st13.os3.su.        3600        IN        RRSIG        DNSKEY 8 3 3600 20171012110724 20170914110724
 ↪  15514 st13.os3.su. LknRzXDdHU7Ork5GIyOu/Igg+cspS252oR2GFS72Wh3515lBisd7+DJsi0tNBXgOBtvw4BWIRwo
 ↪  13vnEjFjBq8Sk64KO+wCwO38y+acRqLgZbYMydaG+IjuDLebnHFXwpcSq/7QaX8f+5FDdPdjzy+BB/B7TNjwEUu233nq8P
 ↪  plV6NZC8dSUpaGYDt6BH7YlTrY9rNDqdQAN+rf6kZ4DVSKO1Meie9AG1yEpCKE3DSVKdl1OzPhoqJ1lxD3rtQJvrzYHJ84
 ↪  IOlOnfxSvUgriyheaeKTnOFOjGUkB39orJOyxZxcUM/X1ikuzkqxyyf8xZzfT27yRs9S/wlo/aOlC1w==
st13.os3.su.        3600        IN        NSEC        info.st13.os3.su. A NS SOA MX RRSIG NSEC DNSKEY
st13.os3.su.        3600        IN        RRSIG        NSEC 8 3 3600 20171012110724 20170914110724
 ↪  18969 st13.os3.su.
 ↪  SZWZlK/duuE2Yf2E6kl4uiVh2DhIOf9NeRMKjC1KWyCoNyH2IgAlHrfQduIz4ifqQctEZ2TRAgCuAQik54zsPsJ3CrREZi
 ↪  xiWoQgkWdB68nlggIQSDeQFFFaonDT8l1idMLJlVJhcAYSUMuLWQEKjBkfA50vDj3LnDhddSEIZtY=
info.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
info.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171012110724
 ↪  20170914110724 18969 st13.os3.su.
 ↪  vxJWHRtxlKY/ee59wo9O64bQ49BOZnI2cG5X3LgRtsPUR2hOdGDVWxch33GFGoNcp3rQngu7UEVhevShqoJo0KeWYEEPQt
 ↪  QyMkxpxUH7xvVdV84ncCPoC88FzZnjwkKz7TWj/Sh4A7qgo/D+qwMbYZaNM3qLn8ufP+/LjxCGMc4=
```

```
info.st13.os3.su.        3600        IN        NSEC        mail1.st13.os3.su. CNAME RRSIG NSEC
info.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   BoKVlkfLE1WXFOAenaLrThxJVZIWy4x60qMDXaABGyAcwxvpWhxM6dmD7MgPRsGPlOezR+w1z1aFxj6bii7x+l181UY27W
 ↪   JlFgWw/XwycvFPOa6pRzvAAVL1sNe1nH7U6etZ8hHlXmk3O1KPLOZ7MgYzWiOqwddSO/ERL/k+YQE=
mail1.st13.os3.su.        3600        IN        A        188.130.155.46
mail1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   q4dsHfGJXwzd4wkNCYBaSrfYl6PUQGUCIDfl9pLRkbqR455R/dfnsTcGbwjMisQmpB3LgYvlJ4IDH6DQcL9U+eNgeA6jnr
 ↪   2dcGE5oVCt7zy12NO9OIpdE/1572qkRzknVSG5SNshC4Y2jqihpOifLCHV1vqv6S7w/ot1cT7GmJw=
mail1.st13.os3.su.        3600        IN        NSEC        mail2.st13.os3.su. A RRSIG NSEC
mail1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   aEsg41rB1cY4ByvFweuSzTTy/tlLmFV9AR8ji3pasBcYeZdpqppyINm1wtAi15nG7Wq5XKRWBOuFTtn+FabFt/vyANbj0t
 ↪   NEERKzxe/0h5zlqmXAom8iEyAgFkMNqb1j407d3jPO749ZYWiN21LWFy9LN3iUW4ZmwYHkA56Mo9M=
mail2.st13.os3.su.        3600        IN        A        188.130.155.46
mail2.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   OtulbCz/dV1BtUAAAUnQuyR5G9kQG4kdsjjFsK2Hh+prkfjFm4Pn42zUkZcUocb77RjiSEK9ViDie1a27lHtDyQW72eN7R
 ↪   vzNRNizKkIn991iOsmML1W5GUOvK3PM22OBSSsigf/+YsbCg4b1qsoAcn2dm/AVoDfFnPR1YA1wtw=
mail2.st13.os3.su.        3600        IN        NSEC        ns1.st13.os3.su. A RRSIG NSEC
mail2.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   Us0vOzaGRRut9pg6STC6cjnolW14VNTsAPIRJ+yW7ow8AON2eoQEQ9D+4V8bSFRF5Kyc8OV8KAslZ9gGWUENN9gws+W6sz
 ↪   NNzr/6C48303cJc3xOLXSWE7F/nyrLYr4eiClfXT4HHHQB3e8r0bYUHV87AKURAZFf6dstynNg144=
ns1.st13.os3.su.        3600        IN        A        188.130.155.46
ns1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171012110724 20170914110724
 ↪   18969 st13.os3.su.
 ↪   McQOjEWZyvZc0jM9/cFLrepKttkLqC1BUKOwtd8XwZW3mA5ca5byS7QsB4WtrzneqxiBxcGQVwbIzxMGlvSOLfhDPJIA8T
 ↪   hxxGKgklS7PuFOJdeiReKdZ525r/pVrOXNDbl5Gymu7hf1cs7+ug8frwMNdNlcOZvnTiWHZN7C4jk=
ns1.st13.os3.su.        3600        IN        NSEC        sub.st13.os3.su. A RRSIG NSEC
ns1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   CPojyAQdZk61gPU9/zW8qlCkhAIX8n99urEXJTKoIkghZwiBOEfqDrfcUQtMB6KOhZ2FtSrFt7ux2ZnPTmD/Zxn8/1JUPU
 ↪   4dayzWXBJq3uCirPTTtrtd+iElvioCOJzRmJfEZ4l1yjoEd3BokLr2orZJFMU7klX7JZIHcJQmww0=
sub.st13.os3.su.        3600        IN        A        188.130.155.45
sub.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171012110724 20170914110724
 ↪   18969 st13.os3.su.
 ↪   PlgrCOJH7QHW1q6Gcvm2I2qJDWDkTGhQJM5qypQxWmKIITcai0s+yyi1ZBaE179q0ZwcOcvZ4fYszjlnVElFBqltIfuC3Y
 ↪   ki6qzAHQVELgDjil5sOArp9bctieqpVSJLCTihEFYIMQl33OeW8Wmekn5CcI2M67IeWnsKUpuxvzY=
sub.st13.os3.su.        3600        IN        NSEC        www.st13.os3.su. A RRSIG NSEC
sub.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   LuoYC5Y4D3A3XUy1lhF4npAKDGW3WlhU+4esRbHmmvE8vBX7B4/VxAPhizgaKXsYpgNk7+MOTSFIFVOVlqu8uGt/kGYzNK
 ↪   E51P/PAbGlAkqL89S4dTeDw/UwpRtiJvDcSd+Jn2KymCc66sDbblmf9y9cxzsC10JuORi7YZoWT5M=
www.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
www.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   HpKltcDATmayq/Z8PQGkDYQSszBpiLcvnRzrFe7yZEj4AiQOMfTO4Pp22CsHB/4XF7jfL25DpCn/qU/HrEiK96xAyjVNbO
 ↪   ebwZ8LOOQyp6TjL2wN1dCiZRzoFlRQ+yX/mQrz+YXVwk9CIkYcdJ9NnC0EZ9NlNPes7k+XnkIbjfQ=
www.st13.os3.su.        3600        IN        NSEC        st13.os3.su. CNAME RRSIG NSEC
www.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171012110724
 ↪   20170914110724 18969 st13.os3.su.
 ↪   FBYjQtgh2Z5cxnpTict4xdDwUShg9j22cNBq37mhp/E2P9xccqsREfvaC+EMl6OdY/oDPZBvmuhRoFoxRscKKwa8jhMUgi
 ↪   5zql59YlXXmIwj7Zrie+tvTNwHETx0YZAB4WzrHiqL9qH0jRm1g7ZbmbPtq72gBynY12EMtzFvaZY=
```

How does it differ from the unsigned version? Any unexpected differences?

Answer:

New records (*DNSKEY*, *RRSIG*, *NSEC*) was added.

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

```
...
zone:
        name: "st13.os3.su"
        zonefile: "st13.os3.su.zone.signed"
...
```

Restart the authoritative server and look at the syslog for errors. If the server appears to be up and running, test DNSSEC by querying your server for the DNSKEY of **st13.os3.su**.

```
$ dig st13.os3.su dnskey @8.8.8.8

; <<>> DiG 9.10.3-P4-Ubuntu <<>> st13.os3.su dnskey @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1625
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;st13.os3.su.                   IN      DNSKEY

;; ANSWER SECTION:
st13.os3.su.            3592    IN      DNSKEY  256 3 8
 ↪  AwEAAdYodQQ7EmyqB03dvx4Vrtg7ct5S6AG4DLePEVIUxTcb079BZNUF
 ↪  17Gvafvuxhw6S8tFpBIvVFNaRZSQzgAbFsfw07hHlP7n6WJoiYg4PwWk
 ↪  Kh0qs2zt0STSWQupTxxgwaLY7C6IlDllFSi8J0bM0+TQYZgT/VGjgdKu xAUNjieD
st13.os3.su.            3592    IN      DNSKEY  257 3 8
 ↪  AwEAAcigr1cqhoUZzX1IoE4goc6XNQaX5mqYsHhzUqfar18qEPSblefB
 ↪  +B3zqR+GcX6W2bfpL40+vjudzQGDP9SodizXxmIRguSs+10YgMExPUCe
 ↪  jNqvaAOxtUo+334LfJo8x9wu5ErWe5rKoeZpFYqAJENTQxSznWo2bFgU
 ↪  JnJJ91u142J0sJ5Tq2B3m9hGrKgXRLqcASHDntuvsFfQXhD3QNUdSNDn
 ↪  8l8urMQIdk+JTI4lvBsXery4BWS9ocvHvltY+ryo7dZzwBmniWEk88/K
 ↪  hn3PEcxN5QDJYQ45DIkLP7EAm7gPYWa2PqJb3lHLfdiXDye6+UjYbGY2 laVtWIwv9vk=

;; Query time: 91 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Sep 14 14:32:33 MSK 2017
;; MSG SIZE  rcvd: 464
```

In order to create a chain of trust, you have to make the right DS record known to your TA, the OS3 system administrator.

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

    Answer:

    The DS record of public KSK should be sent. It allows the transfer of trust from a parent zone to a child zone.

    DS record

    ```
    $ cat Kst13.os3.su.+008+15514.ds
    st13.os3.su.        IN      DS      15514 8 2
     ↪  2f2f6eae52c26623c95c485bb0e343abd0d88cfb8f379752066c54c4c7459336
    ```

what is the DS record?

A **D**elegation of **S**igning (**DS**) record contains a hash of a public KSK record

Once zone administrator has implemented your DS record, use a DNSSEC debugger to examine the chain of trust, see http://dnssec-debugger.verisignlabs.com/ or http://dnsviz.net/.

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

Answer: Figure 4

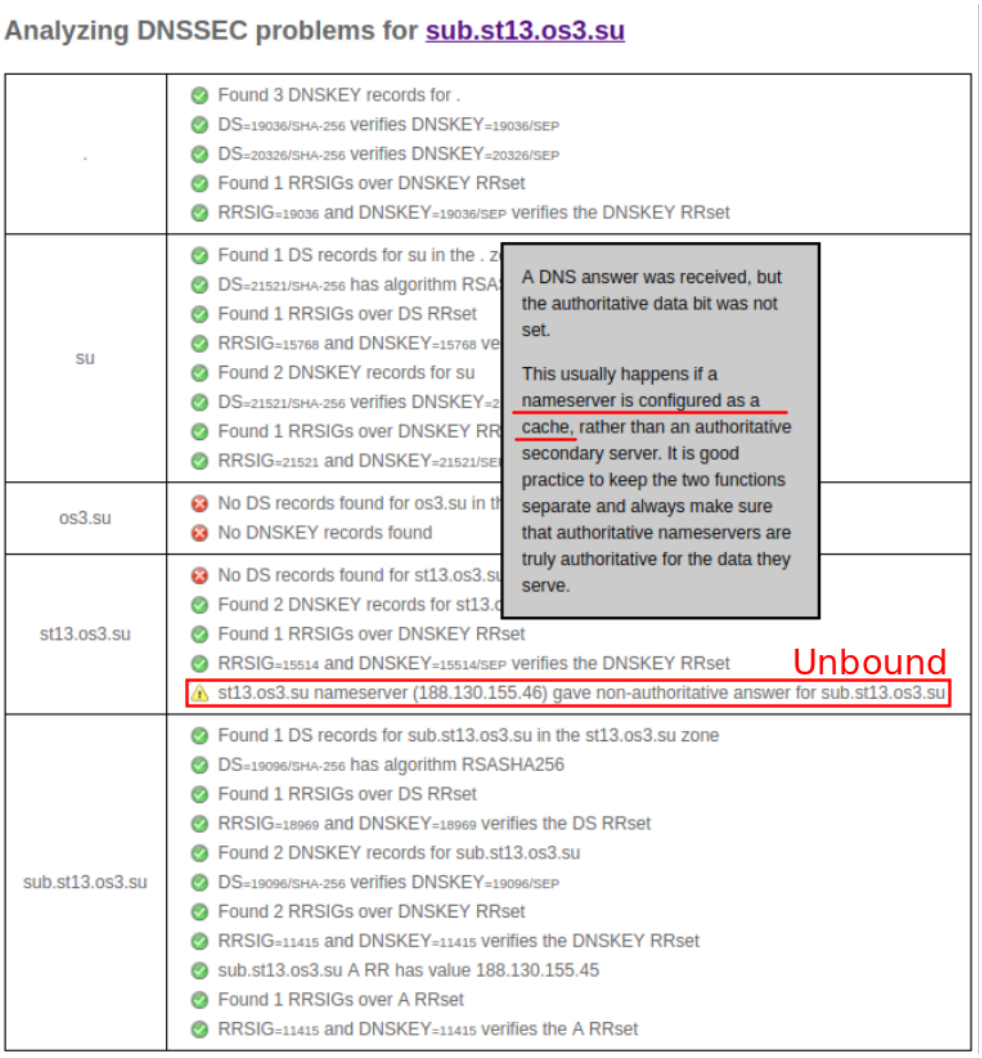

Figure 4: DNSSEC debugger

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

Answer:

The parent's DS record is required for the child zone since it contains a hash of child's public KSK that serves to validate the child's public ZSK.

not full answer, also DS RRSIG, DNSKEY RRSIG should be present

The parent zone os3.su contains the following important records for my domain: **ZSK** from the **DNSKEYset** to validate **RRSIG(RRset)** including **RRSIG(DSset)**; **KSK** from the same **DNSKEYset** to validate **RRSIG(DNSKEYset)**, and **DS** record to validate **KSK**

4 Key Rollovers

At some point it may be necessary to change one or more of your keys that you use for DNSSEC. Fortunately, there is a document that describes some possibilities for this process: RFC 6781 [7].

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.

    Answer:

    The two most common rollover methods for ZSKs are Double-Signature and Pre-Publication. Pre-Publication minimizes the number of signatures over the RRsets in the zone and DNS responses. Double-Signature is the fastest way to roll a ZSK without prior planning. It is preferable to use a Pre-Publication method since this method is best used in case of a key compromise, but Unbound+NSD's tools do not allow to set keys lifetime. Therefore, for Unbound+NSD, it is preferable to use the Double-Signature method.

> Pros and Cons?

> **Pros:** Double-Signature is conceptually the simplest and fastest way to roll a ZSK without prior planning. **Cons:** It suffers from increasing the size of the zone and the size of responses.

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

    Answer:

    The new ZSK's DNSKEY needs to be Known and Safe before old ZSK's DNSKEY can be removed. First, all Validation Components of the new key need to be introduced into the zone. Once all have been propagated, all information of old key can be withdrawn from the zone.

    New ZSK is generated at the generate time using **ldns-keygen** tool. New key is added to the DNSKEY RRset and is immediately used to sign the zone using **ldns-signzone** tool. Existing signatures in the zone are maintained. The information for new key must be published long enough to ensure that the information have reached all validators that may have RRsets from this zone cached. When the new key is said to be propagated, old key can be retired. From the perspective of the authoritative server, the rollover is complete.

    (c) Which timers are important for this procedure?

    Answer:

    - Generation Stage
    - Transition Stage
    - Transited Stage
    - Withdrawal Stage
    - Complete Stage

Please don't foget about TTL and its dependencies.

When you introduce the new key and new signatures, you need to wait for approximately one TTL then remove the old key and old signatures.

(d) Implement the procedure and use a DNSSEC debugger to verify each step.

Generation Stage:

```
$ sudo -u nsd ldns-keygen -a RSASHA256 -b 1024 -r /dev/urandom
 ↪  st13.os3.su
Kst13.os3.su.+008+36381
```

Transition Stage:

```
$ sudo -u nsd ldns-signzone st13.os3.su.zone Kst13.os3.su.+008+15514 Kst13.os3.su.+008+18969 Kst13.os3.su.+008+36381
$ cat st13.os3.su.zone.signed
st13.os3.su.        3600        IN        SOA        ns1.st13.os3.su. vkaser.st13.os3.su. 2017090603 86400 7200 2419200 3600
st13.os3.su.        3600        IN        RRSIG        SOA 8 3 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    TKh5ZuKOEmNJAb+jdtq3yEqvAQbDETKEtObgUyKa/t40cpx2N5RO3T4MjP4evoBkG3xr1bU4Yb52n3202AHgvE+UoRc9xxf815XYuZrEm0wtFgtuvOGMvN
 ↪    BFABSSTmIlxNW149bGB8RCNDHYQf9cLKeVOqmBogWMEYRXhtz7/Zo=
st13.os3.su.        3600        IN        RRSIG        SOA 8 3 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    iV91i3aWtrz0wGvxsvT73UTn5EjRXr2xydznlBm69NE2Qe9GANMlfZPqawe348Jj3Fi7o+ECuUHpO+qHS3dCOKWrQfr++EfO1heSR6/ZQLvk2mle3Va6J1
 ↪    XEtVma5+im15CXy0INogAbkiqrbv0qIja3L9PCfxK+TXvNFbrkUYM=
st13.os3.su.        3600        IN        A        188.130.155.46
st13.os3.su.        3600        IN        RRSIG        A 8 3 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    wojgclGsAPrtDE7OE5UMeNlOZZTDucDl+xrZuhLAr3n85V7EpkpAnrWMpExJPZv+jogPrq5uuOLWh2/oMmxLksiaahU2ggNmiIrPPclZYQHX22NGTvV6UK
 ↪    tx7Kub2ocAt95ReHpDd9DYGzfsNrPSNs2LRBGUtyjhgpqOC8a5rtO=
st13.os3.su.        3600        IN        RRSIG        A 8 3 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    RmQnBhOdnSgVeY9Mp6FpyABldFjnuabQMuZaORAr7xjQ3VVw8ekAO8Y9NBi7wMxF+apFTHS2VS8CLug5qQFhrEobCn8uuFdETG/jSsOeUIGIP+zvobykl5
 ↪    ZW642/3RMEtuPcND2d3PE+CQR7L8AK5FmWD482eYJWrnMsMKFAbCA=
st13.os3.su.        3600        IN        NS        ns1.st13.os3.su.
st13.os3.su.        3600        IN        NS        sub.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        NS 8 3 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    br8w51SOykVQdWWzFYIXKyOfpjDcuA3ghrH1grBTs8yyqNXToCtUv7md5HNKHh4wGDvXABDy4kxuedIfgl8fB+F8GjinSPJry1F/aQ7CxwZBREe4KE9Dz4
 ↪    EikSpWFeVJPLruOwIfhwLxbOS1lcssIhE7HsFc3hDK5ihYcUBm/RU=
st13.os3.su.        3600        IN        RRSIG        NS 8 3 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    rPEwBp51+Srsv45KCp3y5QqFs6FnwqwijyxQpwNFi6ytpXrKf1MWmsa34XtPTOwtNzjkwIzNnol3RHgCALCs8iRlFFX2etsntvErAyqz8jBdXeRBs7kVGg
 ↪    jgHhD9L70a93fUvniRu/ViLHKDP7RYFW1cYqJ39j4DOWT3imwtZf4=
st13.os3.su.        3600        IN        MX        10 mail1.st13.os3.su.
st13.os3.su.        3600        IN        MX        50 mail2.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        MX 8 3 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    f46DkLpSXaN6QT6C3SECW5OhwrkuAvmnHZMcw5IH4rctLAw60C1Jfimz6x6wf029pUXKTcs5pxj4IrvWyMVzoPp+U2/6gEB7zKX3L/2sgFBQGdv1W4TzEO
 ↪    spDvSETk2OXpsZSX/90VP7NtOXEmmFNROkXY1JkNiVfhvuvHqA3p4=
st13.os3.su.        3600        IN        RRSIG        MX 8 3 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    pQGpogiA47ADofVyQ+4yPxlRlFMO8hkm8pSk6UliZV4sv4eCcFRAhJBvDy08q8a0OhYm4/4tOntb3XX6zvqwq+UbnixPnvJPKn4yxB3tq7YJkmut36uNeK
 ↪    rG+LFWTX7StyHYF+GGn8qsWwxejj7CtA4cMGtl7RHs6/2HqFEa/44=
st13.os3.su.        3600        IN        DNSKEY        256 3 8 AwEAAdYodQQ7EmyqBO3dvx4Vrtg7ct5S6AG4DLePEVIUxTcb079BZNUF17Gvaf
 ↪    vuxhw6S8tFpBIvVFNaRZSQzgAbFsfw07hHlP7n6WJoiYg4PwWkKh0qs2ztOSTSWQupTxxgwaLY7C6IlDllFSi8JObMO+TQYZgT/VGjgdKuxAUNjieD
 ↪    ;{id = 18969 (zsk), size = 1024b}
st13.os3.su.        3600        IN        DNSKEY        256 3 8 AwEAAeBrjBtYAor85DStGUOs7u1tJgGF9QHaYyBYCIgb/oBo6WsIhAX2iWLBOg
 ↪    Eo/dHALSDDJoaSWN+6SsyIei+RPUHMGYAGwTHkDFzEaVrmal6RqS9xIaQB5l1bBzMmOdub4qL9TW1UkjzEO21t8JSR+Xk1xCDroeMu/86oPKtHxzIl
 ↪    ;{id = 36381 (zsk), size = 1024b}
st13.os3.su.        3600        IN        DNSKEY        257 3 8
 ↪    AwEAAcigr1cqhoUZzX1IoE4goc6XNQaX5mqYsHhzUqfar18qEPSblefB+B3zqR+GcX6W2bfpL40+vjudzQGDP9SodizXxmIRguSs+1OYgMExPUCejNqvaA
 ↪    OxtUo+334LfJo8x9wu5ErWe5rKoeZpFYqAJENTQxSznWo2bFgUJnJJ91u142J0sJ5Tq2B3m9hGrKgXRLqcASHDntuvsFfQXhD3QNUdSNDn8l8urMQIdk+J
 ↪    TI4lvBsXery4BWS9ocvHvltY+ryo7dZzwBmniWEk88/Khn3PEcxN5QDJYQ45DIkLP7EAm7gPYWa2PqJb3lHLfdiXDye6+UjYbGY2laVtWIwv9vk= ;{id
 ↪    = 15514 (ksk), size = 2048b}
st13.os3.su.        3600        IN        RRSIG        DNSKEY 8 3 3600 20171013055835 20170915055835 15514 st13.os3.su.
 ↪    Sual2EvJK3FrToswYbw9zH19zMGUgOCoYNMUv8KgSyqAxw6/3MPNooZ3MZHO8GUJ2+WML6rYDH1h8yOsmG4ufK88qkbiEWNduVHmkMnUubddOtItVfZiUt
 ↪    ui+211qI46GqPX2Iimb/S1KU8y8qbKnyI3KkUSLcWaQZqeT9Eu1f+tjxr8JiezC9vAn3OnsgrhCeFXJVAhRlrnczx7H2dLfnSjXWnSpTz8aHetp8tUl5+Y
 ↪    CBSDJWrGTJGlkA9r6U1bzZwtKiLDoxUVfdmsZOAmFm1LZE98GaV3FkwzdpMHIYrZzxCKdDfu3esGPTBGD8dNiSfQeHCZLMzKiFXk2hKOYQ==
st13.os3.su.        3600        IN        NSEC        info.st13.os3.su. A NS SOA MX RRSIG NSEC DNSKEY
st13.os3.su.        3600        IN        RRSIG        NSEC 8 3 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    nZzefqLEvONzc6Pj+1AD8IcqQOUIOPj1bpvvMjb3/lR13ibNrJUDuRWFguazzkF/wMhtpaYeweDh9D1OhVzSdb8KPOzCbA6qhQ53sjnNvkdVFgO+GG1G+Q
 ↪    I6gLxLWMdcJxOJSGb/e3DG3FruZM3WB+ObdO+1/zK+ChB+OByw944=
st13.os3.su.        3600        IN        RRSIG        NSEC 8 3 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    bFudwccRAx73aog2I9B2B8WCS4I1zy/JBqhMJ1ltBbIcgANA7/AyuVpJojjp2+cH++oLYVBZ1dnIOf+bPHiPFpOiLcG9YCgNA4MCOwNKriPk8jY4yOMpWq
 ↪    YjL5S/C6QEpZjV75TQZrWq4Zb68cfwfIoMn1VyOvyS8TSx1NN5hTY=
info.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
info.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    eQgq7ypvSfkltLFN3etXnzuOKoi5Gdy0kxauLcfdJs0DbtFoGd/dV8cb5DAO6eMrxsHzMQHQIxuKeZMmkWR/XXCsxmQGd9ncG49Rhuu5Kb90k6HNA2VulV
 ↪    dtgKtfNPS7ioaNe5wuRsq3fJ4Ao/z432Ob9adwuoOko3S/Gpq4nDE=
info.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    l6zVVkQe/UOrAR3h4xtfOB7RbQhHVfitlQCeTK7ddrzxMK1/JW7A4XK4mjmdmvfaWx1VKQ6Usy6/Hmdjiw46i+zEtEyeHsgmSQBGVGmXd3tShGVuYxRVZm
 ↪    ZNNd3UO2g3ET6TvJ8DWdyNqAKbTGAsgGQ923e+pFMqnoEjMjRgO/M=
info.st13.os3.su.        3600        IN        NSEC        mail1.st13.os3.su. CNAME RRSIG NSEC
info.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪    TrVjAuyJvY98KE5TMLxKfyU4n6E+wIEkOUPJOWO9nH2eOI8n1EqwH/BoSraafxEmlXBDevvXfl0MJ+OAwlwM6f0zvyPd2p52ITtpC6cErfFhCNFif4zsXf
 ↪    GFgZzAqNFMJ1hdVg5qegxjZplsIOxDWYZGQ2svK4DF5C+xc13uzeE=
info.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪    m0cpxej3OCR820xWf+6Ci/w8wkuue03iEC3qUWKXlrRIUJ4QdCtQOOHOhqLuvdW97coxRji4pHNiMU7ZlR+zAQSrOL7ixMnW9ItV8j5n4qEAVDBQT+K3tk
 ↪    IJfXv8YkqIXYajMSS4t4YVi6JODlf2cBgCCQH2IiITq8pSazd8QVU=
```

```
mail1.st13.os3.su.        3600        IN        A        188.130.155.46
mail1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     HZd+aPQWTMHn66rTqIqAyW3WAZwekzzuHn8W2GIXZRCERxAcdahBoPBJfHXi9ag3dhp/ISlvn5A4LqztGw0G6J1M9ligDZO9OBUPqHsO8jceJimeqI1RDU
 ↪     SZxoMCQZ95mKyBR+WKjXdjmT/qZz34e8eFkOmLA05cQ6wLGKt4qZk=
mail1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     w5gAhIs2AnJzspT7zOSdZyBaiGc3/OSwVTA1JgxGDQgCXSdHr72yGipxLBmsOUMiBkBt0IWG3wNj1jzqVQLMLIdfINYgZrGgpLtJeyNHRH+aQtF04/GeWc
 ↪     IZQeC5Zxdbm0lbvEObi5ikq/rBOioNf9WprRdEDfp5/yN8fdSCWS4=
mail1.st13.os3.su.        3600        IN        NSEC        mail2.st13.os3.su. A RRSIG NSEC
mail1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     Qt7EmRJA18ENTywBswU/GZVxxKcWi2qisnqRs7qPgFmwBI73RU4BPs8D9FkQG9G9VXsFxzIcJjo9AfE5zTlcv2vqs8GdKRH580qeSMK4BXBBu6cXyX67Bi
 ↪     BA+uiP4fBak+wlwngYICSoNOFUOK1oTICwbWymXVMl+4kkHcSGmp0=
mail1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     k0ZJYMpuG24puSU8gA116X9mmdEWk1kWenXtxhvjsDALZXjV6aTU/WZ1PqY2U91YO3pKWTTqe1A5x9eWygWddRyfDC2KUAnD6SQvKrExfet/xBT+czTaJl
 ↪     gmQsFifiBrppjlkpjTh1oW0BWZ3M8lMuD3P5FMAXd0apoecrf7DIQ=
mail2.st13.os3.su.        3600        IN        A        188.130.155.46
mail2.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     KVJU7R+uaWm32Ed7nTkBVL7YuY+zyvHsXnGrcLr4rYEDAgnho6VPMbFXRsJI+BPc47qkDVbbsXWmRnkQHCqDh80439hOoE1zppyvsWInrdR8modoRM2qYJ
 ↪     MqlaDO06Pv9ZAuUxtYkF2VJ3Dc6aCdXCBV/Gk5a6lROF9OtLohOS8=
mail2.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     xlWMQUvXI4rqXOVensWgK8CpmGw4vELcihNSqlLnABORSAnQL1OtyOZOQ6caN3heVrL6Mp433AUN9Aya1OK+uswnTTdeXarun1imoxNo2SDtc54KxV2RQy
 ↪     YGMEhGJ33GDr+ogyDJFCtWLSIRQpC3NcJc78LC2do7EDXtKwe+oBQ=
mail2.st13.os3.su.        3600        IN        NSEC        ns1.st13.os3.su. A RRSIG NSEC
mail2.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     o+do5q9yiKnyB1uhixomSUzzb7Ti2TceciZpYbUuHrZQ15lltNZzMEo6WOTiW2vzk+htPXgLsYKZ3dsNNA16PEXTG4N4M5HVL7BDJJAsPLhiA/XufFA6XP
 ↪     OSoR2wnrDqVlO6uNwGkRdQdUNFZ9L6MlRtGPqw4HCf8l2Hg/QDEUI=
mail2.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     N9od+O8TQd63MJGchZi9Salo4b9WukNEZPuaFgNk5pFOaHGInbV2WAm5UKb2gOMpGQ1ODes2F/4qD+jMFyNr7IydfUQS8HwZnlGuIpzHJS4QlvDdyXSyoD
 ↪     DyE9KRUWALmqaYeSFIr81IsuGlgqNv3nvv/Lq424qocVzeErZTbaM=
ns1.st13.os3.su.        3600        IN        A        188.130.155.46
ns1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     eaeQ14lZZsc6XJFsTlRGOviuq555udBSYWV2Dbkz2u6yZsGqDHF1vAbkjVZHj+WSOBijHhMKgPwcVmLqvpit3f5M9pDcJyUgdLkiyDEUZwXBaOjY9n1U7R
 ↪     r8HEMiSoiT59rlEUuvfJNO+kPDfrrVqAOPNANL1vndpno0GsJj2DE=
ns1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     qSAdvBb4qEpudsjEvhhLQ5x3/eHTVq3hkaRcmHGB+2bBR7A7Gek/Vwuhsx1Vr87QiNz7OrUqxEIfpFEgUGKFb3e2PRVjj3Dr/vQMoyetR8zlRwzIPJFU2H
 ↪     ioou9MwkCfFOYF/qvpqvOWzLaHHTvN2XLbpDaxdAEp66H48f26oQU=
ns1.st13.os3.su.        3600        IN        NSEC        sub.st13.os3.su. A RRSIG NSEC
ns1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     s+fpgOPRcf+EhNKx7Gf1WUuc55n8re4BwqqEyyUk2S5uJYMvWOIdEeyhyDcG5/9f7QnpXekfRwf93Si7d2QMmg6CmSuSYXr/NK71IypLQdrxCutOXiRLsD
 ↪     vgGZq+d1PhRSWT39EjeP9w+Wgy7qNno1/gHWiJ631Z6fmLsOLuF2E=
ns1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     vtCoUR5eo8upAI97tYa433+Zo2A6Vqd7PHzibxjU2W9GAXgCrYu/tBdro1Jg5LDaWSHUWycFgdy49kVjtJ+TVZ1rJr9vzA0cf5EYOIM4CX+RBMsRnpg/Ab
 ↪     5cLRANWt3sCM2+dnzAeqnzW+Y1/y/aHPmOI7cJNvviceOF82KRdKE=
sub.st13.os3.su.        3600        IN        A        188.130.155.45
sub.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     wqfTJJeI8Z+k+wLwvrMwNB7FEZbLIfbZSSGNSuMPYKLT6HFzS3uq7/RNQHFSA3LW7d5HOBLsEr7+KyKveLuJFk9S+iuD/lFMtz2tcdK1/OhVE13lYuY9+I
 ↪     OYzoZ0PLfclGAVVkTd52xMCtFvaH7zynfrPJKIKp95IustfW9LU50=
sub.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     OROtXlrQqCG+2scrCAmN3LGVOUwUC7xZhqopztGLzdOOtAehpEqpl0dj/TwQKOZSUVSaUNXdFKIJi7RWcbLHSrD2PCxjWfbVTVaEJAjfqrLqDjNhxefN8l
 ↪     c2iFF/yWgtooOcrQJ/tGO4L/EA+9ErOm9C63wwAPg5spTz1MRDaAc=
sub.st13.os3.su.        3600        IN        DS        19096 8 2
 ↪     85bc7d653e3fb6c18e1f37cfb9bfd543ac3d5da2dfa7a3f00705e5c1fc53c8fa
sub.st13.os3.su.        3600        IN        RRSIG        DS 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     RAhOCH3dYo2g08cv75xtMsyYbLo5D6RhG3FKlC5YyjC/hIg32dlgD3zpo/5BwK/oygiXgcy3tNnwofDR+LCNsfzGbNv5OHOu38TtY3ZazMYriVT3NLvd0t
 ↪     R+5PJz1/0onRojvIlAUEhKbCt21Ppk/S1KPgQ4ik1+qPvqFLDGlzM=
sub.st13.os3.su.        3600        IN        RRSIG        DS 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     nlsaZxrWaEXSJyTdyLfV4xvebkYsz0IJqxQvU7FACUmf9+5GpAtIBEWGzO/aQtOuy2PxrJO8SscOjzuqP4fzw11PfyAShFk/lDD6yLA+Qo42YZh+MoAh4i
 ↪     IDzXM1WEXODgfWOFhQxWZQbsX7bNpIha75qSbOxOXrz7dH3IQQprA=
sub.st13.os3.su.        3600        IN        NSEC        www.st13.os3.su. A DS RRSIG NSEC
sub.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     H5rwVLh0QitYT5i/yl+C8xdHjB8a2r4cSbvRzobHWVUTNUgYOriFh2VMhldGOVs0dvlPUkmBLbFPKhLYL5OQl0rGFRxbrDndQ/O1culb6SUTrbIw9QBcD9
 ↪     0sv569uoXhxBqxXe8XgwnnX6v4wHW+7U+X2uxrVnWDCo2DMPcJ8YO=
sub.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     FDboA7CJXljvzu5gumOFctXz8amneiO1yS26PQ8fkwfF95qTb+JtTeOXJCMOqpBE/nDCL12s7wdrkQtmnylWAaSSfMQ96nocHsGveIPbpWk0RkOLStTAQ7
 ↪     woegYRHGBkurQdXupi6m0mkMElpwT7VUpzWlns8xETN8F9vItNiLI=
www.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
www.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     UY/6mlvKN2HJYWvJjna7kNjonBApcho5vYZjSvMFfAcpsJOqtXXXj4rxX2ePDtNTZoKctprUsZk8moe7i6syNmsZ87jilFw423ejfFX/Eh3Wv4Q0I3H2ZJ
 ↪     az3xY024WCilRLsOHa1NhqhFkHGhE1dG9ceKOZBLs/R7eHSKljAtO=
www.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     1mlsNh6i8+dMNM7BOcmqOofo6mTKbVoMhUQvr9GVJwA6kEdf1PZMwghYladHODxhl1ietFO+4asBN1FcQZnOnVb9Og3gEUICIhMOv5nFQDQCd3Wg//hGkz
 ↪     2eHvBFNfmMzHphQYQxDRpYnTZhZ4DIU7O9tw7TgztGLRVhboTSLII=
www.st13.os3.su.        3600        IN        NSEC        st13.os3.su. CNAME RRSIG NSEC
www.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 18969 st13.os3.su.
 ↪     w2Mm++QqnzjoMON766B12K8N/OOJcJzt2hhXzoSaEjtkHYunIc/XSLkFTmx2cSmKDn1n19Bt0wUPQWIk9vc3iQUEvwR+OcEqFNumjQxwKh3LcpbmjaBmsZ
 ↪     9fBFNxVgAecKjT5mJAduNXJgZamXBkjzstzMJK9MugPzAdnmjlv74=
www.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013055835 20170915055835 36381 st13.os3.su.
 ↪     UlQYoIY03I4ujgvvRSOc3SptvCVwKjQ8+Bpp7ITiq9bC8aXZBxOEsSvOqJQ5Sh8jA/mWqFCP4jvi4vkNRP8ONKQ9T+LY1a6WfbJ/HNj2bDQEPs/liWe7+y
 ↪     EP7Aaf+3BifZLAF2mc+tgjMXd1wzjR4CJpUcgeA4I1x54q2Mr+Au0=
```

Transited Stage:

```
$ dig st13.os3.su dnskey @8.8.8.8 +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> st13.os3.su dnskey @8.8.8.8 +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33493
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;st13.os3.su.                   IN        DNSKEY
```

```
;; ANSWER SECTION:
st13.os3.su.                3306        IN        DNSKEY        256 3 8
 ↪    AwEAAdYodQQ7EmyqB03dvx4Vrtg7ct5S6AG4DLePEVIUxTcb079BZNUF 17Gvafvuxhw6S8tFpBIvVFNaRZSQzgAbFsfw07hHlP7n6WJoiYg4PwWk
 ↪    KhOqs2zt0STSWQupTxxgwaLY7C6IlDllFSi8JObMO+TQYZgT/VGjgdKu xAUNjieD
st13.os3.su.                3306        IN        DNSKEY        256 3 8
 ↪    AwEAAeBrjBtYAor85DStGUOs7u1tJgGF9QHaYyBYCIgb/oBo6WsIhAX2 iWLBOgEo/dHALSDDJoaSWN+6SsyIei+RPUHMGYAGwTHkDFzEaVrmal6R
 ↪    qS9xIaQB5l1bBzMmOdub4qL9TW1UkjzEO21t8JSR+Xk1xCDroeMu/86o PKtHxzIl
st13.os3.su.                3306        IN        DNSKEY        257 3 8
 ↪    AwEAAcigr1cqhoUZzX1IoE4goc6XNQaX5mqYsHhzUqfar18qEPSblefB +B3zqR+GcX6W2bfpL4O+vjudzQGDP9SodizXxmIRguSs+10YgMExPUCe
 ↪    jNqvaAOxtUo+334LfJo8x9wu5ErWe5rKoeZpFYqAJENTQxSznWo2bFgU JnJJ91u142JOsJ5Tq2B3m9hGrKgXRLqcASHDntuvsFfQXhD3QNUdSNDn
 ↪    8l8urMQIdk+JTI4lvBsXery4BWS9ocvHvltY+ryo7dZzwBmniWEk88/K hn3PEcxN5QDJYQ45DIkLP7EAm7gPYWa2PqJb3lHLfdiXDye6+UjYbGY2
 ↪    laVtWIwv9vk=
st13.os3.su.                3306        IN        RRSIG         DNSKEY 8 3 3600 20171013055835 20170915055835 15514
 ↪    st13.os3.su. Sual2EvJK3FrToswYbw9zH19zMGUg0CoYNMUv8KgSyqAxw6/3MPNooZ3
 ↪    MZH08GUJ2+WML6rYDH1h8yOsmG4ufK88qkbiEWNduVHmkMnUubdd0tIt VfZiUtui+211qI46GqPX2Iimb/S1KU8y8qbKnyI3KkUSLcWaQZqeT9Eu
 ↪    1f+tjxr8JiezC9vAn3OnsgrhCeFXJVAhRlrnczx7H2dLfnSjXWnSpTz8 aHetp8tUl5+YCBSDJWrGTJGlkA9r6U1bzZwtKiLDoxUVfdmsZ0AmFm1L
 ↪    ZE98GaV3FkwzdpMHIYrZzxCKdDfu3esGPTBGD8dNiSfQeHCZLMzKiFXk 2hKOYQ==

;; Query time: 81 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Sep 15 09:17:08 MSK 2017
;; MSG SIZE  rcvd: 911
```

The result of the Transited Stage is in the Figure 5

Domain Name: st13.os3.su Detail: more(+) / less(-)

Analyzing DNSSEC problems for st13.os3.su

.	✓ Found 3 DNSKEY records for . ✓ DS=19036/SHA-256 verifies DNSKEY=19036/SEP ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
su	✓ Found 1 DS records for su in the . zone ✓ DS=21521/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=15768 and DNSKEY=15768 verifies the DS RRset ✓ Found 2 DNSKEY records for su ✓ DS=21521/SHA-256 verifies DNSKEY=21521/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=21521 and DNSKEY=21521/SEP verifies the DNSKEY RRset
os3.su	✗ No DS records found for os3.su in the su zone ✗ No DNSKEY records found
st13.os3.su	✗ No DS records found for st13.os3.su in the os3.su zone ✓ Found 3 DNSKEY records for st13.os3.su ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=15514 and DNSKEY=15514/SEP verifies the DNSKEY RRset ✓ st13.os3.su A RR has value 188.130.155.46 ✓ Found 2 RRSIGs over A RRset ✓ RRSIG=18969 and DNSKEY=18969 verifies the A RRset

Figure 5: Transited Stage

Withdrawal Stage:

```
$ sudo -u nsd ldns-signzone st13.os3.su.zone Kst13.os3.su.+008+15514 Kst13.os3.su.+008+36381
$ cat st13.os3.su.zone.signed
st13.os3.su.        3600        IN        SOA        ns1.st13.os3.su. vkaser.st13.os3.su. 2017090603 86400 7200 2419200 3600
```

```
st13.os3.su.        3600        IN        RRSIG        SOA 8 3 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    utNB3QFDLz62CMB9y+SA4fYKs48t0CZcJYiwCcEGTBF3Ag0b9I1jU5/t4hYv5uYpZ5ySYkuMlnKSBySgnW3EyhxrN3ko9oZA/i7/tb4EIs26qil0MOScOP
 ↪    U14Y04G8mNVcvFCxOPzLAw8H8B2nuOO66RnX/VKVIEekOhbUqkoLM=
st13.os3.su.        3600        IN        A        188.130.155.46
st13.os3.su.        3600        IN        RRSIG        A 8 3 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    fZT5WWXb9nNQJEjfJBjTHKqCS43zyiBVjc3eXvfvMAaC6Hq7knn1ISurZH2OkQGwA/GHf3BcfdEa+gVp1JLPMBiKP9y7kfPOajOPeFkqRN6hXXEfvDZX45
 ↪    kAb3JoXDduwYTGYufIUfBu9VbJAhgAmtx9l8yUjNbt2V5m5j2KegQ=
st13.os3.su.        3600        IN        NS        ns1.st13.os3.su.
st13.os3.su.        3600        IN        NS        sub.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        NS 8 3 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    fwXAT8D2QMrPHe3WJP7l12tW4r/raluMvAURqcNIaa7gjJ6QujQIecVo9ut+NkxpSNdQtggkcgrix/0+WlNOsOWj8xOwrnGvF2SDLHr/A1MIs/6bHscOVP
 ↪    raUJPx05H2NLjLQGLDEAazxZvi/9wQa1lS9qaOUPxDv4e2YYHlljO=
st13.os3.su.        3600        IN        MX        10 mail1.st13.os3.su.
st13.os3.su.        3600        IN        MX        50 mail2.st13.os3.su.
st13.os3.su.        3600        IN        RRSIG        MX 8 3 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    w80dXAE96V+QTafE8RHbJMlbNOdBFMZ2jrY7Ht9Bvic8kCYIOckLWTwNFztZq5/AwRNPULnXxOhMeVgigreNZSowiehKFNGUpBnN9VqeuyRMo2rm2XCBVH
 ↪    s0Yk/uRdQhng77VwpaHffeIscY/DzOZoT/1osiABP9hA5dCe7/yzo=
st13.os3.su.        3600        IN        DNSKEY        256 3 8 AwEAAeBrjBtYAor85DStGUOs7u1tJgGF9QHaYyBYCIgb/oBo6WsIhAX2iWLBOg
 ↪    Eo/dHALSDDJoaSWN+6SsyIei+RPUHMGYAGwTHkDFzEaVrmal6RqS9xIaQB5l1bBzMmOdub4qL9TW1UkjzEO21t8JSR+Xk1xCDroeMu/86oPKtHxzIl
 ↪    ;{id = 36381 (zsk), size = 1024b}
st13.os3.su.        3600        IN        DNSKEY        257 3 8
 ↪    AwEAAcigr1cqhoUZzX1IoE4goc6XNQaX5mqYsHhzUqfar18qEPSblefB+B3zqR+GcX6W2bfpL40+vjudzQGDP9SodizXxmIRguSs+10YgMExPUCejNqvaA
 ↪    0xtUo+334LfJo8x9wu5ErWe5rKoeZpFYqAJENTQxSznWo2bFgUJnJJ91u142J0sJ5Tq2B3m9hGrKgXRLqcASHDntuvsFfQXhD3QNUdSNDn8l8urMQIdk+J
 ↪    TI4lvBsXery4BWS9ocvHvltY+ryo7dZzwBmniWEk88/Khn3PEcxN5QDJYQ45DIkLP7EAm7gPYWa2PqJb3lHLfdiXDye6+UjYbGY2laVtWIwv9vk= ;{id
 ↪    = 15514 (ksk), size = 2048b}
st13.os3.su.        3600        IN        RRSIG        DNSKEY 8 3 3600 20171013113943 20170915113943 15514 st13.os3.su.
 ↪    UEar5TWeeMEHHAuRO5Ea9rRvB+5oBejgFDVa+eweMIRRwZyhJDMBGPRIdWN3zJjyBrGjkeJuiuUsdowxwG5BHQsfdbNkZsl3QlEC/nMP+9shHOQRURLmS5
 ↪    Kzu9W4GiqcRCj3zNrUe5k0/BOxMmqCihAG2UxlgtBOSywwKxxUAx5WRbaEzQYtjnKZifh9DkWQiNhfmwPs6R8RWpNfhvnBXU9Sq+ZheVP9sQ/fhg3x0Jqb
 ↪    Ju0k/FZdPk5QbU5ORYVGJYxfhidWCWNMBDH+3X9xt+gGDrFkpByOHIn6SerRPs7QkxXV9ADNwlNIvQG4VO4k8Akm25CbQVzYdObDZyD7Wg==
st13.os3.su.        3600        IN        NSEC        info.st13.os3.su. A NS SOA MX RRSIG NSEC DNSKEY
st13.os3.su.        3600        IN        RRSIG        NSEC 8 3 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    c+ZuUW9EQCbZDlpI4LPTmDYhno49pAacIi0vHOyrtgKjvgdXQqrUklWPySKXZoNtrkTZPj+TZGJmzg0FRaRe+RRFcwhQzM6SxYuyX0sLRZ+hXBgqWxkod0
 ↪    GzHZSZnkyOglJyrAFQ+b5Nfa5z/Oh03DfP4w2K0QaY3GXZj3g3hxc=
info.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
info.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    0tTrCaA4clIxiB1YAtbtlKq414rXRNgbEo4AC1K5CZpoZgg6VPPZg8+wDMPsfC2hXOt4xnFt2ZAYYghOoBxwa7nDWCRskHJiu/wTohXh6gJoAvjQVteQfp
 ↪    bIifHf4aRJTsuzOvBlTgdHFa8Cwm5t26LTAubXssJ/FYx4r91xtuM=
info.st13.os3.su.        3600        IN        NSEC        mail1.st13.os3.su. CNAME RRSIG NSEC
info.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    ELUalhq/3JZ8aNxvQ24jIR0jkcCLu8P4pXq0vODGQyBClnQ0rgaikH7MoDMFCrTpPiC6pLOYooskYkeQ/eXJ6nYeaYKV9LAMgriU4UmBpx9oFBau6Qip1k
 ↪    KUGWp3y7GzdBd7xan+agBtfB7j1nDUTLef3leOd1s8GcZtjHV/PCo=
mail1.st13.os3.su.        3600        IN        A        188.130.155.46
mail1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    s5UOxL6mrF9oK++XT4ElJDYcwXxoe6mq7xVpwWXnKMIDWeo2ulILwHLIR0wjFMaI6aYF1gzL/2s3V8tRfzpJCU4A5IFrY80zvTD+fhxB8Mnl9kSUB3MEwf
 ↪    wQwi8DhgTB1ahHcQFj2nbYu+H/C3WTNzfamC/ZpVR2Y5BvF3j4uGY=
mail1.st13.os3.su.        3600        IN        NSEC        mail2.st13.os3.su. A RRSIG NSEC
mail1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    a66syVL/6J1BqZ6pQ5ql9or28t6RB2Eisq+S7R7OklTSE9g1lpn9UyQ8fBbzjjxRxcAkkCf2zfzVaLGGlXtn71VHG6xPPZFxThKbCRq7PPFSKzG0T1gMzQ
 ↪    4XVvSHANJaZ/Qv5MJP4kv9CDszKyg5FsqL90hvBixjMI6Ji33plmc=
mail2.st13.os3.su.        3600        IN        A        188.130.155.46
mail2.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    qPX4JQ7KLkuJNLcLe8Joh7crgzNJRAi0jWhJ+1R5ZT73So4LfmlpVB8pKQUBhhtVR1REZ+InyxLuCZYuPqv7SUcu+4VassO32/nqvoNbz468KCtT4Iki/G
 ↪    2c3bJH1zVf5BiyaY8WLXcoQOHPjj5Pb98jNElzHwUFpvk3ECzVNkE=
mail2.st13.os3.su.        3600        IN        NSEC        ns1.st13.os3.su. A RRSIG NSEC
mail2.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    Fwirgh4LuvSFMJDYeG6ih9/qyjyhG0+rzHI2v70QpkcSkV5qgKvmcO+Fxtypw0L8wWs9Z/YciYijCMU9FRWOZ/l8uaBi4bMjolrn0jFB4HPTfa2bITihnY
 ↪    kT/YqkG+zXN+6fcsaNOjOZacdqKD84e1SVjiy7vr2lKxc7cqkcxUM=
ns1.st13.os3.su.        3600        IN        A        188.130.155.46
ns1.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    MUMNOxdkwqzsoNgN5F+0tidyq8+y+qkDRBic82a43OcZNarYz6pMuhK35Y56rm2+cVI89xYQsleog5tHEHmPK/bV3hYLFrrwlWJkNtpgI1ZsRcVPYSVSJY
 ↪    t/RlZQ2MAtFMSi7ZB0/qTV5l2GNF5PX+Jv1ovywbvknKL146QRVP4=
ns1.st13.os3.su.        3600        IN        NSEC        sub.st13.os3.su. A RRSIG NSEC
ns1.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    HKpY7QvAu9KgKk+dVGO09Ym+3Ngb5AZAJooOsWos3jK4gv+/SuCWyOfRI5AHCx8TGltKaOMK1h9jT+74KLTaP2OmJ54B+Wf1AGXOrEqRVou4cZSIVkVPq
 ↪    v0YCsuY7rsxJFGhGQfBItM6/5RWv0JW3PS2iX1jrFcHWgUy3Wf8xE=
sub.st13.os3.su.        3600        IN        A        188.130.155.45
sub.st13.os3.su.        3600        IN        RRSIG        A 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    G8zEsrZWOX92z5Eh0XK1aAD0AABaDXiIl4mPPLgni/SAkU0wasE7Vt31vmSv8oC+WKSoreVLVESw6Y6xticppVkj+rXan7Qn8y/BNTTPWT+iodF7mi+C78
 ↪    iq+APe0dsf4w9JV5Nc6g3hzwQan8alLPcF1MI7FUROuOGwhL/glZA=
sub.st13.os3.su.        3600        IN        DS        19096 8 2
 ↪    85bc7d653e3fb6c18e1f37cfb9bfd543ac3d5da2dfa7a3f00705e5c1fc53c8fa
sub.st13.os3.su.        3600        IN        RRSIG        DS 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    1ratxMoOCwj+pxeUvWG1JKSmnKuBakxCMG2wrPgZywQBlYZelMI6c6m0vR4JuBJQrME1NA/UaJnFliZYV9nvbuzhufXNPkOUjsDoiYWNjkqDZQ3vwg1+Nf
 ↪    gj+flS+OqkAVpzVCTbELZ7r8rNhBaxpFgsFsDTrlu7sHkPYkkYKSY=
sub.st13.os3.su.        3600        IN        NSEC        www.st13.os3.su. A DS RRSIG NSEC
sub.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    o0+xi6nbRHs71LAwWsbGetzaM9LAAyS7CHy+6ym3u1vx4AjMrXfBbgxnROUkC8LfFGLwkN3qqkrD4IcQyGegQuX5LFIBxmw19NFPpEPSvF4sznreD/McWA
 ↪    I4ziUnFuao7fJO0whE+8C0WyxVuW/kFmhJQe1obytEZOyyV+/6X9M=
www.st13.os3.su.        3600        IN        CNAME        st13.os3.su.
www.st13.os3.su.        3600        IN        RRSIG        CNAME 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    Ja71D0dGV1ZapB9TUgjHODWUcfm8S+oPccKPbzmRM5q31lYLLsDbx/zszCC+Q1icGlwxetycPelRWpSiW8OtVFNTNa5fbOik1Ye9KTaeeGXQIOhZAWyTVy
 ↪    m1jGC3+vhBeONnShy2KhhLrq8EiGFxvvzBl/7QqFoLGkBYmjoOK5o=
www.st13.os3.su.        3600        IN        NSEC        st13.os3.su. CNAME RRSIG NSEC
www.st13.os3.su.        3600        IN        RRSIG        NSEC 8 4 3600 20171013113943 20170915113943 36381 st13.os3.su.
 ↪    zqNoQ+0mwmOi2n8pJq6RIKwidriCRNsWRDIPyRk1UH++kCtB6TTbvyVXpHsPxRF2eBnZ11dhWPDkMUByHYZnBqikTjl/uJD59JzkkiQaVuDpKhlGFNCUyZ
 ↪    O9LQoTPDREN7zrKg/4xDcRdmYBEettUzTs1Ac568c/i2V1OCuWXww=
```

Complete Stage: The result of the Complete Stage is in the Figure 6

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

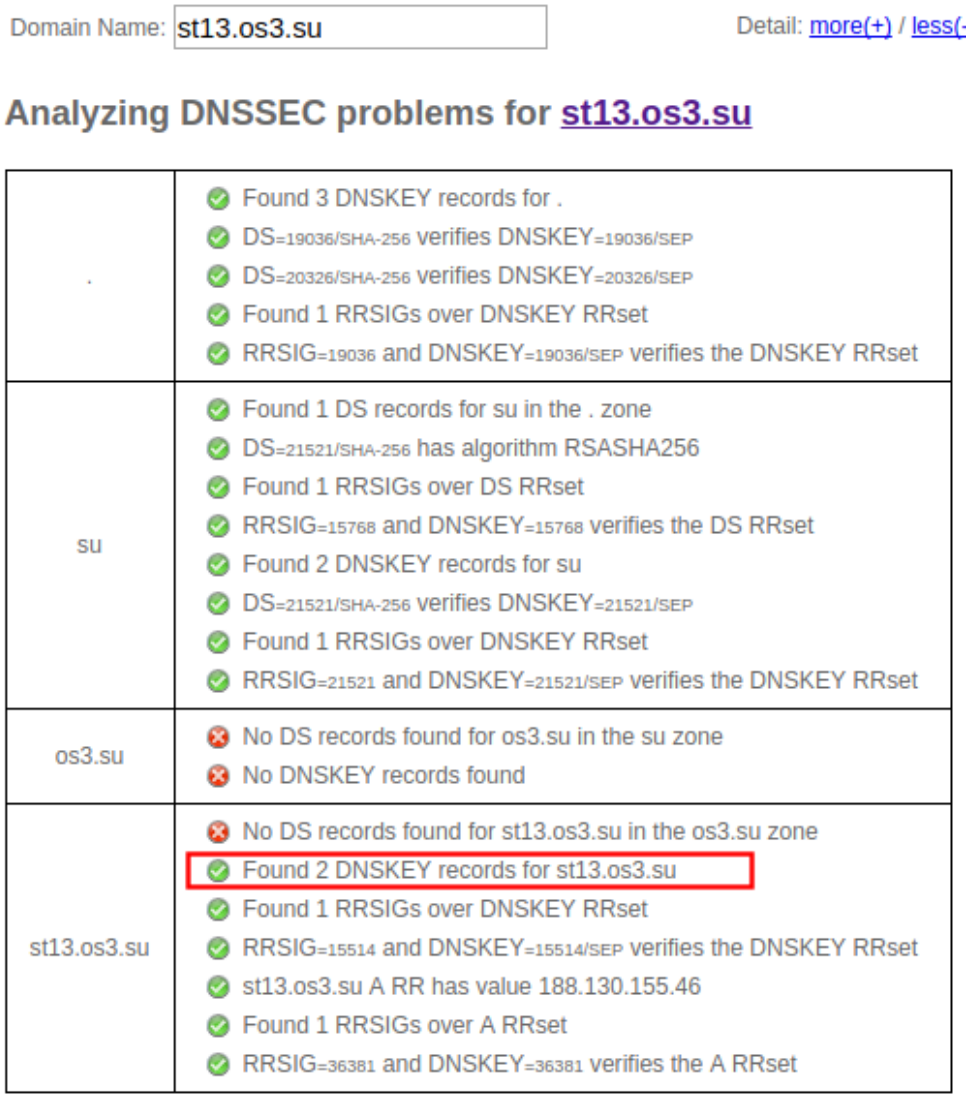

Figure 6: Complete Stage

Answer:

Yes. A KSK rollover requires interaction with the parent and the ensuing delay while waiting for it.

5 Extra Assignments (Optional)

5.1 Delegating A Secure Zone

Have you completed this task ? You should make it with your partner ? It will be better if you describe the procedure with steps.

Domain Name: sub.st12.os3.su Detail: more(+) / less(-)

Analyzing DNSSEC problems for sub.st12.os3.su

.	✓ Found 3 DNSKEY records for . ✓ DS=19036/SHA-256 verifies DNSKEY=19036/SEP ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
su	✓ Found 1 DS records for su in the . zone ✓ DS=21521/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=15768 and DNSKEY=15768 verifies the DS RRset ✓ Found 2 DNSKEY records for su ✓ DS=21521/SHA-256 verifies DNSKEY=21521/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=21521 and DNSKEY=21521/SEP verifies the DNSKEY RRset
os3.su	✗ No DS records found for os3.su in the su zone ✗ No DNSKEY records found
st12.os3.su	✗ No DS records found for st12.os3.su in the os3.su zone ✓ Found 2 DNSKEY records for st12.os3.su ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=25413 and DNSKEY=25413 verifies the DNSKEY RRset
sub.st12.os3.su	✓ Found 1 DS records for sub.st12.os3.su in the st12.os3.su zone ✓ DS=18649/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=25413 and DNSKEY=25413 verifies the DS RRset ✓ Found 2 DNSKEY records for sub.st12.os3.su ✓ DS=18649/SHA-256 verifies DNSKEY=18649/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=18649 and DNSKEY=18649/SEP verifies the DNSKEY RRset ✓ sub.st12.os3.su A RR has value 188.130.155.46 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=1056 and DNSKEY=1056 verifies the A RRset

Figure 7: Delegating A Secure Zone

6 Conclusion

A caching name server is the main component of the DNS architecture. It is subject to various types of attacks, such as cache poisoning attacks. DNSSEC was specifically designed to deal with cache poisoning and a set of other DNS vulnerabilities such as man in the middle attacks and data modification in authoritative servers.

7 References

[1] RFC 4033. DNS Security Introduction and Requirements

[2] RFC 4034.Resource Records for the DNS Security Extensions

[3] IANA: DNSSEC Information [https://www.iana.org/dnssec]

[4] RFC 4035. Protocol Modifications for the DNS Security Extensions

[5] RFC4509. Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)

[6] RFC6944. Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status

[7] RFC6781. DNSSEC Operational Practices, Version 2

[8] DNSSEC tools [https://www.dnssec-tools.org/wiki/index.php?title=Main_Page]

[9] Domain Name System Security (DNSSEC) Algorithm Numbers [https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml]

[10] Chapter 4. Advanced DNS Features [https://ftp.isc.org/isc/bind/9.8.0-P4/doc/arm/Bv9ARM.ch04.html#DNSSEC]

[11] DNSSEC Key Timing Considerations Follow-Up draft-mekking-dnsop-dnssec-key-timing-bis-02 [https://tools.ietf.org/html/draft-mekking-dnsop-dnssec-key-timing-bis-02#section-3.2]