Implementing DNSSEC with DynDNS and GoDaddy

Lawrence E. Hughes
Sixscape Communications

27 December 2017

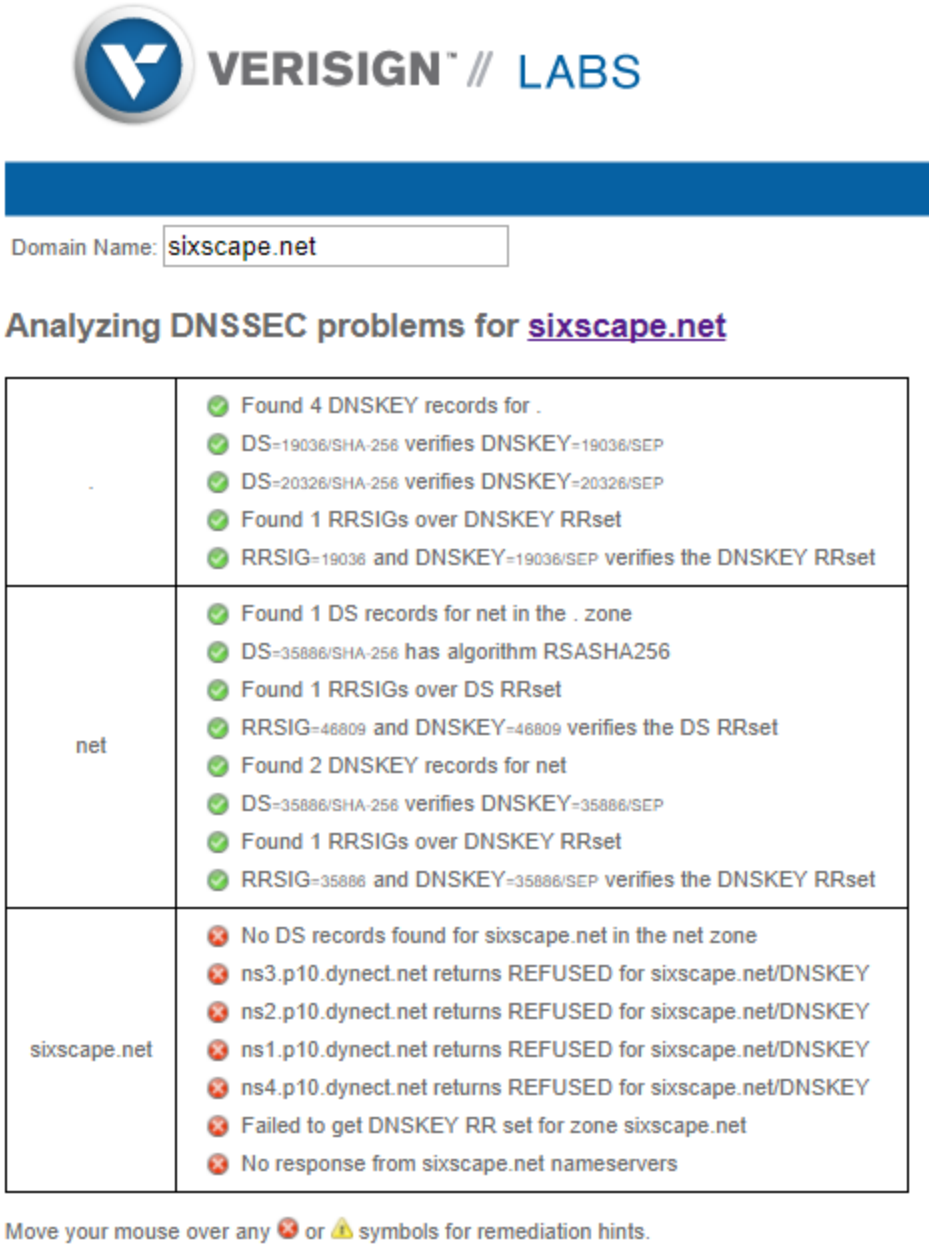
DNSSEC is an IETF standard for adding security to the DNS system, by digitally signing every resource record in a zone. This was specified in RFC 4033, “DNS Security Introduction and Requirements”, March 2005.

The signing of records is done only in the authoritative server for a given zone, but caching servers and client resolvers need to be able to process the signature (RRSIG) record to determine the validity of the corresponding record. The signature is created using a private key on the signing server, and is verified using the corresponding public key (from a published certificate).

Our domains happen to be hosted at DynDNS (Managed DNS). They have an option to digitally sign any zone(s) managed by them. I will show the steps involved in this. There is another step related to publishing the certificates needed to verify the signature which must be done on the domain registrar from whom you obtained the domain (in our case GoDaddy). This involves adding one or two DS records at the domain registrar.

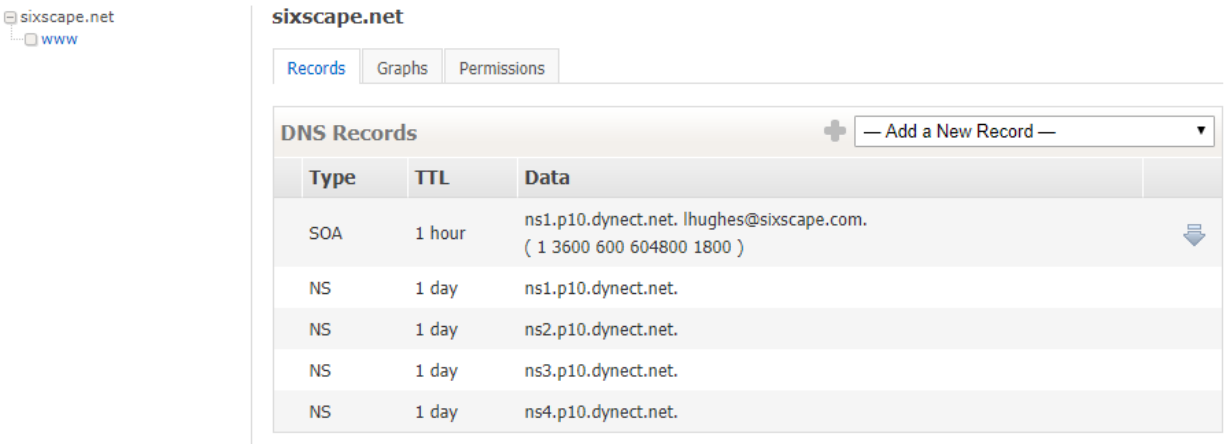
There are tools to verify the correct deployment of DNSSEC from VeriSignLabs, which we will show how to use. Our main domain (Sixscape.com) has already been signed and validated. You can verify this using the VeriSignLab tools if you like.

I will add DNSSEC to another of our domains, sixscape.net in this writeup. At the start of this process it is not currently secured:

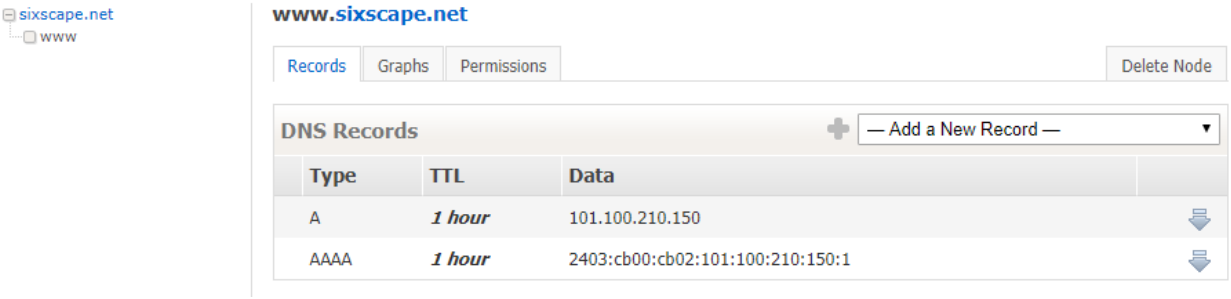


As you can see from the above, the DNS root is signed, and the TLD .net has been signed, but our domain sixscape.net has not been signed.

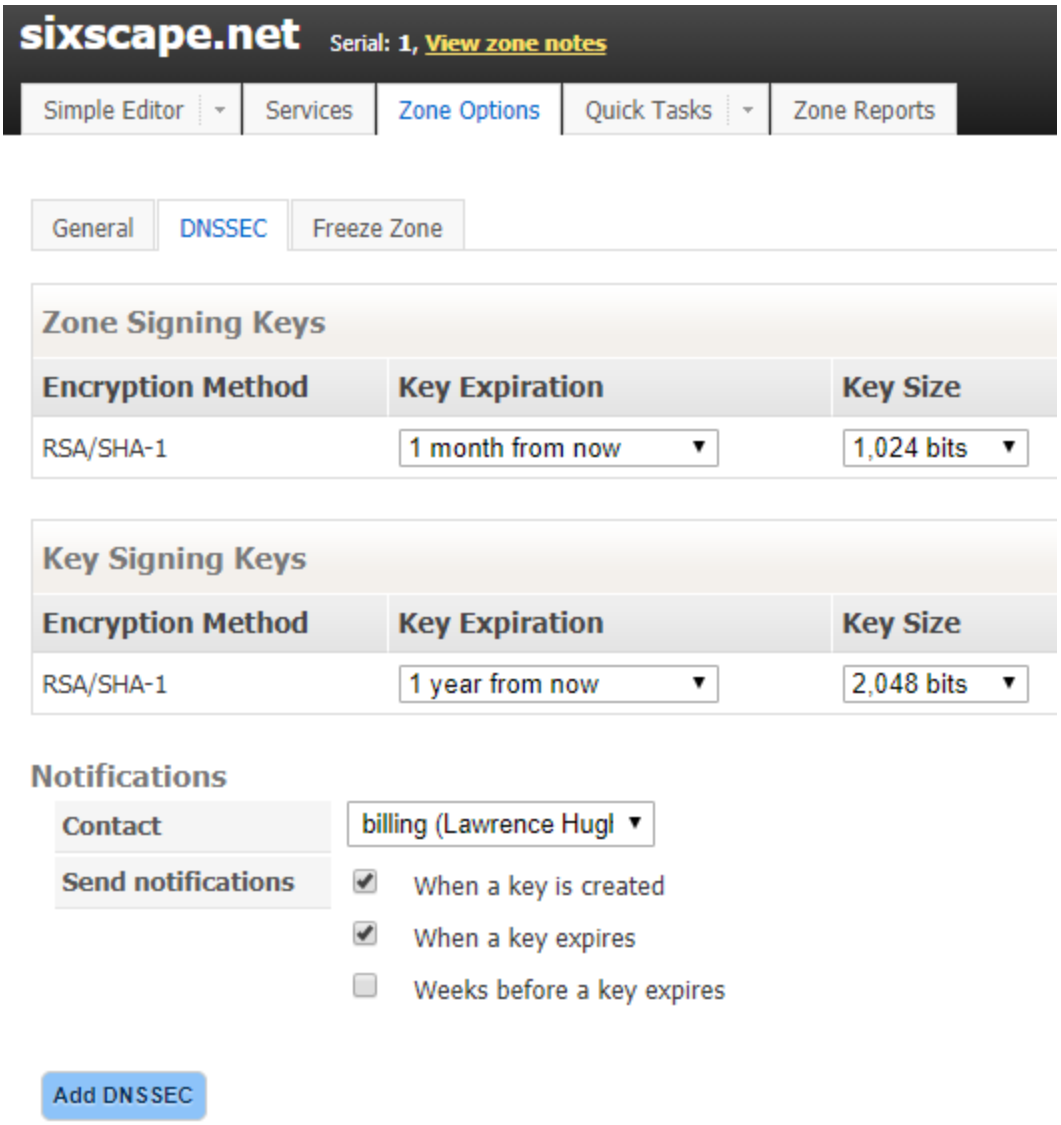
First, we bring up the DynDNS management tool. The basic records for Sixscape.net look like this:



There are A and AAAA records for one node, www.sixscape.net:

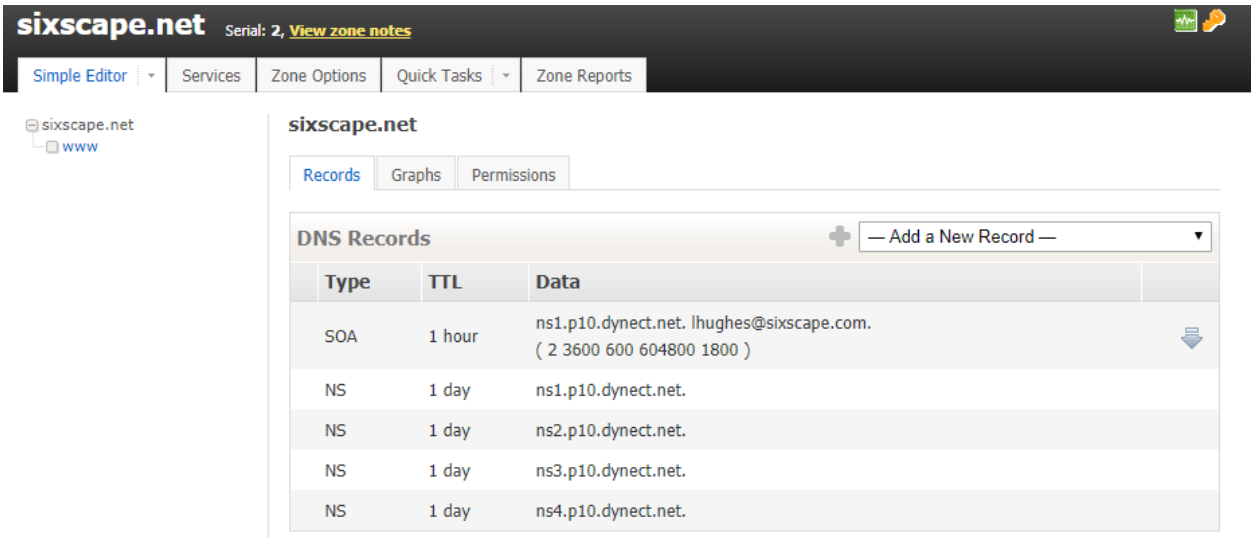


We click on the Zone Options, then select the DNSSEC tab:

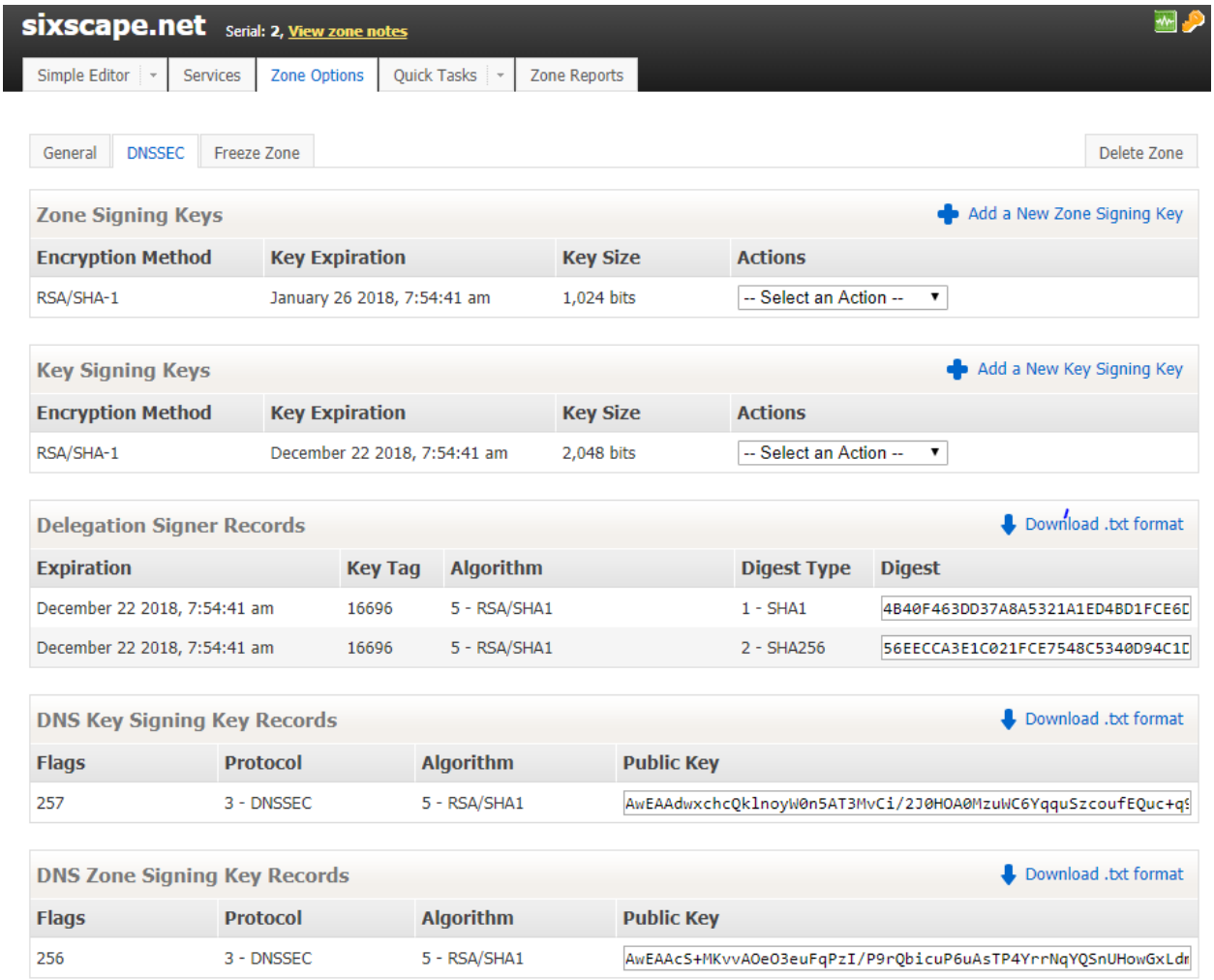


Select options and click *Add DNSSEC*.

No DNSSEC records show up in the editor, but a small orange key now denotes that this is a signed zone:



Now if you go to Zone Options, DNSSEC there will be various information about the DNSSEC setup:



The same orange key indicates that the node www.sixscape.net is now signed.

You can use dig to verify the zone and A record are signed:

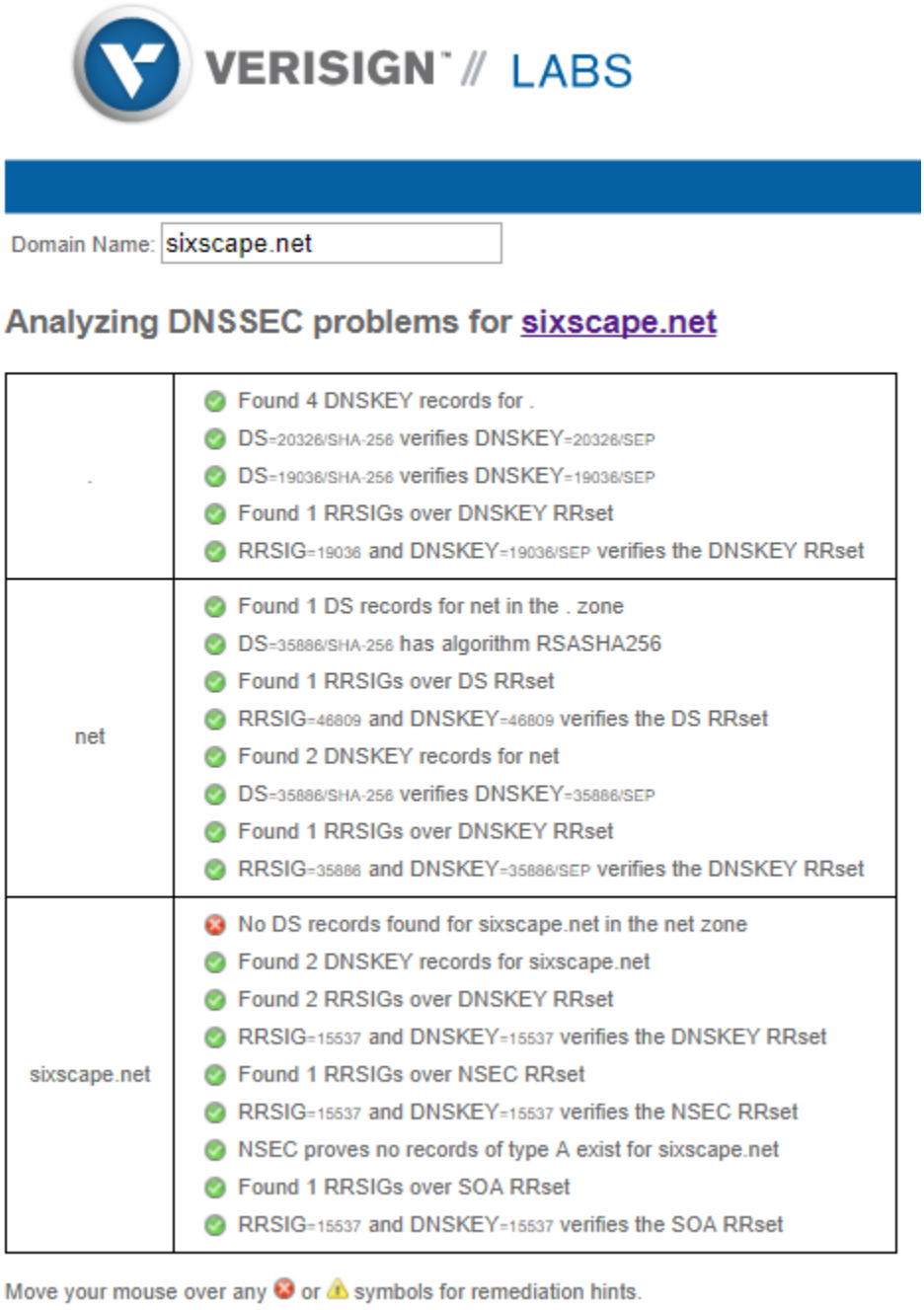
```
C:\Users\lhughes>dig sixscape.net +dnssec

; <<>> DiG 9.10.6 <<>> sixscape.net +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55843
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
sixscape.net.           1800    IN      SOA     ns1.p10.dynect.net.
lhughes.sixscape.com. 2 3600 600 604800 1800
sixscape.net.           1800    IN      RRSIG   SOA 5 2 3600 20180126065443
20171227065443 15537 sixscape.net.
DPY39b8jlLTV7I4Ep59AUrjMQJY+U2DTYnCAt3Qoqx8MLTuaPHRn6z3P
umLHntj1TcBTu+RJDB8oTaY4wQXHHIcqTNY+Xi+CL4B2yxR1mgp0vnKs
Q3pfkuwcqJS+usXUqbq+wLrh8b1uwu7xlY7Ex77exqxRS1N8zmkolXhs C6M=
sixscape.net.           1800    IN      NSEC    www.sixscape.net. NS SOA RRSIG NSEC
DNSKEY
sixscape.net.           1800    IN      RRSIG   NSEC 5 2 1800 20180126065443
20171227065443 15537 sixscape.net.
M191VmyVBE+qBkqt3oNPxyMOH0TemgTnmJSMkU38WN5Bi+hGXEROMIXV
4kPlTtnVYTGntHvGWl0TGNBhpU4pk+quNHBLyVZP4HgefdyTRtbK0Xk/
Lj5wftOdcl/QBnoV9BYos6TI2XbJ/pwlGZyzTr4/YBSrDffWZAXzntyr UaE=

;; Query time: 311 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Dec 27 15:57:57 Malay Peninsula Standard Time 2017
;; MSG SIZE  rcvd: 495
```

You can use dig to verify the zone and AAAA record are also signed:

```
C:\Users\lhughes>dig sixscape.net AAAA +dnssec

; <<>> DiG 9.10.6 <<>> sixscape.net AAAA +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21372
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;sixscape.net.                  IN      AAAA

;; AUTHORITY SECTION:
sixscape.net.           1800    IN      SOA     ns1.p10.dynect.net.
lhughes.sixscape.com. 2 3600 600 604800 1800
sixscape.net.           1800    IN      RRSIG   SOA 5 2 3600 20180126065443
20171227065443 15537 sixscape.net.
```

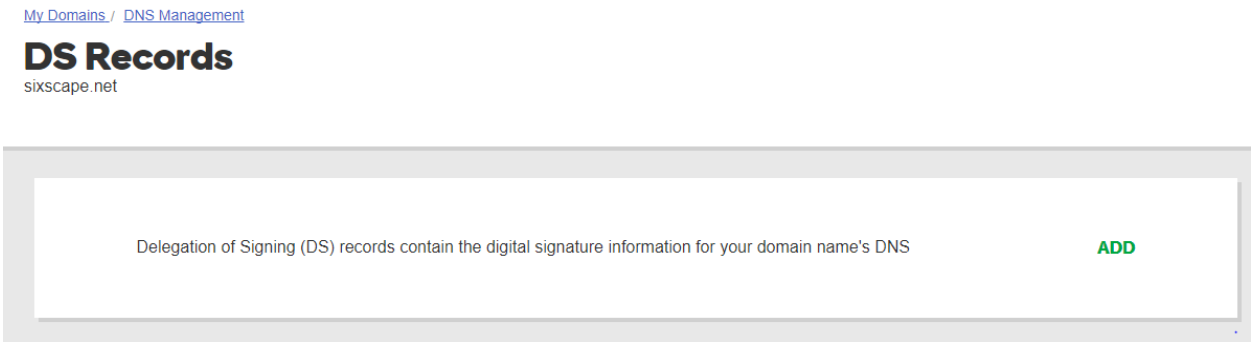
```
DPY39b8jlLTV7I4Ep59AUrjMQJY+U2DTYnCAt3Qoqx8MLTuaPHRn6z3P
umLHntj1TcBTu+RJDB8oTaY4wQXHHIcqTNY+Xi+CL4B2yxR1mgp0vnKs
Q3pfkuwcqJS+usXUqbq+wLrh8b1uwu7xlY7Ex77exqxRS1N8zmkolXhs C6M=
sixscape.net.           1800    IN      NSEC    www.sixscape.net. NS SOA RRSIG NSEC
DNSKEY
sixscape.net.           1800    IN      RRSIG   NSEC 5 2 1800 20180126065443
20171227065443 15537 sixscape.net.
M191VmyVBE+qBkqt3oNPxyMOH0TemgTnmJSMkU38WN5Bi+hGXEROMIXV
4kPlTtnVYTGntHvGWl0TGNBhpU4pk+quNHBLyVZP4HgefdyTRtbK0Xk/
Lj5wftOdcl/QBnoV9BYos6TI2XbJ/pwlGZyzTr4/YBSrDffWZAXzntyr UaE=

;; Query time: 56 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Dec 27 16:00:22 Malay Peninsula Standard Time 2017
;; MSG SIZE  rcvd: 495
```

But if we test Sixscape.net with the VeriSignLabs tool, we find errors:



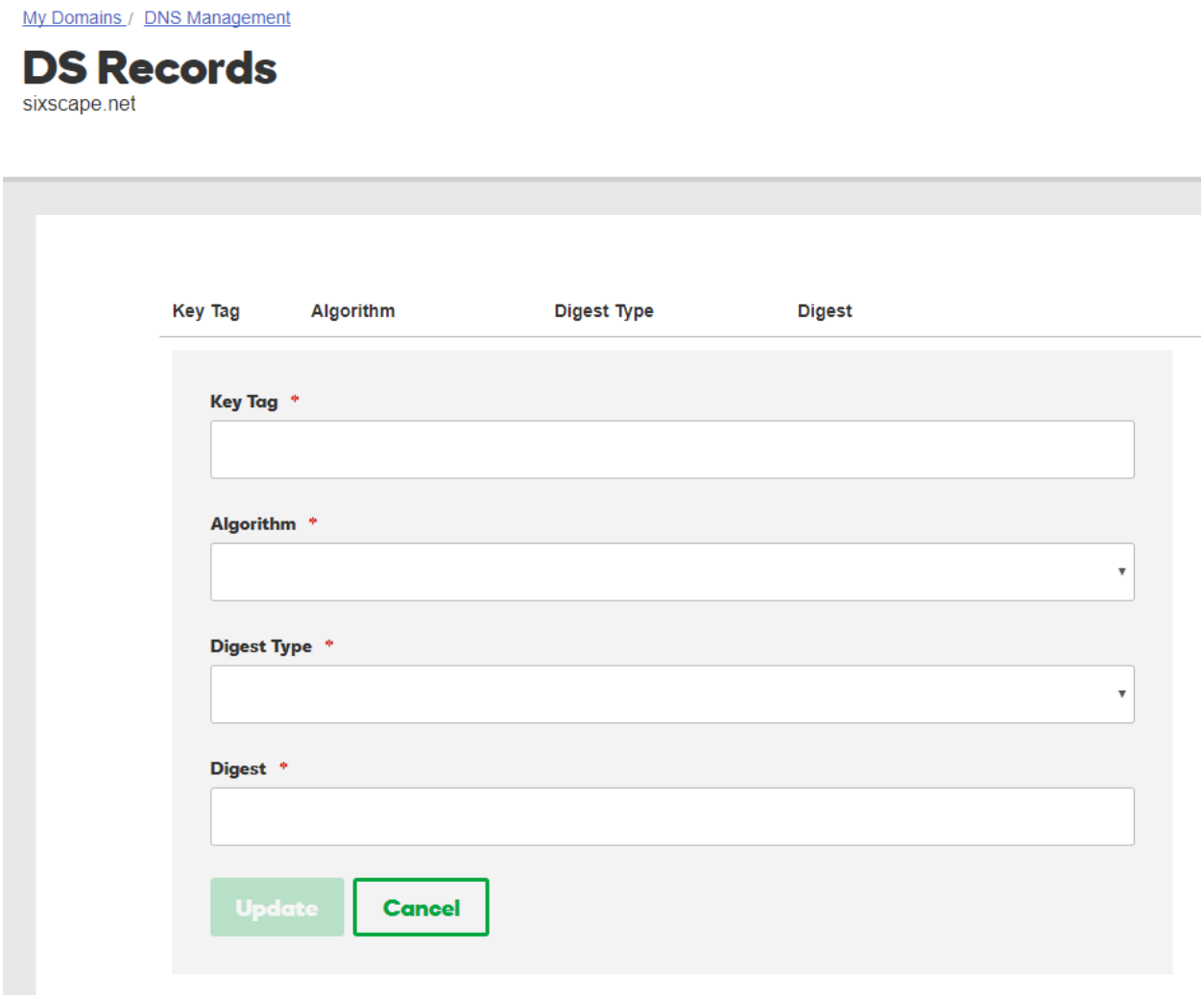
The error indicates that the required DS records are missing. These must be created not at DynDNS, but at the domain registrar where you obtained the domain. In my case, this is GoDaddy.

I go to the GoDaddy domain manager, and bring up info on Sixscape.net. At the bottom of this page there is a link for “Manage DNS”. On that page, under Advanced Features, there is a DNSSEC link. Click that:



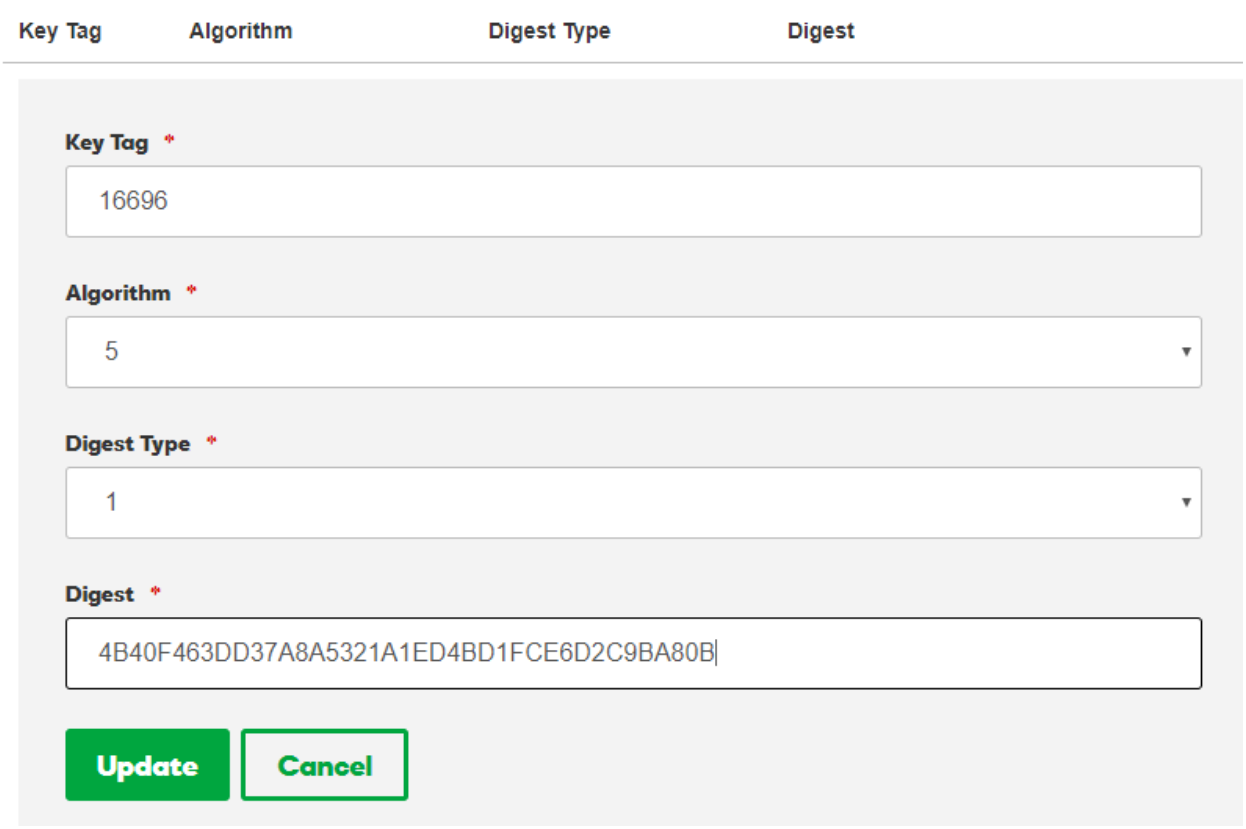
Click the ADD button to add DS record(s).

You will see the following form to create them:



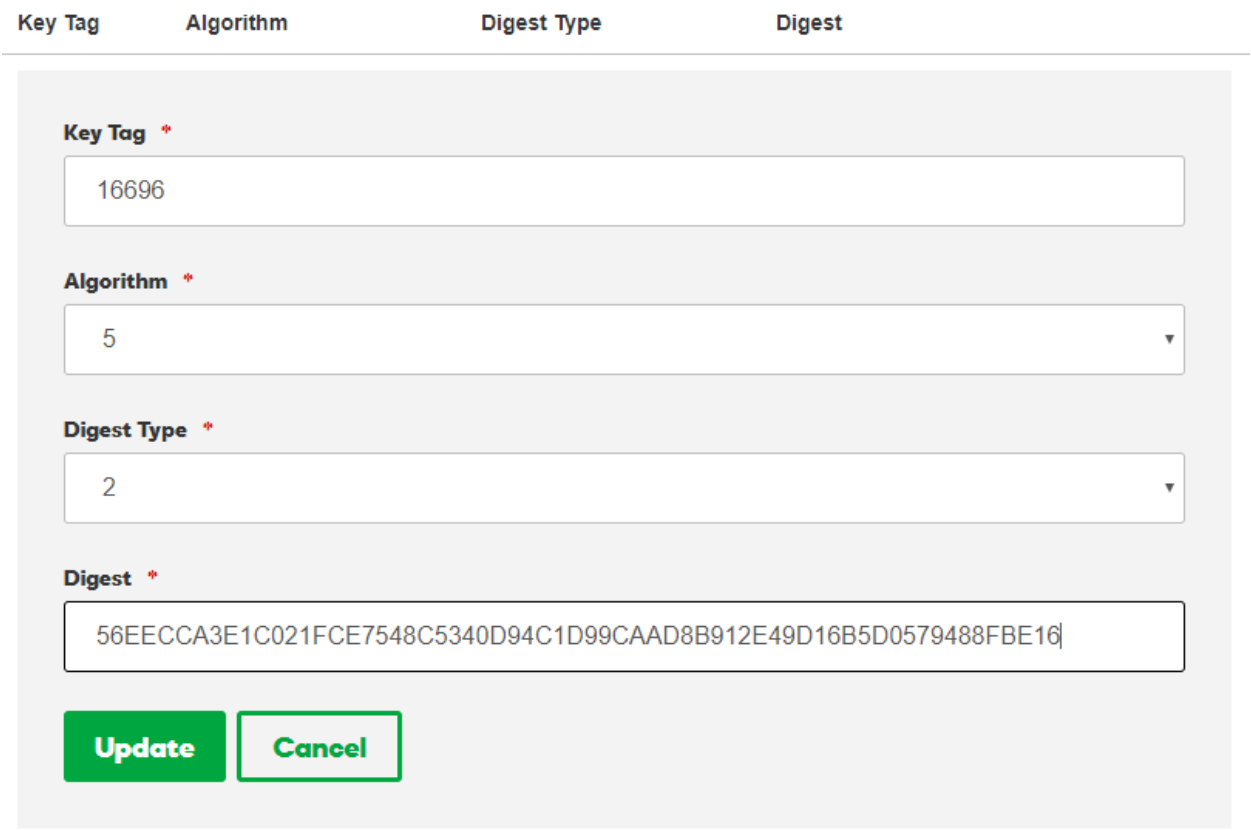
The information needed for this is in the DNSSEC details from DynDNS (see above).

Fill in the information for the first DS record (for RSA/SHA1):



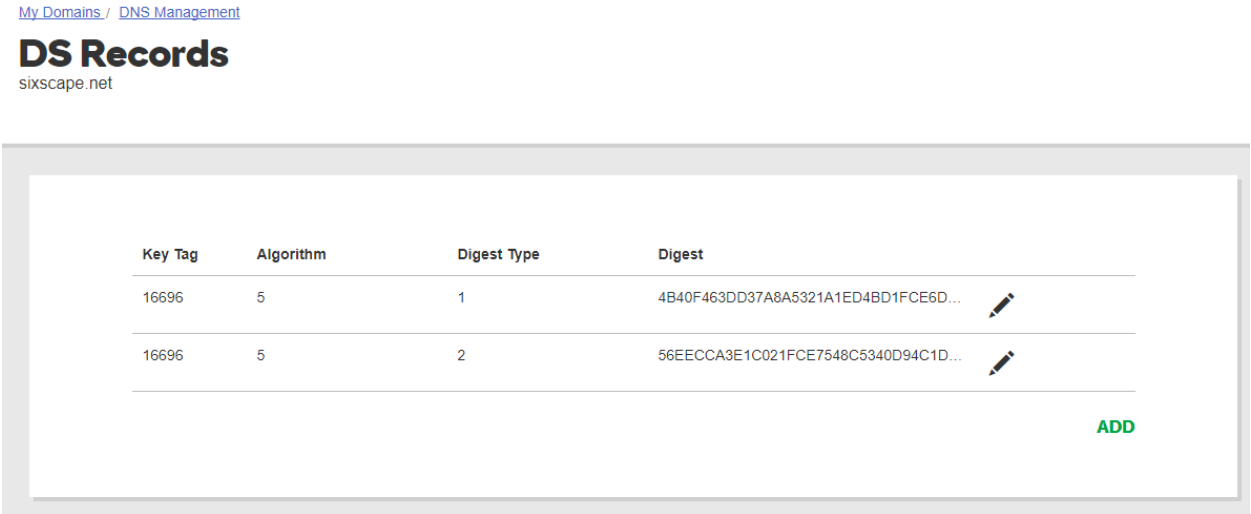
Click Update.

Now add another DS record (for RSA/SHA256):



Click Update again.

You should now have two DS records in GoDaddy:



Now recheck the DNSSEC for www.sixscape.net with the VeriSignLab tool:

Domain Name: www.sixscape.net

Analyzing DNSSEC problems for www.sixscape.net

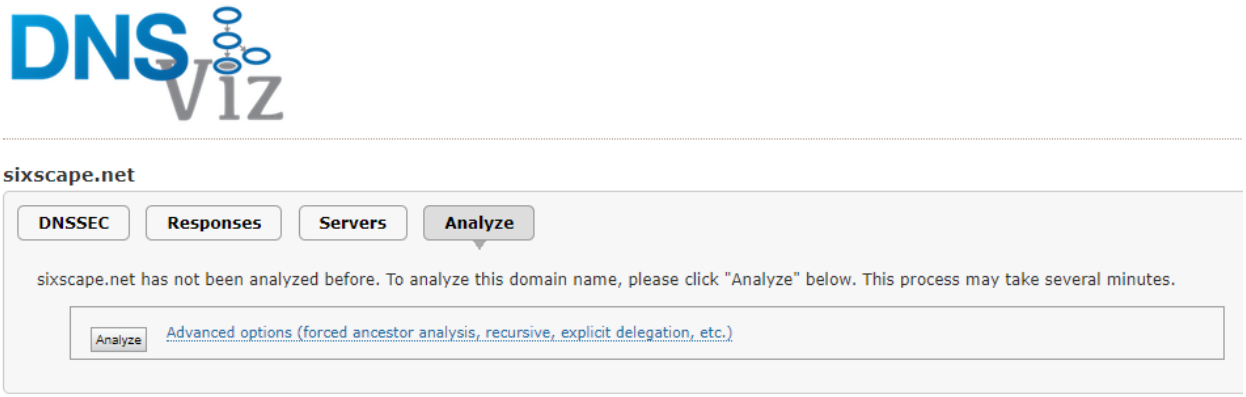
.	Found 4 DNSKEY records for . DS=19036/SHA-256 verifies DNSKEY=19036/SEP DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
net	Found 1 DS records for net in the . zone DS=35886/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=46809 and DNSKEY=46809 verifies the DS RRset Found 2 DNSKEY records for net DS=35886/SHA-256 verifies DNSKEY=35886/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=35886 and DNSKEY=35886/SEP verifies the DNSKEY RRset
sixscape.net	Found 2 DS records for sixscape.net in the net zone DS=16696/SHA-256 has algorithm RSASHA1 DS=16696/SHA-1 has algorithm RSASHA1 Found 1 RRSIGs over DS RRset RRSIG=18737 and DNSKEY=18737 verifies the DS RRset Found 2 DNSKEY records for sixscape.net DS=16696/SHA-256 verifies DNSKEY=16696/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=15537 and DNSKEY=15537 verifies the DNSKEY RRset www.sixscape.net A RR has value 101.100.210.150 Found 1 RRSIGs over A RRset RRSIG=15537 and DNSKEY=15537 verifies the A RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test www.sixscape.net at dnsviz.net.

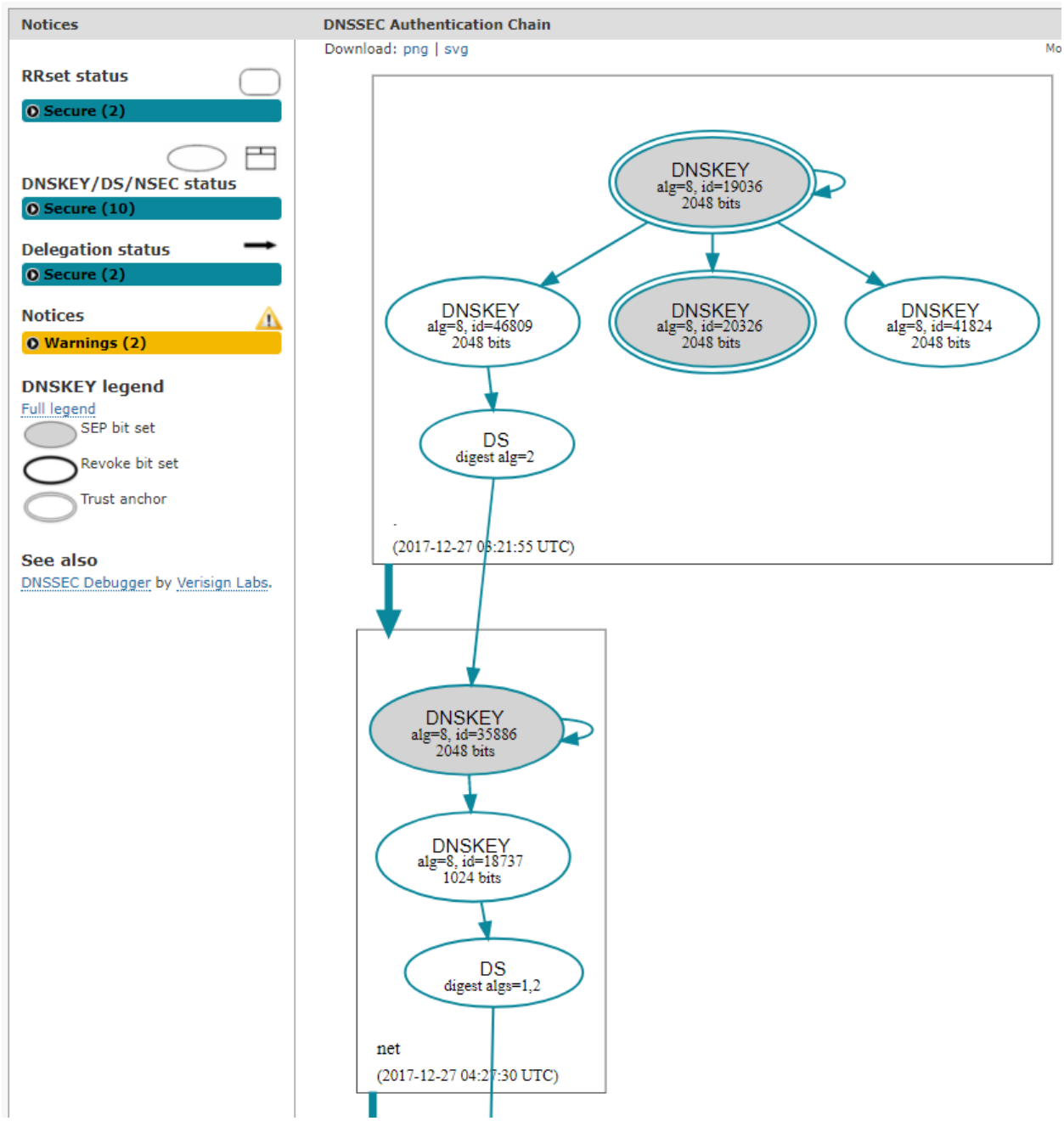
No more errors!

Now click on the link to get a second opinion from DNSViz:

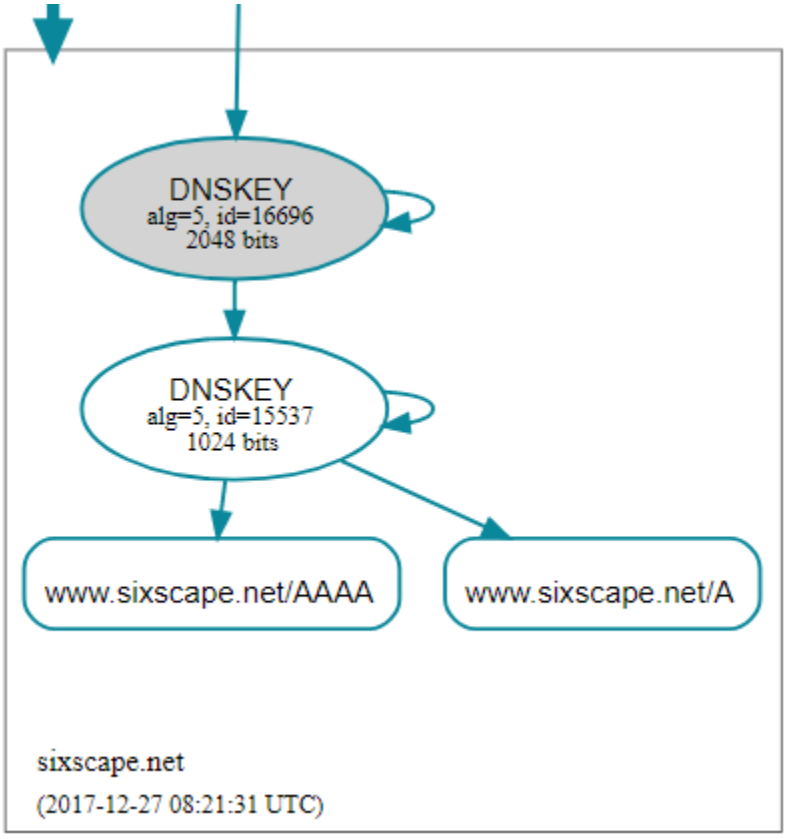


Click on the Analyse button. When analysis is complete, click on the Continue button. A detailed map of the domain will be shown.

You can now see that the root zone is signed, and the .net zone is signed:

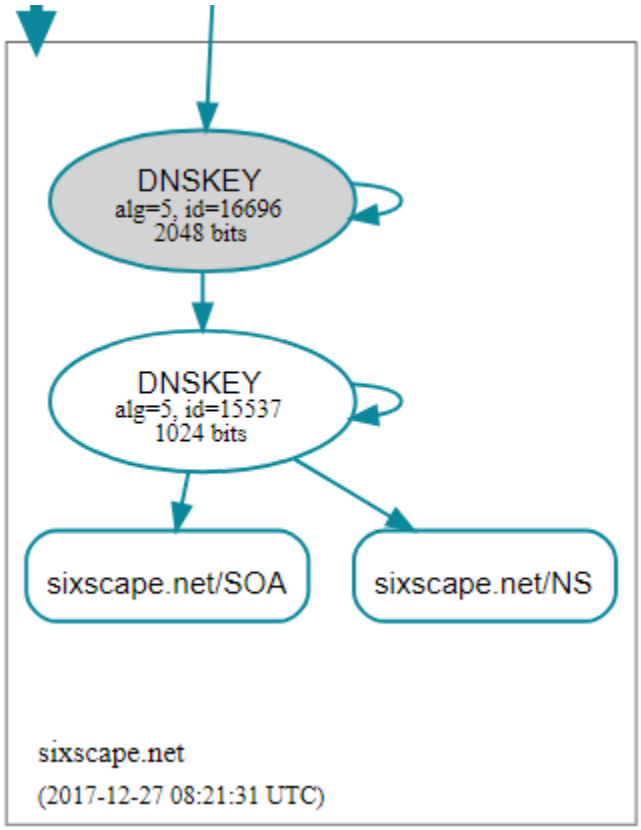


Below that, the Sixscape.net domain is now signed:



If you mouse over the AAAA and A records, it will show that they are secured.

If you look at the lower level for sixscape.net (the domain, not the node) you will see that the domain records are also secure:



Your domain is now secured with DNSSEC. If a hacker tampers with the records in this zone, it will be detected and you will be prevented from connecting to the bogus server.