30/10/2007

SIGNING THE ROOT ZONE
Olivier's investigations

* Although there is no real dnssec deployment in the ccTLD community at this stage, some operators publish already signed zones (.se, .pr, .bg..);

* IANA publishes experimental signed root zone on the web
→ https://ns.iana.org/dnssec/status.html
as well as on a dns server:
→ ns.iana.org

WHAT DOES REALLY MEAN "TO SIGN THE ROOT ZONE"?

* Let's look at a signed DNS response :

```
$ dig fr ns @A.ROOT-SERVERS.NET +dnssec +multiline
$ dig fr ns @NS.IANA.ORG +dnssec +multiline
```

INTERACTION WITH END USERS :

* trust anchor and DNSKEY publication:

```
$ dig . dnskey @a.root-servers.net +multiline +dnssec
$ dig . dnskey @ns.iana.org +multiline +dnssec
```

→ DNS users on the internet will need to copy the "." DNSKEY and paste it in their resolver as a trust anchor for "."

? Why are there two root KSK in the testbed ?

? Would I need to regularly update the root KSK(s) introduced in my resolver ?

? If yes, how would I be adviced I need to do so ? By who ? What would be the frequency ?

? As a user (aka a DNS operator), which guaranty will I really get once I have configured my resolver to use the root KSK(s) as a trust anchor(s) for . ?

? Under which conditions would I trust the . key(s) that I have "copy and pasted" ?

? Under which conditions would the cc community trust root KSK published as a trust anchor for the top of the public DNS tree ?

* AVOID HACKING: GET A CERTIFIED KSK DNSKEY

see https://ns.iana.org/dnssec/status.html

→ copy a "certified" . DNSKEY, check it and paste it in your resolver as a trust anchor for .

? who certifies the root KSK for publication ? Under which conditions would I trust these people ?

ROOT ZONE MANAGEMENT AND SIGNING PROCESS:

* Key management and root zone file production:

? Who does operate the root KSK(s)? How ?

? Who does operate the root ZSK(s)? How ?

? Is the key infrastructure and key management procedure secured ?

? Who sign the root zone, using which procedures ?

? What are the rollover frequencies (KSK and ZSK) ?

? Which plan in case of key corruption ?

INTERACTIONS WITH ccTLDs:

* Build a CHAIN OF TRUST :

Let's find another signed zone:

```
$ dig se ns @ns.iana.org +dnssec +multiline
$ dig se dnskey @a.ns.se +dnssec +multiline
$ dig se DS @ns.iana.org +dnssec +multiline
```

→ Will DNS user need to copy and paste .se KSK in their resolver and to declare it as a trust anchor for .se ? NO IF:

* they have configure a trust anchor for .
* DS for ".se" are introduced and signed in the root zone (with a key that I know)
* DS are published by root name servers

→ ONCE THIS IS DONE, MY RESOLVER CAN COLLECT SECURELY THE .se KEY OVER DNS QUERIES

? ccTLD keys need to be collected for DS inclusion in the root zone. Some of them have already this information present in the IANA test plateform: who should gather, introduce and sign those DS ? Using which procedures ?

IN SUMMARY

WHEREAS THE COMPLEXITY OF PROCESSES AND VARIOUS OPERATIONS THAT NEED TO BE PERFORMED TO DEPLOY AND PUBLISH A USABLE SIGNED ROOT ZONE "WHO SIGN THE ROOT" IS NOT REALLY A VALID QUESTION AND SHOULD CLARIFIED :

- WHO WOULD CERTIFY (SIGN) THE PUBLIC ROOT KEY (KSK) FOR DISSEMINATION ? WHICH CERTIFICATION MECANISM (PGP?) ? WHICH CHANEL(s) WOULD BE USED FOR USER INFORMATION AND INTERACTION ?

- WHO WOULD OPERATE AND USES THE DNSKEYS FOR ROOT ZONE SIGNATURE ?

- WHO WOULD COLLECT CCTLD PUBLIC KEYS FOR DS INTRODUCTION IN THE ROOT ZONE ? HOW WOULD THIS CHANEL BE SECURED ?

ADDITIONAL QUESTIONS "on the flight":

About KSK publication and interactions with users:

* As the root zone is at the top of the DNS tree, rather than introducing the root key as a trust anchor for ".", wouldn't it be possible to publish the root key DS information along with the list of root servers that already need to be collected by users ? → "hint file" here: ftp://ftp.internic.net/domain/

? who maintains the hint file, and more generally the official domain repository on ftp.internic.net ? Who guaranty the relevancy, the authenticity and the integrity security of these critical information today ? How ?

Other considerations

? What would be the incidence of a coexistance between signed and unsigned spaces at the at highest level of the public DNS tree ?

? What would be the incidence of eterogeneous practises for dnssec management ? Isn't there a risk for lack of readibility about DNS service ?

? Aren't there any side effects and new risks to be expected deploying this technology (Ddos amplification, accessibility problems -size of the paquets-, what about dns cache)?

? What is the demand for DNSsec ? Who ask for it ? What for ?

? Will DNSsec strengthen the DNS accountability ?