DNSSEC for Managers – The Three Spheres

By
Mark Elkins
July 2013

Introduction – Nameserver roles

- An Authoritative Nameserver knows everything about a zone and can be asked by anyone for information about its zone.

  In DNSSEC terms, this is where we "Sign a Zone"

- A Recursive Nameserver knows nothing but can hunt down the answer. It should only do this job for a select group of people.

  In DNSSEC terms, Recursive Servers do DNSSEC Validation. They Validate what they find.

- These two roles **do not overlap.**
- They should be **run on separate machines.**

DNS
Domain Name Services (Pty) Ltd

Sphere One - Validation

The "Trust Anchor" is needed.

```
# dig . dnskey | grep -w 257 > root.key
```

Manipulate into the "named.conf" file as:-

```
managed-keys {
. initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
 FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
 bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
 X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
 W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
 Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
 QxA+Uk1ihz0=";
};
```

Stick it just after the "options" section.
For more info - please look at:
http://dnssec.co.za (.or.tz, .na)

DNS
Domain Name Services (Pty) Ltd

Sphere One - Validation

If you use Chrome or Firefox, install the "DNSSEC Validator" Add-on.

Search for "DNSSEC Validator"

 - Signed and Validates, Chain of Trust is intact.

 - Signed, but Chain of Trust is broken.

 - Signed, but does not Validate, Chain of Trust is intact.

 - Not Signed.

DNS
Domain Name Services (Pty) Ltd

Sphere Two - Zone Signing

Signing can be quite simple

There are Scripts (eg. mine) (*http://posixafrica.com*)
and black box solutions (*eg. OpenDNSSEC*)

This can be done in just three commands....
(*Assuming you have a zone called 'web.za'*)

```
# dnssec-keygen -a RSASHA256  -b 1024  web.za
# dnssec-keygen -a RSASHA256  -b 2048 -f KSK  web.za
# dnssec-signzone -S web.za
```

Domain Name Services (Pty) Ltd

Sphere Two - Zone Signing

'web.za' is now signed and the new zone is called 'web.za.signed'

There is also a file called 'dsset-web.za.' *(discussed next slide)*

Edit your 'named.conf' to use the new 'signed' version of the zone.

In reality - one should at some regular determined frequency, generate new keys and roll out the old keys....

Domain Name Services (Pty) Ltd

Sphere Three – Chain of Trust

The contents of the file 'dsset-web.za.' needs to be securely installed into the parent zone of 'za'.

```
web.za. IN DS 52867 8 1 921AFBC6DF6....
web.za. IN DS 52867 8 2 9FBC5FBC6B9....
```

1 - Encrypted e-mail *(How I talk to Tanzania or Namibia)*

2 - Via a web front-end *(AFRINIC, Root)*

3 - Via the Registries EPP system *(COZA/dotAfrica)*

Conclusion – Why all this work ?

1 - DNS Security - helps you and your customers to get to the right place. The Internet relies on DNS working correctly!

2 - Certification Security - DANE (*DNS-Based Authentication of Named Entities*)

a) Secure your Web Security Certificate

(so it c*an only come from your supplier*)

b) Create and use your own Certificate (Self-Sign).

3 - Potential other uses:

DANE-for-SMTP-and-MUAs

DANE-for-S/MIME

DANE-for-XMPP (*instant messaging*)

DNS
Domain Name Services (Pty) Ltd