Managing the Root KSK Rollover, Step by Step for Operators

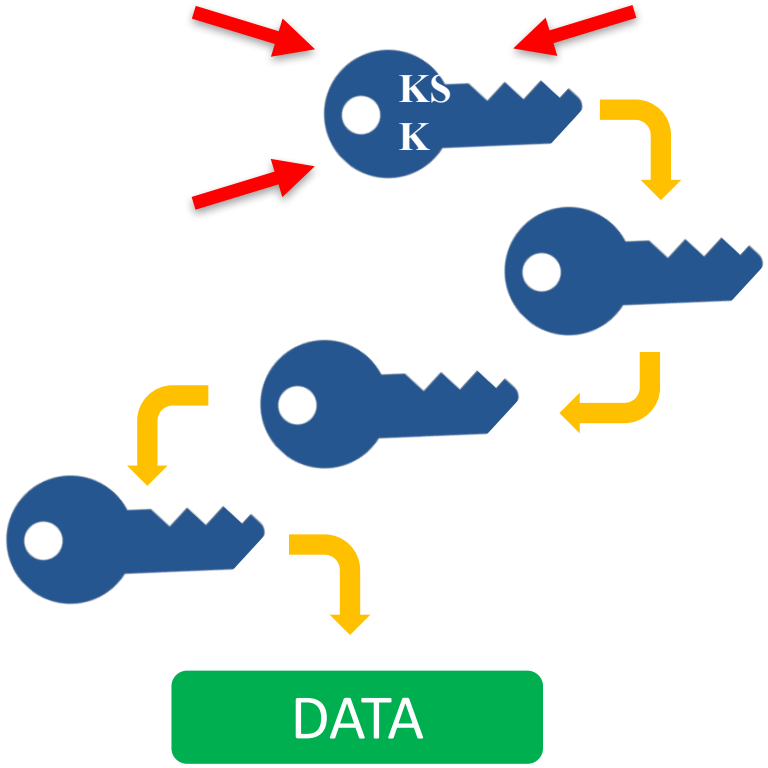
Quickly spun by Edward.Lewis @ ICANN.ORG
Changed-by: carlos @ lacnic.net
LACNIC 27 – Foz do Iguassu

Agenda

- What is the problem here ?
- Some tools to check operation
- Notes for BIND
- Notes for unbound

The Root Zone DNSSEC KSK

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy
- Public portion of the KSK is configuration parameter in DNS validating revolvers



Rollover of the Root Zone DNSSEC KSK

- **There has been one functional, operational Root Zone DNSSEC KSK**
  - Called "KSK-2010"
  - Since 2010, nothing before that
- **A new KSK will be put into production later this year**
  - Call it "KSK-2017"
  - An orderly succession for continued smooth operations
- **Operators of DNSSEC recursive servers may have some work**
  - As little as review configurations
  - As much as install KSK-2017

Important Milestones

Event	Date
Creation of KSK-2017	~~October 27, 2016~~
Production Qualified	~~February 2, 2017~~
Out-of-DNS-band Publication	Now, onwards
In-band (*Automated Updates*) Publication	July 11, 2017 and onwards
Sign (Production Use)	October 11, 2017 and onwards
Revoke KSK-2010	January 11, 2018
Remove KSK-2010 from systems	Dates TBD, 2018

High-level steps

- Prepare yourself
  - Learn and document your plan
- Survey your network
  - Learn what you have to manage
- Test your network
  - Verify your expectations
- Set up monitoring
  - Impossible to manage what is not monitored
- Do what needs to be done

Prepare Yourself

- ICANN documentation
  - It starts here:**https://www.icann.org/resources/pages/ksk-rollover**
  - **And here: http://www.lacnic.net/web/lacnic/key-signing-key**
  - Do you use DNSSEC validation? Even if no, there might be side effects like IP fragmentation
  - Document your plans, know what you expect to expect and who to contact if help is needed

- Mailing lists for those interested
  - **https://mm.icann.org/mailman/listinfo/ksk-rollover**
  - **https://mm.icann.org/mailman/listinfo/root-dnssec-announce**

Survey Your Network

- Discover whether any servers are performing DNSSEC validation
  - **A previous administrator may have turned it on**
- Discover whether servers are running on IPv6
  - **IPv6 fragmentation is different from IPv4 fragmentation**
- Discover what DNS software is in use, what version and how to re-configure it
  - DNS is "buried" in OS and application releases, not as obvious as it used to be
  - Version is important (again) as tools for managing DNSSEC trust anchors get exercised

What versions?

- Newer versions are always better than older versions (minus bugs)
  - Functionality is added, improved tooling
  - Newer versions are not a MUST, recent older versions also work
  - The Automated Updates code has been stable for a few years, it's the debugging tools that improve
- Mind the age of configuration files
  - Software updates may just replace binaries, make sure your hand-crafted configurations make use of new options and features
  - What is "old" depends on the software in use
  - This is chiefly a BIND concern due to its long history in operations

Test Yourself

- Check for the ability to exchange large DNS messages:
  - **http://keysizetest.verisignlabs.com/**
  - **https://www.dns-oarc.net/oarc/services/replysizetest**
- Check whether your DNS tools can follow Automated Updates
  - **https://automated-ksk-test.research.icann.org/**

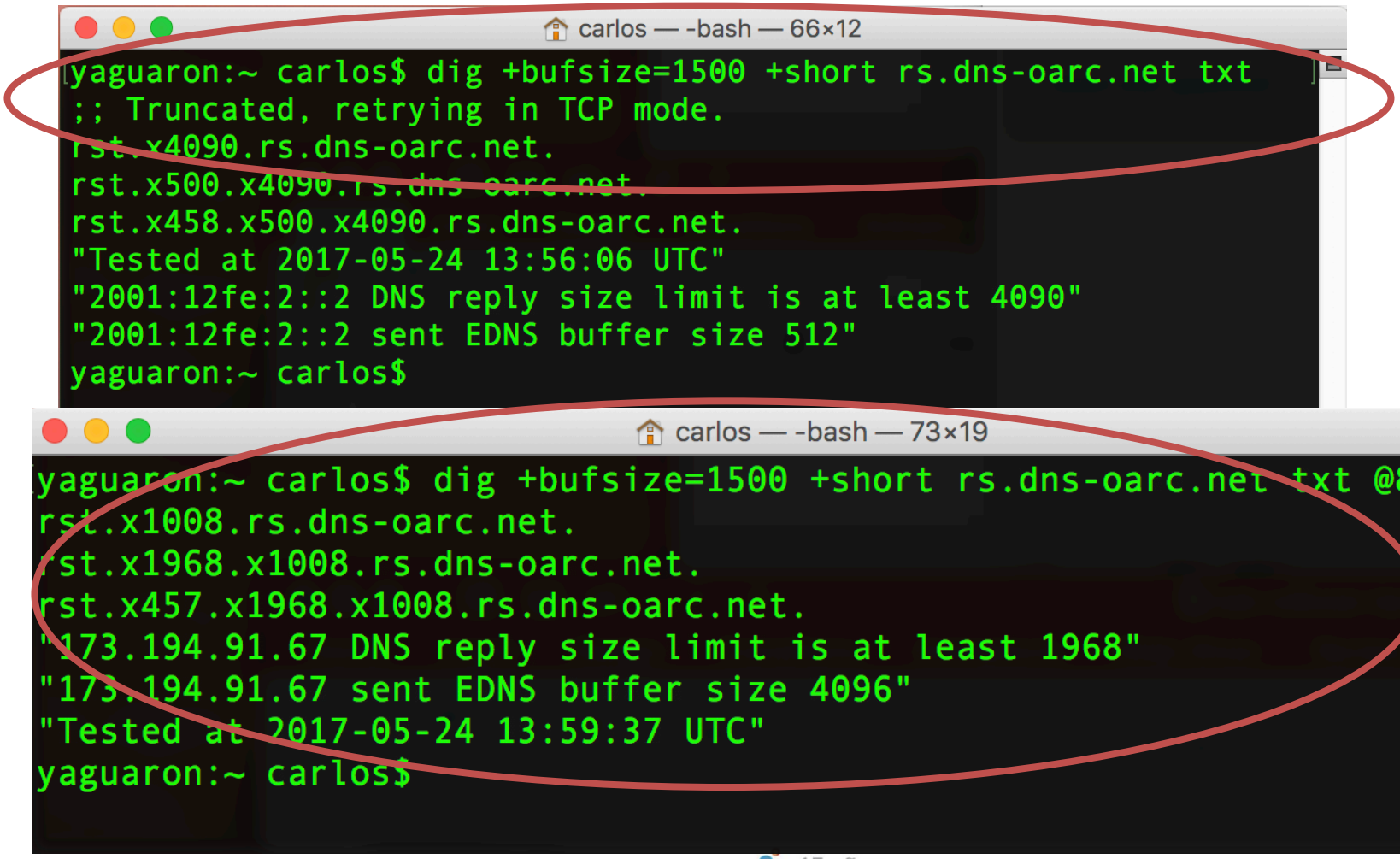
Key Size Test

This web page is designed to test your network's ability to resolve domain names that have been signed with "large" DNSSEC keys. See the explanations below for additional information.

Test ID *1022919778* at *Sun, 21 May 2017 19:44:20 GMT*

#	Description	KSKs	ZSKs	Signed DNSKEY Size	Result
1	2048 ZSK Normal	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign	949	PASS
2	2048 ZSK Rollover	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish 2048-bit RSASHA256 publish+sign	1237	PASS
3	KSK Rollover with 2048 ZSK	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish+sign+revoke	2048-bit RSASHA256 publish+sign	1571	PASS
4	KSK Rollover with 2048 ZSK rollover	2048-bit RSASHA256 publish+sign+revoke 2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish	1865	PASS
5	This should fail			0	FAIL

Key Size Test (ii)



Set Up Monitoring

- Pay (more) attention to
  - DNSSEC failures in DNS log messages
    - This may indicate trouble with configured trust anchors
  - Fragmented packets in the network
    - This may indicate trouble with large DNS messages
  - DNS recursive servers' trust anchor sets
    - Verify "it" is working
- Monitor appropriately
  - Don't get overwhelmed by alerts (so they are ignored)
  - Don't take silence as "good", a monitor may fail!

Do What Needs to be Done

- Follow your plan
  - Even if you don't DNSSEC validate
    - Watch for packet fragments
  - If you follow Automated Updates
    - Verify your server and configuration are set properly
    - Be sure you see the new KSK as trusted in August/September 2017
  - If you opt to configure manually
    - Set up a plan to establish trust
    - Plan to update all servers

Retrieving the new KSK "manually"

- To assist those opting out of Automated Updates
  - A python script called *get_trust_anchor.py*
  - **https://github.com/iana-org/get-trust-anchor**
  - Script generates files which can be used to configure servers
  - Script is an example of how to evaluate trust

Notes for BIND

- Check configuration
  - If you validate, don't use "trusted-keys" option
  - Replace it with "managed-keys"
- Learn diagnostic tools
  - rndc "secroots" (in version 9.9 and maybe earlier)
  - rndc "managed-keys status" (from version 9.11)
  - file managed-keys.bind
- Configure managed-keys

Bad dog! (Apologies to Geoff Huston)

- options { dnssec-validation auto;};
- trusted-keys { . 257 3 8 "AwEAAag ... +Uk1ihz0=";};

or "yes"

Good dog! (Apologies to Geoff Huston)

- `options { dnssec-validation auto;};`
- `managed-keys { . initial-key 257 3 8 "AwEAAag ... +Uk1ihz0=";};`

Better dog! (Apologies to Geoff Huston)

- All you need in named.conf is:

- `options { dnssec-validation auto;};`

BIND & the automated updates testbed

- Sign up for the mailed instructions via
  - https://automated-ksk-test.research.icann.org/

- A "sample" configuration is:

```
options { dnssec-validation auto;};
managed-keys {
    2017-03-05.automated-ksk-
test.research.icann.org
    initial-key 257 3 8
    "AwEAAa9qsSLDI....wuKupscP8KHBluZyOSK
    w4RMTk6YBdE=";
};
```

What to expect

- A file called "managed-keys.bind" which lists keys trusted or in the automated updates process

- rndc – "secroots" dumps named.secroots, the trust anchors
- rndc – "managed-keys" (in 9.11) lists automated-update status of key

- If a key is in managed-keys.bind but not listed in named.secroots, it is likely in the addpend state (see RFC 5011)

Notes for unbound

- To add a managed root trust anchor:
  - auto-trust-anchor-file: "root.key"
- And in the file "root.key"
  - Place a DS or DNSKEY record for the current appropriate trust anchor
  - E.g.
  - . 172800 IN DNSKEY 257 3 8 AwEAAagAIKlVZrpC6Ia...+Uk1ihz0=
  - This file will be rewritten by unbound, if not there's a problem!
- For manual management
  - unbound-anchor is a tool to get and evaluate the current trust anchors published via the web

¡Muchas gracias!