DNSSEC DEPLOYMENT CHALLENGES

Abdalmonem Galila / ICANN-60 / 01-Nov-2017

.masr IDN ccTLD (.مصر)

ICANN 60
ANNUAL GENERAL
ABU DHABI
28 October–3 November 2017

CHALLENGES BEFORE DEPLOYMENT

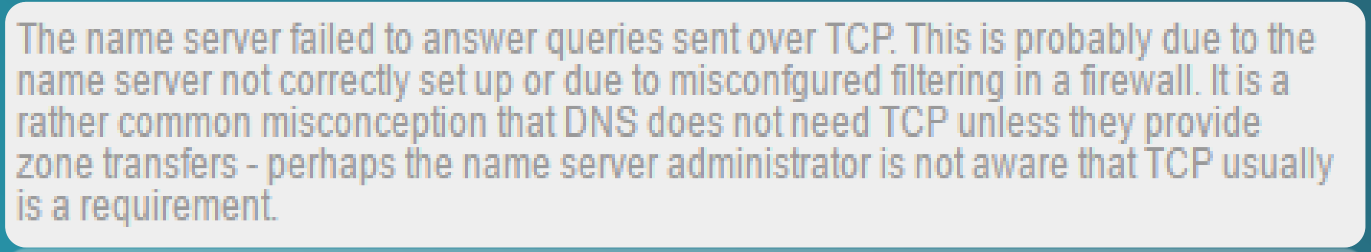
- What is DNSSEC !!
- How DNSSEC works !!
- From Where should we start deploying DNSSEC !!
- Keys attributes that should be used for signing !!
- Do we have to do changes to registry system before DNSSEC deployment !!
- DNSSEC Secures the communication between master & slaves DNS's or not
- Firewall should be well prepared before taking DNSSEC into production.

CHALLENGES AFTER DEPLOYMENT

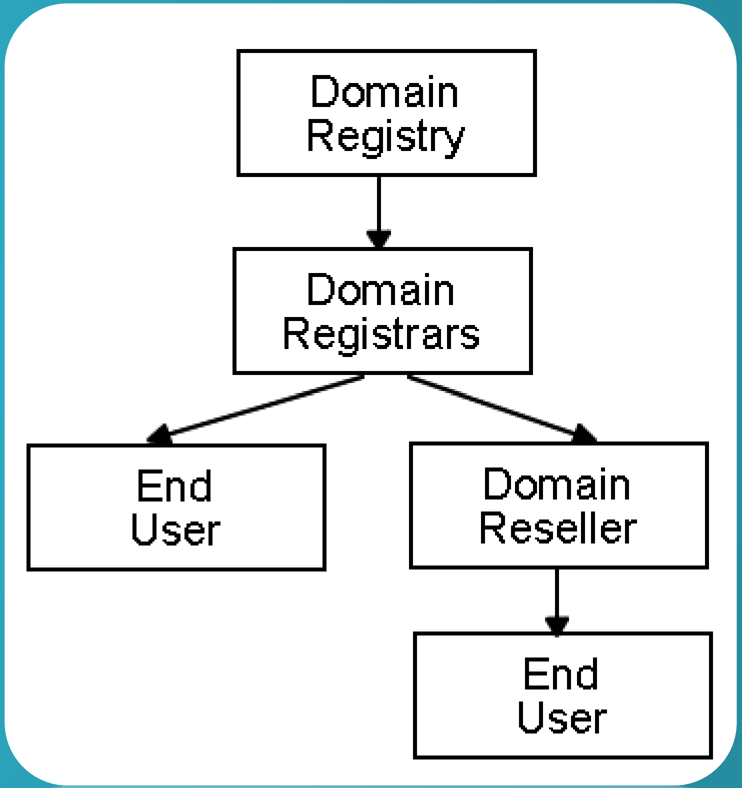
- What is next after deployment
- How to keep our domains active all the time
- Domain re-signing automation
- How often do we have to roll keys
- How to spread the word of DNSSEC to Our Registrars

CHALLENGES AFTER DEPLOYMENT3

- ❑ One of .masr DNS servers does not respond to TCP queries.
- ❑ Response size exceeded 1500 if using both KSK and ZSK for signing
- ❑ DNSSEC also introduces new operational tasks such as rolling the keys and resigning the zone. Such tasks must be performed at regular intervals.
- ❑ ISP DNSSEC validation off



The name server failed to answer queries sent over TCP. This is probably due to the name server not correctly set up or due to misconfgured filtering in a firewall. It is a rather common misconception that DNS does not need TCP unless they provide zone transfers - perhaps the name server administrator is not aware that TCP usually is a requirement.



Domain Registry

Domain Registrars

End User

Domain Reseller

End User

CHALLENGES AS A REGISTRAR1

We have 4 registrars , 3 of them are an ISP

- ❑ Our customers do not have idea's about DNSSEC
- ❑ Hard.
- ❑ System is stable so why we have to change
  - ❖ More time required to resolve domain name

CHALLENGES AS A REGISTRAR$_2$

- Domains with invalid signatures will be blocked.
- Attacks on the DNS are too rare to raise concerns
- We have many attacks and we can mitigate it
- Registrants do not have an idea about DNSSEC
- No enough staff to monitor & troubleshoot DNSSEC

DNSSEC Zone *Signing Automation

Script For **.masr (مصر.)**

Perl

SCRIPT STRUCTURE

Script Initialization Inputs

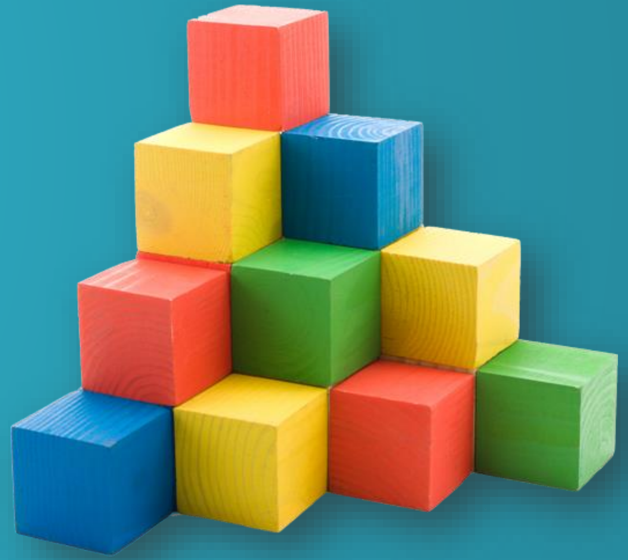
Apply Checks

Unzip Registry Generated Zones

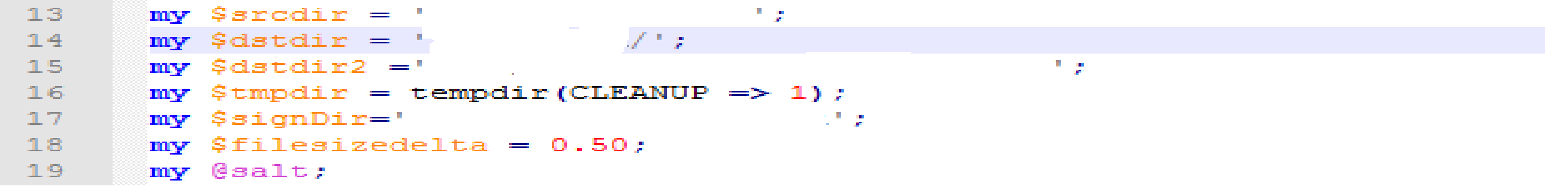
Loop Zones

Sign Zones

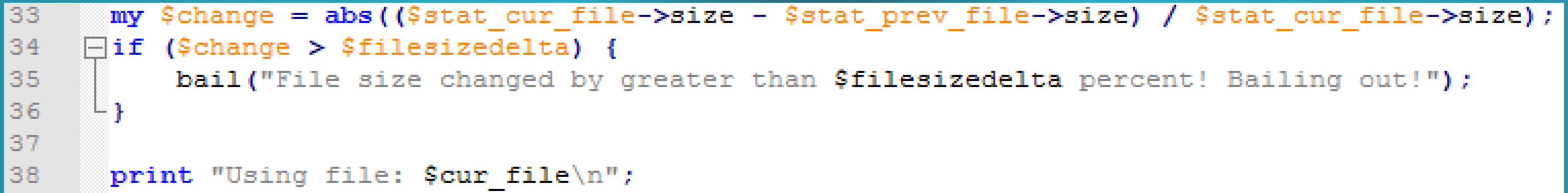
RNDC Reload



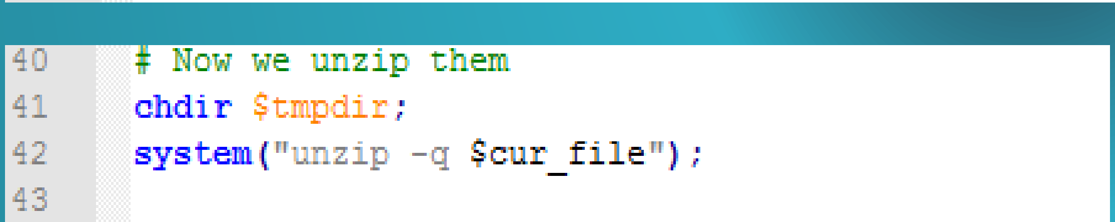
SCRIPT ELEMENTS SAMPLES



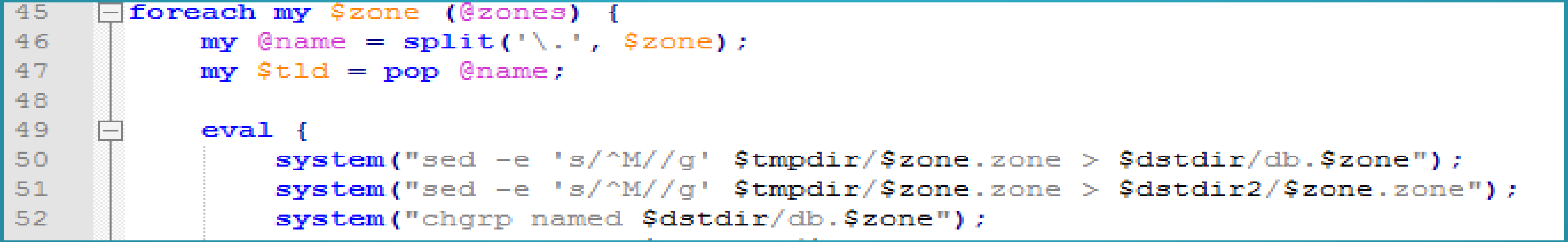
```
my $srcdir = '                              ';
my $dstdir = '                    /';
my $dstdir2 ='                                          ';
my $tmpdir = tempdir(CLEANUP => 1);
my $signDir='                        ';
my $filesizedelta = 0.50;
my @salt;
```



```
my $change = abs(($stat_cur_file->size - $stat_prev_file->size) / $stat_cur_file->size);
if ($change > $filesizedelta) {
    bail("File size changed by greater than $filesizedelta percent! Bailing out!");
}

print "Using file: $cur_file\n";
```

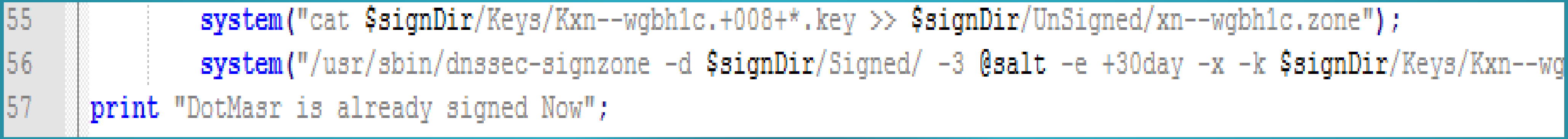


```
# Now we unzip them
chdir $tmpdir;
system("unzip -q $cur_file");

```

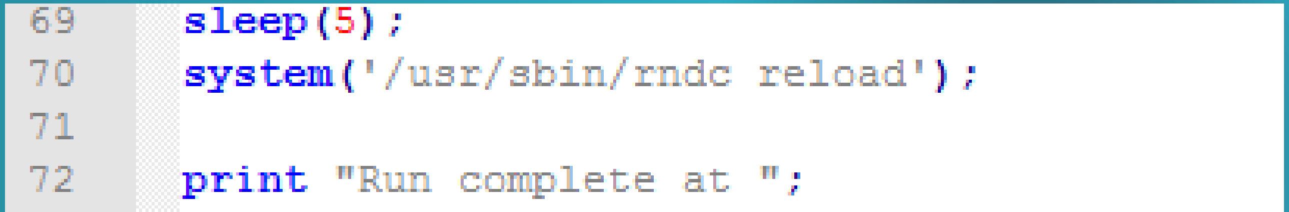


```
foreach my $zone (@zones) {
    my @name = split('\.', $zone);
    my $tld = pop @name;

    eval {
        system("sed -e 's/^M//g' $tmpdir/$zone.zone > $dstdir/db.$zone");
        system("sed -e 's/^M//g' $tmpdir/$zone.zone > $dstdir2/$zone.zone");
        system("chgrp named $dstdir/db.$zone");
```

SCRIPT ELEMENTS SAMPLES



```
        system("cat $signDir/Keys/Kxn--wgbh1c.+008+*.key >> $signDir/UnSigned/xn--wgbh1c.zone");
        system("/usr/sbin/dnssec-signzone -d $signDir/Signed/ -3 @salt -e +30day -x -k $signDir/Keys/Kxn--wg
print "DotMasr is already signed Now";
```



```
sleep(5);
system('/usr/sbin/rndc reload');

print "Run complete at ";
```

ICANN 60 ANNUAL GENERAL

ABU DHABI

28 October–3 November 2017