

DNSSEC Signing Only Operations Transition Checklist

Abbreviations

RO = Relinquishing DNS Operator (DNSSEC Zone Operator)
 AO= Acquiring DNS Operator (DNSSEC Zone Operator Successor)
 ADMIN= Zone Administrator

AO sets up Signer/Hidden Master NS-AO=(K2,Z2,Z1)K2 (NS)Z2 (*)Z2

Step	Activity	Initial	Time
1	ADMIN sends request to AO to configure, manage, and serve SIGNED zone via a Hidden Master (NS-AO). RO and AO cooperate in zone database access/transfer (e.g. enable AXFR..etc).		
2	RO and AO agree on timing of TRANSITION PERIOD. RO will not perform any routine ZSK rollovers during this period.		
3	AO extracts RO ZSK (Z1) from RO nameserver and verifies with RO.		
4	In a Key Ceremony, AO generates DNSKEY RRset using the SAME algorithm as RO incorporating RO ZSK (Z1) and AO KSK (K2) + ZSK (Z2) (signed with AO KSK) covering agreed TRANSITION PERIOD. This TRANSITION DNSKEY RRset will be used to transition from keys under RO control to keys under AO control.		
5	At the same Key Ceremony AO generates second DNSKEY RRset using the SAME algorithm as RO but without adding RO ZSK (Z1) covering the same agreed TRANSITION PERIOD. These represent the NORMAL DNSKEY RRset at the completion of the transition.		
6	Corresponding AO DS (DS2) is recorded for later transmission to IANA		

RO adds AO ZSK to DNSKEY RRset NS=(K1,Z1,Z2)K1 (NS)Z1 (*)Z1

Step	Activity	Initial	Time
7	In a Key Ceremony, RO generates DNSKEY RRset incorporating VERIFIED AO ZSK (Z2) and RO KSK (K1) + ZSK (Z1) (signed with RO KSK) covering agreed TRANSITION PERIOD. This TRANSITION DNSKEY RRset will be used to transition from keys under RO control to keys under AO control.		
8	RO incorporates this DNSKEY RRset in current zone, increments SOA Serial, and publishes signed zone on its nameservers.		

ADMIN sends add DS request to IANA root=DS1,DS2

Step	Activity	Initial	Time
9	ADMIN sends a request to IANA to add AO DS (DS2) to current zone RO DS (DS1) root entry. Note: this may return an error. Request IANA to proceed anyway.		

Wait for processing and caches to update

Step	Activity	Initial	Time
10	AO and RO wait until the changes appear in the root plus any caching and propagation delays for current zone and root zone.		

Switch Hidden Master from NS to NS-AO

Step	Activity	Initial	Time
11	AO incorporates TRANSITION DNSKEY RRsets in the SIGNED zone it generates and serves via its Hidden Master. The SIGNED zone should duplicate the currently published zone in every way including NSset. RRSIGs will be calculated based on AO ZSK and KSK.		
12	AO's Hidden Master (NS-AO) is configured to allow transfer and provide notification to the current zone nameservers.[1]		
13	The current zone nameservers are reconfigured to draw the zone from the AO Hidden Master (NS-AO). [1]		
14	Finally AO updates the SOA Serial past the current RO published zone, re-signs the zone, and publishes it on the Hidden Master for the public nameservers to load from.		

Wait for processing and caches to update

Step	Activity	Initial	Time
15	AO and RO wait until the changes appear plus any caching and propagation delays for zone.		

AO returns to publishing AO only DNSKEY RRset NS-AO=(K2,Z2)K2 (NS)Z2 (*)Z2

Step	Activity	Initial	Time
16	AO reverts to using NORMAL DNSKEY RRsets containing only AO KSK and AO ZSK (signed by AO KSK), and increments SOA Serial, to generating and publish a new zone via its Hidden Master.		

ADMIN sends remove DS request to IANA root=DS2

Step	Activity	Initial	Time
17	ADMIN sends a request to IANA to remove RO DS (DS1).		

Wait for processing and caches to update

Step	Activity	Initial	Time
18	AO and RO wait until the changes appear in the root plus any caching and propagation delays for zone.		

Transition complete

Step	Activity	Initial	Time
19	Transition of operations from RO to AO is now complete. RO may cease producing a signed zone.		

Notes:

[1] Please refer to PCH TLD Administrator's Anycast Configuration Checklist for details and guidance.

Summary:

In Cache: DS1 (K1,Z1)K1 (NS)Z1 (*)Z1

AO generates DNSKEY RRsets (K2,Z2,Z1)K2
RO adds AO ZSK to DNSKEY RRset HM=NS=(K1,Z1,Z2)K1 (NS)Z1 (*)Z1 SOA++
ADMIN sends add DS request to IANA root=DS1,DS2
Wait for processing and caches to update

In Cache: DS1 DS2 (K1,Z1,Z2)K1 (NS)Z1 (*)Z1
Switch Hidden Master HM=NS-AO=(K2,Z2,Z1)K2 (NS)Z2 (*)Z2 SOA++
Wait for processing and caches to update

In Cache: DS1 DS2 (K2,Z2,Z1)K2 (NS)Z2 (*)Z2
AO returns to publishing AO only DNSKEY RRset HM=NS-AO=(K2,Z2)K2 (NS)Z2 (*)Z2 SOA++
ADMIN sends remove DS request to IANA root=DS2
Wait for processing and caches to update

In Cache: DS2 (K2,Z2)K2 (NS)Z2 (*)Z2
Transition complete

Example 1:

```
STEP 1
STEP 2 TRANSITION PERIOD = NOW until +604800 (1 week)
STEP 3 AO
dig -t dnskey dnssec2.net
Cut and paste ZSK into ROkey.key
dig axfr dnssec2.net @ns3.xtcn.com > slave/dnssec2.net.zone

STEP 4 AO

tar zxf bind-9.7.3.tar.gz
cd bind-9.7.3
configure
make
cd ..
bind-9.7.3/bin/dig/dig axfr dnssec2.net @ns.xtcn.com > slave/dnssec2.net.zone

bind-9.7.3/bin/dnssec/dnssec-keygen -a RSASHA256 -b 2048 -f KSK dnssec2.net
Kdnssec2.net.+008+12850

bind-9.7.3/bin/dnssec/dnssec-keygen -a RSASHA256 -b 1024 dnssec2.net
Kdnssec2.net.+008+60294

STEP 5 AO

cat slave/dnssec2.net.zone Kdnssec2.net.+008+12850.key Kdnssec2.net.+008+60294.key
> normal

bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +604800 -o dnssec2.net. normal
Kdnssec2.net.+008+60294 Kdnssec2.net.+008+12850
dnssec-signzone: warning: tmpii:25: using RFC1035 TTL semantics
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                        ZSKs: 0 active, 1 present, 0 revoked
normal.signed
Extract DNSKEY RRset = NORMAL

cat slave/dnssec2.net.zone Kdnssec2.net.+008+12850.key Kdnssec2.net.+008+60294.key
ROkey.key > roll
bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +3600 -o dnssec2.net. roll
Kdnssec2.net.+008+60294 Kdnssec2.net.+008+12850
dnssec-signzone: warning: tmpii:25: using RFC1035 TTL semantics
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                        ZSKs: 0 active, 2 present, 0 revoked
roll.signed
Extract DNSKEY RRset = ROLL

edit named.conf to server roll.signed
rndc.key
rndc.conf
mkdir data
mkdir logs

bind-9.7.3/bin/named/named -c named.conf -u root

dig -t dnskey dnssec2.net @127.0.0.1

STEP 6 AO save dsset-dnssec2.net. for DS2. Send to ADMIN

cat dsset-dnssec2.net.
dnssec2.net.      IN DS 12850 8 1 56CCC27A83CE97637223F12EA05272205A0FF90B
dnssec2.net.      IN DS 12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C 62C90D19

Step 7 RO
```

```
cp Kdnssec2.net.+008+60294.key AOkey.key
AOkey.key from above (same as Kdnssec2.net.+008+60294.key contents)
```

```
km_no_roll dnssec2.net 20110309231442 604800 Z201121 AOkey.key
```

```
km_check 20110309231442.dnssec2.net.keybundle.tar.gz | less
```

STEP 8 RO

```
scp -p 20110309231442.dnssec2.net.keybundle.tar.gz
dnssec@192.101.186.215:~/msigner/zones/dnssec2.net
```

STEP 9 ADMIN

```
Send DS
dnssec2.net.          IN DS 12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C 62C90D19
```

```
Root should now have:
dnssec2.net. IN DS 43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B6050434B
dnssec2.net. IN DS 12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C62C90D19
```

STEP 10 WAIT

```
dig +dnssec -t dnskey dnssec2.net
```

```
; <<>> DiG 9.7.2-P3 <<>> +dnssec -t dnskey dnssec2.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33955
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
;; QUESTION SECTION:
;dnssec2.net.          IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.          241        IN          DNSKEY 257 3 8
AwEAAfTGhvzs7HNodhm/iIRKrcA6/bETHHhd0S9/d4AXagEH9txLKL/Z
gsgEJKEtNTDKCbIBJz9aEako5aMzJlw00ZQyEj4hs3h8sYVU27ias60B
lMs+Dnn1laMAnd0sQZ1Y/3MOLN2PsyQyMXeHYg7SAOg4B7B+iLg6H6IH
iS4WMG7mKDNkt6o2B67FGrl/VmQtgAkaGQJ2WZo9alydH9wlOvw6nysi
eaX7X9vVDvIYFGKnYiRP+q74Gk82YpDbS0AqzbzV2M0XLLpRgomGGPGT
wlUlo9mXZU169tBxASc8r01LtgMj+xHrRnDc8joc8ywCpIiq60c3tICp JSyJntox4VU=
dnssec2.net.          241        IN          DNSKEY 256 3 8
AwEAAa2WWF9Jjm3khSq80fIlHS7JVhlyrNEll++ISHT3RGEFO8a8YrHs
DleSQScIziFe9x5PXd32Dl0cZDXnikA6SEp/cJRHYJ5Z0Pzy3eSYSZNV
ipoEgGzvnbnosCczxAT96fK0tUrP5nJvBpTYU4esIGNSniNgN8RaPBdr z5egvi39
dnssec2.net.          241        IN          RRSIG  DNSKEY 8 2 3600 20110310021500
20110309223000 43621 dnssec2.net.
XVj8wbjN1HPyZPfwzVY8Uf/abWARRt8qhHUoKFhuK+wPs5FRSGfBhhwz
gx14Up0uTizTLkHomqEV9Fk/5RIWqM16L8c7ixldzQb6z0XPiBoRK9/E
CbLw5P8TD1mUx1eT7716FgXklVZFZQmwPJPhXWHX0QXHiNG402s3RfCb
fZqIlgDN08FNlup/y5jN4wSWCP/tSXS4AxW/IMEiMgCfPaIVvHQLjBJd
m/B RTPNDRmBosm9StrE15RwM9PTAn8YHuG1foydOd4YSwXNAHqomJlJj
Jl0q50E2RJI92zh4YMYlxMHjoWpyHvy8exXyWpGRWhCJm/Q8PSe8WC3X BJ4b6g==
```

```
dig +dnssec -t dnskey dnssec2.net
```

```
; <<>> DiG 9.7.2-P3 <<>> +dnssec -t dnskey dnssec2.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 53944
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
```

```

;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                3600       IN          DNSKEY    257 3 8
AwEAAfTGHvzs7HNodhm/iIRKrCA6/bETHHhd0S9/d4AXagEH9txLKL/Z
gsgEJKeTnTDKCbIBJz9aEako5aMzJlw00ZQyEj4hS3h8sYVu27ias60B
lMs+Dnn1laManD0sQZ1Y/3MOLN2PsyQyMXeHYg7SAOg4B7B+iLg6H6IH
iS4WMG7mKDNKt6o2B67FGrl/VmQtgAkaGQJ2WZo9alydH9w1Ov6nysi
eaX7X9vVDvIYfGKnYiRP+q74Gk82YPDbS0AqzbzV2M0XLlpRqomGGPGT
wLUlo9mXZU169tBxAsc8r01LtgmJ+xHrRnDc8joc8ywCpIiq60c3tICp JSyJntox4VU=
dnssec2.net.                3600       IN          DNSKEY    256 3 8
AwEAAa2WWF9Jjm3khSq80f1lHS7JVhlyrNEll++ISHT3RGEF08a8YrHS
DleSQScIziFe9x5PXd32D10cZDXnikA6SEp/cJRHYSJ5Z0Pzy3eSYSNV
ipoEgGzvnbnNosCczxAT96fK0tUrP5nJvBpTYU4esIGNSniNgN8RaPBdr z5egvi39
dnssec2.net.                3600       IN          DNSKEY    256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZtZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETfHe3BiW4AdH8 54n90YSv
dnssec2.net.                3600       IN          RRSIG     DNSKEY 8 2 3600 20110310025942
20110309231442 43621 dnssec2.net.
eYmZpMFZzuF5txMCTVBv5uY0NsY5QMj7gAHBbQwX8pagsiNeZCaMzv
/4EUuCLZZXGFOYErLZ2UulqjnZ21B0HtnJoRlMciKLiddC10lqLgKwr3
K4iLqRyc81TdbbQbB318iqdefP6kFs2JZSsWcmM3FTgkdRpj/aJWe+DL
YHEy3K2d8314Mm/QxNJI41g7k1aanZBJBoOMGB3wwjCnmNNnul18AWtw
KR2HUX7gYoAlKACoXewetiKZCPH1QtFCkLdVrqYdxymwiCd2tnlx9bzV
HRVqvi8LqdUhgwyUuUVz5g9arAmwfbS6WLe24igG+wlpdIPEhTfy3TAg v8hHNg==

dig +dnssec -t ds dnssec2.net @192.101.186.214

; <<>> DiG 9.7.2-P3 <<>> +dnssec -t ds dnssec2.net @192.101.186.214
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24354
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
;; QUESTION SECTION:
;dnssec2.net.                IN          DS

;; ANSWER SECTION:
dnssec2.net.                85331     IN          DS          12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C 62C90D19
dnssec2.net.                85331     IN          DS          43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B 6050434B
dnssec2.net.                85331     IN          RRSIG     DS 8 2 86400 20110316223457
20110309222457 3980 net. xge51Lkqu9sCYCJ8i6Jyh5rUsOtFkqjgH1Sf8C4pLPuIIHzOscZy1Bpd
SF5HNVKnzX/MfTae/uDd7h5xVT0TxE3UHR5SiNW7H8tV+dfjzYdRuYH0
NmVVT6CgIkUn2J2OKVd4uu8hmJxgC1lWQ7pRH3Wu+UOfuXwFEO2V3YZ zLE=

STEP 11 AO

cat slave/dnssec2.net.zone ROLL > roll
bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +3600 -o dnssec2.net. roll
Kdnssec2.net.+008+60294
roll.signed

STEP 12
Edit hiddent master to allow transfer and notify these NS's...

STEP 13
Edit named.conf on ns3.xtcn.com and ns.dnssek.org to pull from a different hidden master

STEP 14
Increment SOA on AO from current HM.
emacs roll
bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +3600 -o dnssec2.net. roll
Kdnssec2.net.+008+60294

```

roll.signed

```
rndc reload dnssec2.net  
new HM will send out notifies and transfer new zone
```

STEP 15 WAIT

STEP 16 AO

```
cat slave/dnssec2.net.zone NORMAL > roll  
emacs roll (increment SOA Serial)  
bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +3600 -o dnssec2.net. roll  
Kdnssec2.net.+008+60294  
roll.signed
```

```
rndc reload dnssec2.net
```

STEP 17 ADMIN sends request to IANA to remove RO DS (DS1)

STEP 18 WAIT

STEP 19
RO deletes key material

Example 2

```
STEP 1 Setup own HM: AO$ dig -t soa dnssec2.net @127.0.0.1
```

```
STEP 2 Pick a time when ZSK is not rolling. RO$ dig +dnssec -t dnskey dnssec2.net
; <<>> DiG 9.7.1-P2 <<>> +dnssec -t dnskey dnssec2.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50624
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                587        IN          DNSKEY 257 3 8
AwEAAaQRiVavDSL/Z46apOi5WnI2ddTG8RicjMtLPdZkTplRPY7q7ToS
iE0dCpXaYH7t1EaeO8tpSrUybj+rImZxDjt9tKKREjmnCwsOGqGn97Nk
O5Wd3w9zG/gB4s8UzIG4NceQwolyT4yWwEAY+wjeIVhDrEDdwRurDs37
6ydOJy3gJfneabkDJcmxrlxNCKsrnGdZQOqz5qwbDEMWMJWvhMsGkPNh
AVRHgpVwHM+6snbNUQjvspjhJGJ7NPsItCcBB3n0FBDKVrO+pSKsPBHq
Y6KkECnfSc0Mho26/fmu7KTbdZiFQYO1s+rvfp1MweLJ+D02jleOWAuW eL8SuY4jel0=
dnssec2.net.                587        IN          DNSKEY 256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETFHe3BiW4AdH8 54n90YSv
dnssec2.net.                587        IN          RRSIG   DNSKEY 8 2 3600 20110317012447
20110310012447 12850 dnssec2.net.
NheqsB98jFNObIY30dZcT4puM0bV2BqZ8BjecNRCZUtjWZmQNBd7cMm+
IqAwXl2u9KxrRXem4BqJNCEDj2B0+ZCtCoJrGwZVUKai0XUJ20t6vH0
sESDizuah0mlggWGeuTnVMYaDUXGbnDioRetS8xy4zu6ocuP75poKQi4
JEBmiGwghDsJzyB3vdOrG3cRqyhjf2CYpvn7N5IQs65QLLV99tedin3
Ur6WM0aFwrOcwRGLenmqNxUa2WWLfkC6zW5JhF3ppGVF7Flvai/qXRyU
mE3fi9XzrgVWUmj74HQZ8kYauQx8vvyz9O1331yoJZ/yIgk5bcV2tR6s TS4Igg==
```

Looks like NOW until 20110317012447 is ok.

TRANSITION PERIOD = transition can start now and should be complete in less than a month

```
STEP 3 AO$ dig -t DNSKEY dnssec2.net
; <<>> DiG 9.7.1-P2 <<>> -t DNSKEY dnssec2.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34792
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                3600       IN          DNSKEY 257 3 8
AwEAAaQRiVavDSL/Z46apOi5WnI2ddTG8RicjMtLPdZkTplRPY7q7ToS
iE0dCpXaYH7t1EaeO8tpSrUybj+rImZxDjt9tKKREjmnCwsOGqGn97Nk
O5Wd3w9zG/gB4s8UzIG4NceQwolyT4yWwEAY+wjeIVhDrEDdwRurDs37
6ydOJy3gJfneabkDJcmxrlxNCKsrnGdZQOqz5qwbDEMWMJWvhMsGkPNh
AVRHgpVwHM+6snbNUQjvspjhJGJ7NPsItCcBB3n0FBDKVrO+pSKsPBHq
Y6KkECnfSc0Mho26/fmu7KTbdZiFQYO1s+rvfp1MweLJ+D02jleOWAuW eL8SuY4jel0=
dnssec2.net.                3600       IN          DNSKEY 256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETFHe3BiW4AdH8 54n90YSv

STEP 4
ROkey.key: dnssec2.net. 3600 DNSKEY 256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETFHe3BiW4AdH8 54n90YSv
AOKM$ date -u +%Y%m%d%H%M%S = 20110310231240
```



```
HSM keys with CKA_LABELs K200081 (KSK) and Z200308 (ZSK) were previously generated
AOKM$ km_no_roll dnssec2.net 20110310231240 2592000 Z200308 ROkey.key
Generating 288 key bundles from 20110310231240 to 20110409231240
Used K200081 Z200308
SHA256(20110310231240.dnssec2.net.keybundle.tar.gz)=
28bb8fca78ba3e651c601124bd926b5615005340eccf5b564c02a1d6e00dcbf6
```

STEP 5

```
Notice that start time is one second later to avoid overwriting last keybundle file name
AOKM$ km_no_roll dnssec2.net 20110310231241 2592000 Z200308
Generating 288 key bundles from 20110310231241 to 20110409231241
Used K200081 Z200308
SHA256(20110310231241.dnssec2.net.keybundle.tar.gz)=
ca3cf82a6e3d9c9795faf0e5b4de4b5904641839403bf0721926e67306536d42
```

```
AOKM$ km_check 20110310231240.dnssec2.net.keybundle.tar.gz | less
SHA256(20110310231240.dnssec2.net.keybundle.tar.gz)=
28bb8fca78ba3e651c601124bd926b5615005340eccf5b564c02a1d6e00dcbf6
=== sample file format
dnssec2.net. 3600 DNSKEY 257 3 8
AwEAAfTGHvzs7HNodhm/iIRKrCA6/bETHHhd0S9/d4AXagEH9txLKL/ZgsgEJKeTnTDKCbIBJz9aEako5aMzJlW0
ZQyEj4hS3h8sYVu27ias60BlMs+Dnn1laMAnD0sQZ1Y/3MOLN2PsyQyMXeHYg7SAOg4B7B+iLg6H6IHIS4WMG7mKD
NKt6o2B67FGrl/VmQtgAkaGQJ2WZo9alydH9w1Ovw6nysieaX7X9vVDvIYfGKnYiRP+q74Gk82YPDbS0AqzbvZ2M0
XLLpRqomGGPGTwlUlo9mXZU169tBxASc8r01LtgmJ+xHrRnDc8joc8ywCpIiq60c3tICpJSyJntox4VU=
; CKA_LABEL K200081 TAG 43621
dnssec2.net. 3600 DNSKEY 256 3 8
AwEAAaHiTfzAEiRnN4K6A2UQa/UWqYgMrM0zInr23ghJBTt0uLoKfeX/RVlpgaUCi6iMByyXQsWpvef/W7eMeFPo
fhrTdz2zeC3uNrwhBEtuBg8Ce3USA9csqciuOKngyD7Pn4RiAW7O6Q0od2RZ5tGT+R7TN3Cly+RPuFaG3HNHkiV
; CKA_LABEL Z200308 TAG 6510
dnssec2.net. 3600 DNSKEY 256 3 8 AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpWLC3
myFLY50NohOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETFHe3BiW4AdH8 54n90YSv
; external keys from FILE ROkey.key
dnssec2.net. 3600 IN RRSIG DNSKEY 8 2 3600 20110311025740 20110310231240 43621
dnssec2.net.
PXG0e7K63D08//jRS3qiJ5xSRVj+7WfHMX5EtiB2PD31TZWwAh2vnhWvXdzct6MtXsmgGFhb8pDkLROjxYlc7Mtzv
8j3wA5UzFtzUTlSxxPj67Lpp8vukgEP2PR9F/Jj70A72b4Iw89uaT7Pj1hbdhe3rfnWzUSY1rHgaSn67c07ernsQS
bwUZxGtA3xS+4XDmXTCqPfhiv3oggrIM4xQqeh7bJKr00Unj+JBci+eZFC3vJBzdNRlfaTlNoIPtDp74M5V8vZYsc
ByisdbpLLYRAoxBfAMBT+PoTFKqQdv0RXD3B7RXrWYTiFx6IM9DchsJyALmzinZQspcSIS5WIAQ==
; CKA_LABEL K200081:aep.hsmconfig:1 tag:43621 20110310231952
; dnssec2.net. IN DS 43621 8 1 E057E6D88B681F2A409D5303C70614CA8776FBC2
; dnssec2.net. IN DS 43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B6050434B
; USE:Z200308 RSASHA256 13500
=== 20110310231240.rrsig.kb 20110310231240 20110311025740
; CKA_LABEL K200081 TAG 43621
; CKA_LABEL Z200308 TAG 6510
; CKA_LABEL K200081:aep.hsmconfig:1 tag:43621 20110310231952
; USE:Z200308 RSASHA256 13500
KSK 43621
ZSK 6510
ZSK 60294
KSK 43621 RRSIG validated
```

STEP 6 From above DS2 and AOzsk:

```
dnssec2.net. IN DS 43621 8 1 E057E6D88B681F2A409D5303C70614CA8776FBC2
dnssec2.net. IN DS 43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B6050434B
```

AOkey.key:

```
dnssec2.net. 3600 DNSKEY 256 3 8
AwEAAaHiTfzAEiRnN4K6A2UQa/UWqYgMrM0zInr23ghJBTt0uLoKfeX/RVlpgaUCi6iMByyXQsWpvef/W7eMeFPo
fhrTdz2zeC3uNrwhBEtuBg8Ce3USA9csqciuOKngyD7Pn4RiAW7O6Q0od2RZ5tGT+R7TN3Cly+RPuFaG3HNHkiV
```

STEP 7

```
RO$ cat dnssec2.net.zone Kdnssec2.net.+008+12850.key Kdnssec2.net.+008+60294.key
AOkey.key > transition
RO$ emacs transition (increment SOA serial)
```

STEP 8

```

RO$ bind-9.7.3/bin/dnssec/dnssec-signzone -A -3 - -x -s now -e +2592000 -o dnssec2.net.
transition Kdnssec2.net.+008+60294 Kdnssec2.net.+008+12850
dnssec-signzone: warning: transition:24: using RFC1035 TTL semantics
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                    ZSKs: 0 active, 2 present, 0 revoked

transition.signed
RO$ cp -p transition.signed master/
RO$ bind-9.7.3/bin/rndc/rndc -c rndc.conf reload
server reload successful
RO$ dig -t dnskey dnssec2.net @127.0.0.1
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.1-P2 <<>> -t dnskey dnssec2.net @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 15687
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                3600       IN          DNSKEY  256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZIZL0AfgRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtqNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRjQv7rgpMrpwLC3
myFLY50NoHmHxBcjdq+7x4hw3FoMxbtU1emxOeK5KETfHe3BiW4AdH8 54n90YSv
dnssec2.net.                3600       IN          DNSKEY  257 3 8
AwEAAaQRiVavDSL/Z46apOi5WnI2ddTG8RicjMtLPdZkTplRPY7q7ToS
iE0dCpXaYH7t1Eae08tpSrUybj+rLmZxDjt9tKKREjmnCwsOGqGn97Nk
O5Wd3w9zG/gB4s8UzIG4NceQwolyT4yWwEAY+wjeIVhDrEDdwRurDs37
6y0QJy3gJfneabkDJcmxrLxNCKsrnGdZ0Qqz5qwbDEMWMJWvhMsGkPNh
AVRHgpVwHM+6snbNUQjvspjhJGJ7NPsItCcBB3n0FBDKvRo+pSKsPBHq
Y6KkECNFSc0Mho26/fmu7KTBDziFQYOls+rvfp1MweLJ+D02jleOWAuW eL8SuY4jel0=
dnssec2.net.                3600       IN          DNSKEY  256 3 8
AwEAAaHiTfzAEiRnN4K6A2Uqa/UWqYgMrM0zInr23ghJBTTt0uLoKfeX
/RVlpgaUCi6iMByyXQsWpvef/W7eMeFPofhrTdz2zeC3uNrwhBetuBg8
Ce3USA9csqciuOKngyD7Pn4RiAW706Q0od2RZ5tGT+R7TN3Cly+RPuFa G3HNHkiV

```

STEP 9

```

ADMIN sends request to IANA to add to DS list
dnssec2.net. IN DS 43621 8 2
6832150BBCAAB6872FEbb60CE59A2D2516F36D90CD7A8B3E856BB37B6050434B

```

STEP 10 WAIT

```

$ dig -t dnskey dnssec2.net @192.101.186.214

; <<>> DiG 9.7.1-P2 <<>> -t dnskey dnssec2.net @192.101.186.214
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 51780
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                1288       IN          DNSKEY  257 3 8
AwEAAaQRiVavDSL/Z46apOi5WnI2ddTG8RicjMtLPdZkTplRPY7q7ToS
iE0dCpXaYH7t1Eae08tpSrUybj+rLmZxDjt9tKKREjmnCwsOGqGn97Nk
O5Wd3w9zG/gB4s8UzIG4NceQwolyT4yWwEAY+wjeIVhDrEDdwRurDs37
6y0QJy3gJfneabkDJcmxrLxNCKsrnGdZ0Qqz5qwbDEMWMJWvhMsGkPNh
AVRHgpVwHM+6snbNUQjvspjhJGJ7NPsItCcBB3n0FBDKvRo+pSKsPBHq
Y6KkECNFSc0Mho26/fmu7KTBDziFQYOls+rvfp1MweLJ+D02jleOWAuW eL8SuY4jel0=

```

```

dnssec2.net.          1288      IN          DNSKEY      256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtgNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdg+7x4hw3FoMxbtUlemxOeK5KETfHe3BiW4AdH8 54n90YSv

```

Only need to wait a few hours for DNSKEY. BUT.....

```

$ dig -t ds dnssec2.net @c.gtld-servers.net.

; <<>> DiG 9.7.1-P2 <<>> -t ds dnssec2.net @c.gtld-servers.net.
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 10260
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnssec2.net.                IN          DS

;; ANSWER SECTION:
dnssec2.net.                86400      IN          DS          12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C 62C90D19
dnssec2.net.                86400      IN          DS          43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B 6050434B

```

Must wait for at least two days (2x86400) after seeing this.

STEP 11

Copy 20110310231240.dnssec2.net.keybundle.tar.gz to signer to automatically pickup and use new keybundles

STEP 12

```

AO$ dig -t ns dnssec2.net

; <<>> DiG 9.7.1-P2 <<>> -t ns dnssec2.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 34374
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dnssec2.net.                IN          NS

;; ANSWER SECTION:
dnssec2.net.                3600      IN          NS          ns3.xtcn.com.
dnssec2.net.                3600      IN          NS          ns.dnssek.org.

```

```

AO$ cat confs/dnssec2.net.signed
zone "dnssec2.net." IN {
  type master;
  file "master/dnssec2.net.zone.signed";
  max-journal-size 1M;
  also-notify {
    ... // ns3.xtcn.com and ns.dnssek.org backend IP addresses
  };
  allow-transfer {
    ... // ns3.xtcn.com and ns.dnssek.org backend IP addresses
  };
};

```

STEP 13

```

zone "dnssec2.net." IN {
  type slave;
  file "slave/dnssec2.net.zone";
  masters { 128.107.191.115; };
  max-journal-size 1M;
};

```

```
$HOME/named/bind-9.7.2-P3/bin/rndc/rndc -c $HOME/named/rndc.conf reload
```

```
STEP 14
```

```
dig -t dnskey dnssec2.net @192.101.186.214
;; Truncated, retrying in TCP mode.
```

```
;<<>> DiG 9.7.1-P2 <<>> -t dnskey dnssec2.net @192.101.186.214
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8166
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
;dnssec2.net.                IN          DNSKEY
```

```
;; ANSWER SECTION:
```

```
dnssec2.net.                1778       IN          DNSKEY 256 3 8
AwEAAaHiTfzAEiRNn4K6A2Uqa/UWqYgMrM0zInr23ghJBTTt0uLoKfeX
/RVlpgauCi6iMByyXQsWpvef/W7eMeFPofhrTdz2zeC3uNrwhBEtuBg8
Ce3USA9cscqciuOKngyD7Pn4RiAW7O6Q0od2RZ5tGT+R7TN3Cly+RPuFa G3HNHKiV
dnssec2.net.                1778       IN          DNSKEY 256 3 8
AwEAAcGCrJQ5WsuAbU2RXcZiZL0AfgRL5LsD9PT5bu5yHFdVE9xlawgb
J0nfOtgqNPFKsTUytsz+RUF5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50NohOmHxBCjDq+7x4hw3FoMxbtUlemxOeK5KETfHe3BiW4AdH8 54n90YSv
dnssec2.net.                1778       IN          DNSKEY 257 3 8
AwEAAaQRiVavDSL/Z46apOi5WnI2ddTG8RicjMtLPdZkTplRPY7q7ToS
iE0dCpXaYH7t1EaeO8tpSrUybj+rLmZxDjt9tKKREjmnCwsOGqGn97Nk
O5Wd3w9zG/gB4s8UZIG4NceQwolyT4yWwEAY+wjeIVhDrEdwRurDs37
6yd0Jy3gJfneabkDJcmxrLxNCksrnGdZ0Qqz5qwbDEMWMJWvhMsGkPNh
AVRHgpVwHM+6snbNUQjvspjhJGJ7NPsItCcBB3n0FBDKvRo+pSKsPBHq
Y6KkECNFSc0Mho26/fmu7KTbdZiFQYOls+rvfp1MweLJ+D02jleOWAuW eL8SuY4jel0=
```

```
;; Query time: 1 msec
;; SERVER: 192.101.186.214#53(192.101.186.214)
;; WHEN: Thu Mar 10 17:29:01 2011
;; MSG SIZE rcvd: 601
```

```
RO$ cat zones/dnssec2.net/lastsignedserial
2010110484
```

```
RO$ $ dig +dnssec -t soa dnssec2.net @127.0.0.1
```

```
;<<>> DiG 9.7.1-P2 <<>> +dnssec -t soa dnssec2.net @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43322
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags: do; udp: 4096
```

```
;; QUESTION SECTION:
```

```
;dnssec2.net.                IN          SOA
```

```
;; ANSWER SECTION:
```

```
dnssec2.net.                3600       IN          SOA      ns.dnssek.org. postmaster.dnssec2.net.
2010110484 1800 1800 7200 3600
dnssec2.net.                3600       IN          RRSIG   SOA 8 2 3600 20110311051043
20110310230000 6510 dnssec2.net. Dvi4aAcXptkSE3+wu8tZ+Ms5YXBSKmCYlxsCvkdYlTwz7je2WiZ//DgC
iiQFDA+hsgF6ZwZpAsaxYpokbQ0JWx9C/9isfdzoy9sES0103YE2k4ox
j/iPQ7/tCMKausSaOgb04Kxea5nZuuHK5p/Vc0arnAMHZmSWjq36AaL3 9Ik=
```

```
RO$ dig +dnssec -t dnskey dnssec2.net @127.0.0.1
```

```
;<<>> DiG 9.7.1-P2 <<>> +dnssec -t dnskey dnssec2.net @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25393
```

```

;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                3600       IN          DNSKEY    256 3 8
AwEAACGCrJQ5WsuAbU2RXcZiZL0AfGRL5LsD9PT5bu5yHfDVE9xlawgb
J0nfOtgNPFKsTUytsz+RUFc5z/tGbEa6A8dOAV5TSRJqv7rgpMrpwLC3
myFLY50N0hOmHxBCjdq+7x4hw3FoMxbtU1emxOeK5KETfHe3BiW4AdH8 54n90YSv
dnssec2.net.                3600       IN          DNSKEY    257 3 8
AwEAafTGHvzs7HnOdhm/iIRKrcA6/bETHHhd0S9/d4AXagEH9txLKL/Z
gsqEJKETnTDKChIBJz9aEako5aMzJlw00ZQyEj4hS3h8sYVu27ias60B
lMs+Dnn1laManD0sQZ1Y/3MOLN2PsyQyMXeHYg7SAOg4B7B+iLg6H6IH
iS4WMG7mKDNKt6o2B67FGrl/VmQtgAkaGQJ2Wzo9alydH9w1Ovw6nysi
eaX7X9vVDvIyFGKnYiRP+q74Gk82YPDbS0AqzbzV2M0XLLpRqomGGPGT
wLUlo9mXZUL69tBxASc8r01LtgmJ+xHrRnDc8joc8ywCpIiq60c3tICp JSyJntox4VU=
dnssec2.net.                3600       IN          DNSKEY    256 3 8
AwEAAaHiTfzAEiRnN4K6A2Uqa/UWqYgMrM0zInr23ghJBTTt0uLoKfEX
/RVlpgaUCi6iMByyXQsWpvef/W7eMeFPofhrTdz2zeC3uNrwhBETuBg8
Ce3USA9csqciuoKngyD7Pn4RiAW7O6Q0od2RZ5tGT+R7TN3Cly+RPuFa G3HNHkiV
dnssec2.net.                3600       IN          RRSIG     DNSKEY 8 2 3600 20110311025740
20110310231240 43621 dnssec2.net.
PXG0e7K63D08//jRS3qijSxSRVj+7wfHMX5Etib2PD31TZWwAh2vnhWv
Xdzct6MtXsmgGFhb8pDkLRojxYlc7Mtzv8j3wA5UzFtzUT1sxxPj67Lp
p8vukgEP2PR9F/Jj70A72b4Iw89uaT7Pj1hbdhe3rfnWzUSY1rHgaSn6
7c07ernsQSBwUZxGtA3xS+4XDmXTcqpFhiv3oggRIM4xQQeh7bJKr00U
nj+JBCI+eZFC3vJBzdNrlfAt1NoIPtDp74M5V8vZYscByisdbpLLYRAo
xBfAMBT+PoTfKqQdvORXD3B7RXrWYTiFx6IM9DchsJyALmzinZQspcSI S5WIAQ==

```

STEP 15 WAIT

```
$ dig +dnssec -t soa dnssec2.net @192.101.186.214
```

```

; <<>> DiG 9.7.1-P2 <<>> +dnssec -t soa dnssec2.net @192.101.186.214
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 63394
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
;; QUESTION SECTION:
;dnssec2.net.                IN          SOA

;; ANSWER SECTION:
dnssec2.net.                1503       IN          SOA       ns3.xtcn.com. postmaster.dnssec2.net.
2010110448 1800 1800 7200 3600
dnssec2.net.                1503       IN          RRSIG     SOA 8 2 3600 20110317233749
20110310233749 60294 dnssec2.net.
H19X9px0uK4kZvDbA+3ZYHfL7eXSCme4GcdPxMdutmtzpzRzbeqf9buG
jQRUhJDFmX1/WgCKLTAtSAuiWiPD9xjgV566GVy9ylu3YdepXf6vI33k
E3qcTFV1Gq7vhj292V2fJBcp7sI7g5+6/Y/UCFcP9PdW20WpB3Flfmlh S/s=

```

Twice the TTL (two hours) should do it

STEP 16

```

Copy 20110310231241.dnssec2.net.keybundle.tar.gz to signer to automatically pickup and
use new keybundles
tools/dnsxnotifytest 127.0.0.1 dnssec2.net -2

```

```
AO$ dig +dnssec -t dnskey dnssec2.net @127.0.0.1
```

```

; <<>> DiG 9.7.1-P2 <<>> +dnssec -t dnskey dnssec2.net @127.0.0.1
;; global options: +cmd

```

```

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51905
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec2.net.                IN          DNSKEY

;; ANSWER SECTION:
dnssec2.net.                3600       IN          DNSKEY  257 3 8
AwEAAfTGHvzs7HNodhm/iIRKrCA6/bETHHhd0S9/d4AXagEH9txLKL/Z
gsgEJKeTnTDKChIBJz9aEako5aMzJlw0OZQyEj4hS3h8sYVu27ias60B
lMs+Dnn1laMAnD0sQZ1Y/3MOLN2PsyQyMXeHYg7SAOg4B7B+iLg6H6IH
iS4WMG7mKDNKt6o2B67FGrl/VmQtgAkaGQJ2WZo9alydH9w1Ovw6nysi
eaX7X9vVDvIYfGKnYiRP+q74Gk82YPDbS0AqzbzV2M0XLLpRqomGGPGT
wLUlo9mXZUL69tBxAsc8r01LtgmJ+xHrRnDc8joc8ywCpIiq60c3tICp JSyJntox4VU=
dnssec2.net.                3600       IN          DNSKEY  256 3 8
AwEAAaHiTfzAEiRnN4K6A2UQa/UWqYgMrM0zInr23ghJBTt0uLoKfeX
/RVlpgaUCi6iMByyXQsWpvef/W7eMeFPofhrTdz2zeC3uNrwhBEtuBg8
Ce3USA9csqciUOKngyD7Pn4RiAW7O6Q0od2RZ5tGT+R7TN3Cly+RPuFa G3HNHkiV
dnssec2.net.                3600       IN          RRSIG   DNSKEY  8 2 3600 20110311052741
20110311014241 43621 dnssec2.net.
eG5quqrWyBHtOOEEV4DUs5LLbRMJ1Xz7Q5FUitDFYClQsdK+LUX57UWO
mTePguCwv1WtUqEi346gtWOrwZFlDLbEoi6WwCFsQ9luRhF6ulzcf8dn
a835Pzwhv7ET2gch7LEUXyabZOazbBx2c4D30TeXsLubzfXkJdGXrgoI
Xhu/AHyAQ1ci9+rA5gsNM+bRu/DV00US0jHCpp86hzurcYdrREvYiR/
0AWE3NVHwdByTSwvCvpzwTasJBN25UbPbnsYWgEQcTUIzehTsa j5Psq
3VT7BS0IWGI8gKpRU5cSPetyJQOkWlwAPs2hWz+TT9qu3CmbGTmJE7et vTgLnA==

```

STEP 17

```

$ dig +dnssec -t ds dnssec2.net @192.101.186.214

; <<>> DiG 9.7.1-P2 <<>> +dnssec -t ds dnssec2.net @192.101.186.214
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20044
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1024
;; QUESTION SECTION:
;dnssec2.net.                IN          DS

;; ANSWER SECTION:
dnssec2.net.                84092     IN          DS       12850 8 2
BA8F0D511DA81EF57F5D8E85EDA62062DA334EE330E0F5629AF6887C 62C90D19
dnssec2.net.                84092     IN          DS       43621 8 2
6832150BBCAAB6872FEBB60CE59A2D2516F36D90CD7A8B3E856BB37B 6050434B

```

ADMIN sends request to IANA to REMOVE old DS (tag=12850) from list

STEP 18 WAIT

```

$ dig -t ds dnssec2.net @c.gtld-servers.net.

; <<>> DiG 9.7.1-P2 <<>> -t ds dnssec2.net @c.gtld-servers.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5668
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 12
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnssec2.net.                IN          DS

;; ANSWER SECTION:

```

```
dnssec2.net.      86400  IN      DS      43621 8 2  
6832150BBCAAB6872FE6B60CE59A2D2516F36D90CD7A8B3E856BB37B 6050434B
```

But must wait another two days for changes in root to trickle out...

STEP 19 COMPLETE
AO can now manage keys as they wish