

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:

Domain Name:

Analyzing DNSSEC problems for sixscape.net

.	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✘ No DS records found for sixscape.net in the net zone ✘ ns3.p10.dynect.net returns REFUSED for sixscape.net/DNSKEY ✘ ns2.p10.dynect.net returns REFUSED for sixscape.net/DNSKEY ✘ ns1.p10.dynect.net returns REFUSED for sixscape.net/DNSKEY ✘ ns4.p10.dynect.net returns REFUSED for sixscape.net/DNSKEY ✘ Failed to get DNSKEY RR set for zone sixscape.net ✘ No response from sixscape.net nameservers

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

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:

sixscape.net
www

sixscape.net

Records Graphs Permissions

Type	TTL	Data	
SOA	1 hour	ns1.p10.dynect.net. lhughes@sixscape.com. (1 3600 600 604800 1800)	⬇
NS	1 day	ns1.p10.dynect.net.	
NS	1 day	ns2.p10.dynect.net.	
NS	1 day	ns3.p10.dynect.net.	
NS	1 day	ns4.p10.dynect.net.	

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

sixscape.net
www

www.sixscape.net

Records Graphs Permissions

Delete Node

Type	TTL	Data	
A	1 hour	101.100.210.150	⬇
AAAA	1 hour	2403:cb00:cb02:101:100:210:150:1	⬇

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

Simple Editor ▾

Services

Zone Options

Quick Tasks ▾

Zone Reports

General

DNSSEC

Freeze Zone

Zone Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 month from now ▾	1,024 bits ▾

Key Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 year from now ▾	2,048 bits ▾

Notifications

Contact

billing (Lawrence Hugl ▾)

Send notifications

- When a key is created
- When a key expires
- Weeks before a key expires

Add DNSSEC

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:

sixscape.net Serial: 2, [View zone notes](#)

Simple Editor | Services | Zone Options | Quick Tasks | Zone Reports

sixscape.net
www

sixscape.net

Records | Graphs | Permissions

DNS Records + Add a New Record

Type	TTL	Data
SOA	1 hour	ns1.p10.dynect.net. lhughes@sixscape.com. (2 3600 600 604800 1800)
NS	1 day	ns1.p10.dynect.net.
NS	1 day	ns2.p10.dynect.net.
NS	1 day	ns3.p10.dynect.net.
NS	1 day	ns4.p10.dynect.net.

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

sixscape.net Serial: 2, [View zone notes](#)

Simple Editor | Services | Zone Options | Quick Tasks | Zone Reports

General | DNSSEC | Freeze Zone Delete Zone

Zone Signing Keys + Add a New Zone Signing Key

Encryption Method	Key Expiration	Key Size	Actions
RSA/SHA-1	January 26 2018, 7:54:41 am	1,024 bits	-- Select an Action --

Key Signing Keys + Add a New Key Signing Key

Encryption Method	Key Expiration	Key Size	Actions
RSA/SHA-1	December 22 2018, 7:54:41 am	2,048 bits	-- Select an Action --

Delegation Signer Records Download .txt format

Expiration	Key Tag	Algorithm	Digest Type	Digest
December 22 2018, 7:54:41 am	16696	5 - RSA/SHA1	1 - SHA1	4B40F463DD37A8A5321A1ED4BD1FCE6C
December 22 2018, 7:54:41 am	16696	5 - RSA/SHA1	2 - SHA256	56EECCA3E1C021FCE7548C5340D94C1C

DNS Key Signing Key Records Download .txt format

Flags	Protocol	Algorithm	Public Key
257	3 - DNSSEC	5 - RSA/SHA1	AwEAAAwXchcQk1noyW0n5AT3MvCi/2J0HOA0MzUwC6YqquSzcoufEQuc+qS

DNS Zone Signing Key Records Download .txt format

Flags	Protocol	Algorithm	Public Key
256	3 - DNSSEC	5 - RSA/SHA1	AwEAAcS+MKvvA0eO3euFqPzI/P9rQbicuP6uAsTP4YrrNqYQSnUHowGxLdr

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.
DPY39b8j1LTv7I4Ep59AUrjMQJY+U2DTYnCA3Qoqx8MLTuaPHRn6z3P
umLHntj1TcBTu+RJDB8oTaY4wQXHHIcqTNY+Xi+CL4B2yxRlmgp0vnKs
Q3pfkuwcqJS+usXUqbq+wLrh8bluwu7xly7Ex77exqxRS1N8zmkolXhs 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+CL4B2yxRlmgp0vnKs
Q3pfkuwcqJS+usXUqbq+wLrh8bluwu7xly7Ex77exqxRS1N8zmkolXhs 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:



Domain Name:

Analyzing DNSSEC problems for sixscape.net

.	<ul style="list-style-type: none">✔ Found 4 DNSKEY records for .✔ DS=20326/SHA-256 verifies DNSKEY=20326/SEP✔ DS=19036/SHA-256 verifies DNSKEY=19036/SEP✔ Found 1 RRSIGs over DNSKEY RRset✔ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
net	<ul style="list-style-type: none">✔ 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	<ul style="list-style-type: none">✘ No DS records found for sixscape.net in the net zone✔ Found 2 DNSKEY records for sixscape.net✔ Found 2 RRSIGs over DNSKEY RRset✔ RRSIG=15537 and DNSKEY=15537 verifies the DNSKEY RRset✔ Found 1 RRSIGs over NSEC RRset✔ RRSIG=15537 and DNSKEY=15537 verifies the NSEC RRset✔ NSEC proves no records of type A exist for sixscape.net✔ Found 1 RRSIGs over SOA RRset✔ RRSIG=15537 and DNSKEY=15537 verifies the SOA RRset

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

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:

DS Records

sixscape.net

Delegation of Signing (DS) records contain the digital signature information for your domain name's DNS

[ADD](#)

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

You will see the following form to create them:

DS Records

sixscape.net

Key Tag	Algorithm	Digest Type	Digest
---------	-----------	-------------	--------

Key Tag *

Algorithm *

Digest Type *

Digest *

Update

Cancel

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):

Key Tag	Algorithm	Digest Type	Digest
Key Tag * <input type="text" value="16696"/>	Algorithm * <input type="text" value="5"/>	Digest Type * <input type="text" value="1"/>	Digest * <input type="text" value="4B40F463DD37A8A5321A1ED4BD1FCE6D2C9BA80B"/>
<input type="button" value="Update"/> <input type="button" value="Cancel"/>			

Click Update.

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

Key Tag	Algorithm	Digest Type	Digest
Key Tag * 16696	Algorithm * 5	Digest Type * 2	Digest * 56EECCA3E1C021FCE7548C5340D94C1D99CAAD8B912E49D16B5D0579488FBE16
<input type="button" value="Update"/> <input type="button" value="Cancel"/>			

Click Update again.

You should now have two DS records in GoDaddy:

[My Domains / DNS Management](#)

DS Records

sixscape.net

Key Tag	Algorithm	Digest Type	Digest	
16696	5	1	4B40F463DD37A8A5321A1ED4BD1FCE6D...	
16696	5	2	56EECCA3E1C021FCE7548C5340D94C1D...	
ADD				

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

Domain Name:

Analyzing DNSSEC problems for www.sixscape.net

.	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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:



sixscape.net

DNSSEC

Responses

Servers

Analyze

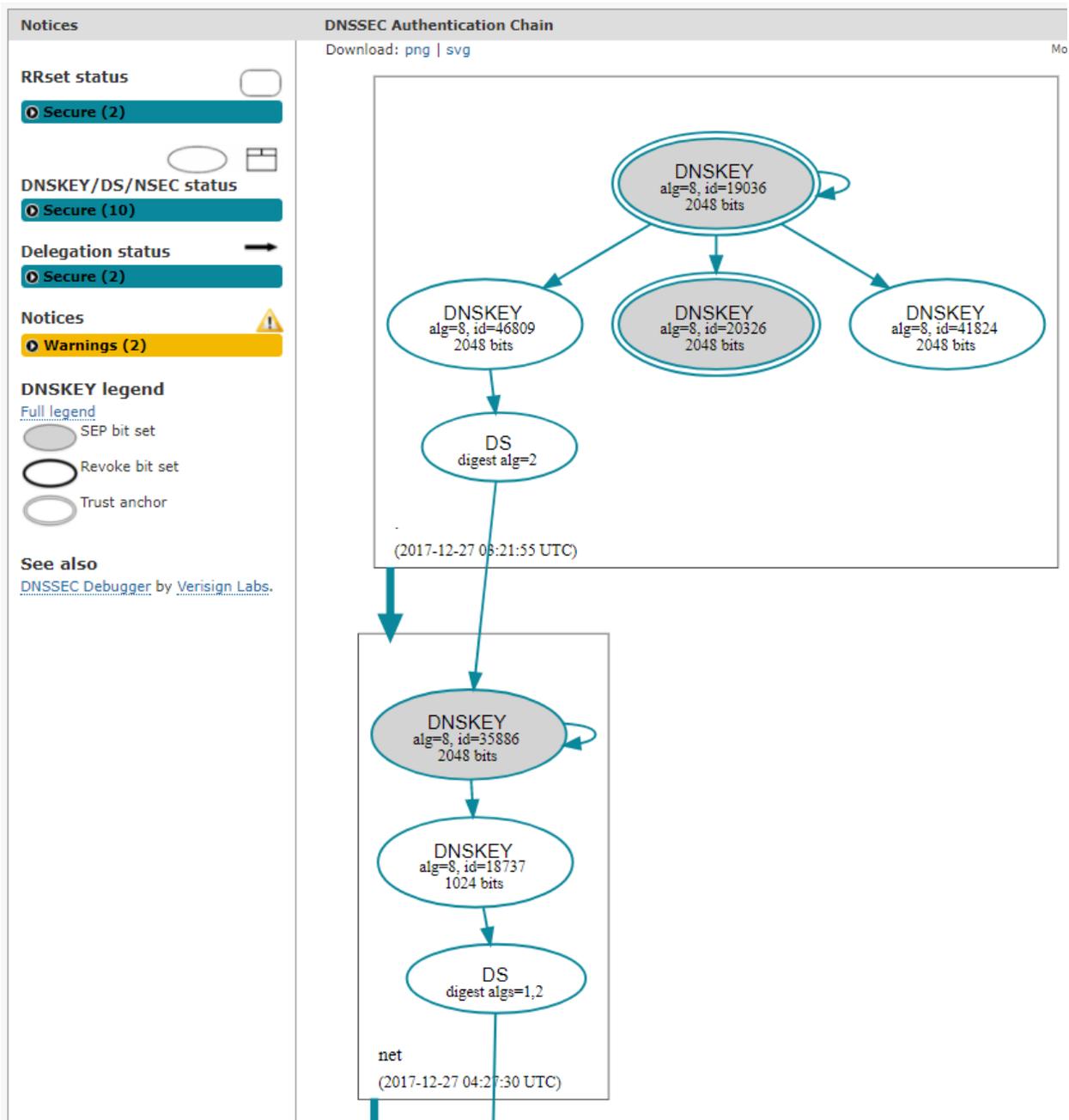
sixscape.net has not been analyzed before. To analyze this domain name, please click "Analyze" below. This process may take several minutes.

Analyze

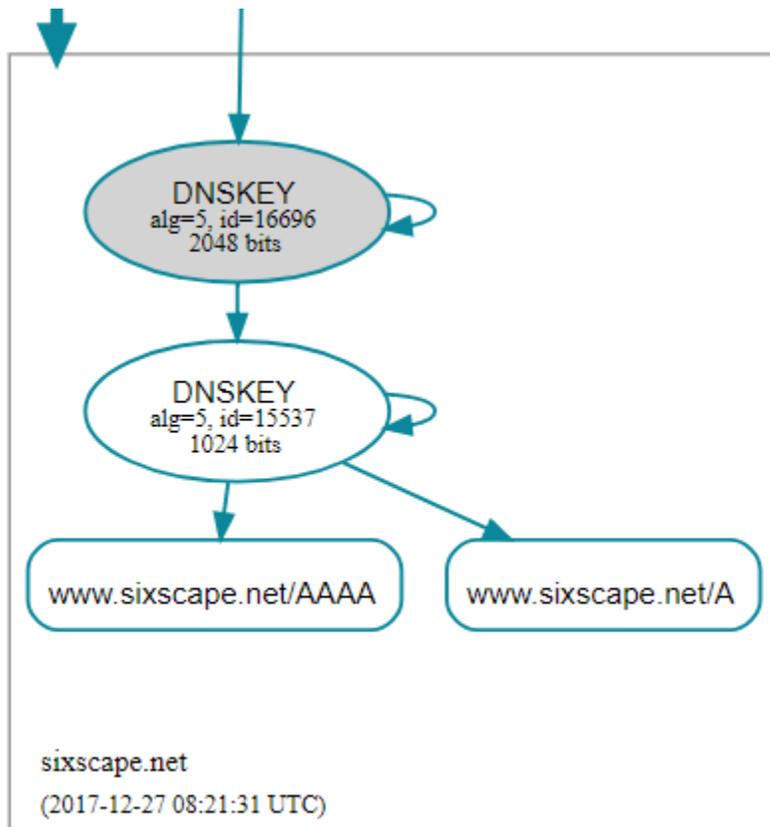
[Advanced options \(forced ancestor analysis, recursive, explicit delegation, etc.\)](#)

Click on the Analyze 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:

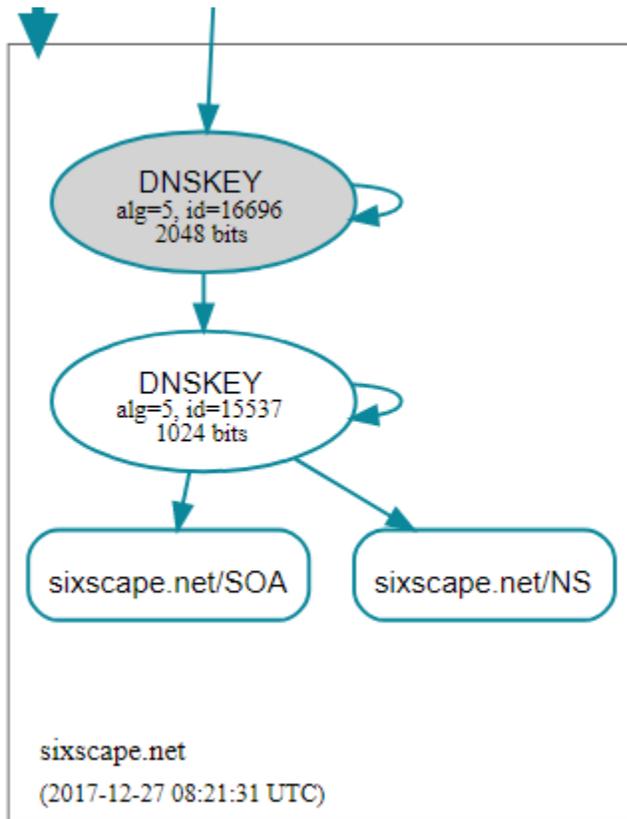


Below that, the Sixscape.net domain is now signed:



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.