DNS Security / DNSSEC Tutorial

In collaboration with SANOG32

Champika Wijayatunga
Regional Security Engagement Manager – Asia Pacific

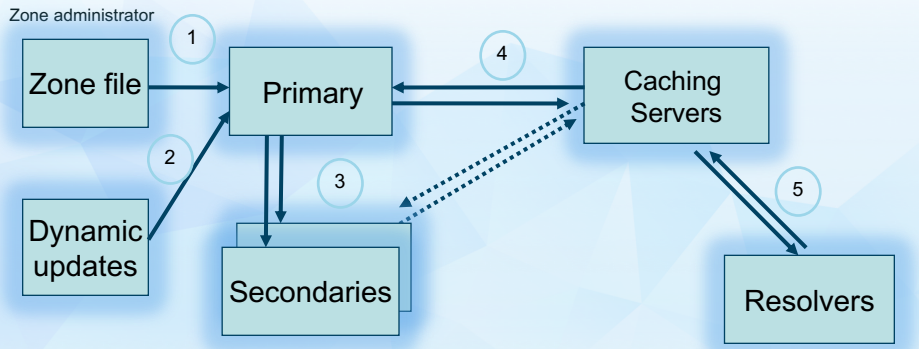
07 August 2018

Agenda

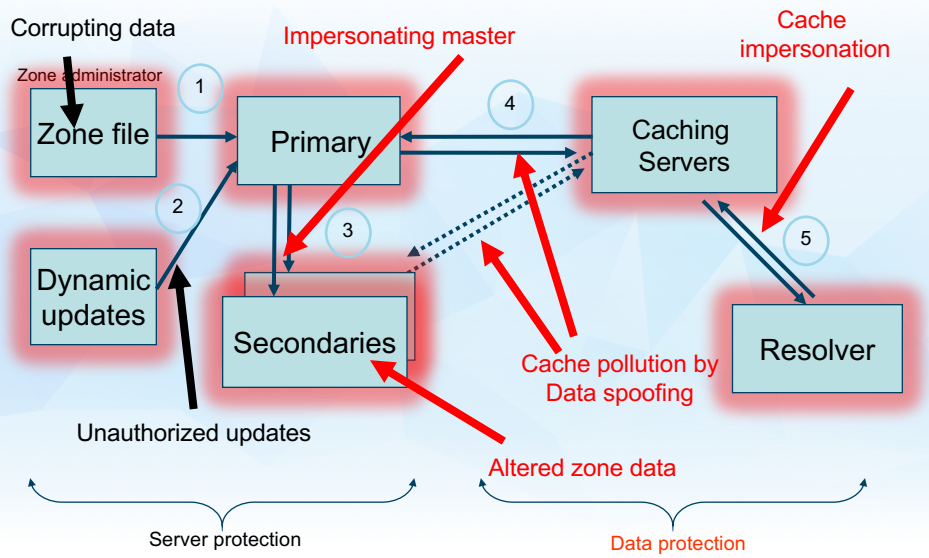
1. DNS Security
2. DNSSEC
3. Root Zone KSK Rollover

DNS Security

DNS: Data Flow



DNS Vulnerabilities



The Bad

- Cache Poisoning Attacks
  - Vulnerable resolvers add malicious data to local caches
- DNS Hijacking
  - A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
- E.g. DNSChanger
  - One of the biggest cybercriminal takedown in history
- And many other DNS hijacks in recent times
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate.
- DNS is relied on for unexpected things though insecure.

Securing DNS

- There are two aspects when considering DNS Security
  - Server protection
  - Data protection
- Server protection
  - Protecting servers
    - Make sure your DNS servers are protected (i.e. physical security, latest DNS server software, proper security policies, Server redundancies etc.)
  - Protecting server transactions
    - Deployment of TSIG, ACLs etc. (To secure transactions against server impersonations, secure zone transfers, unauthorized updates etc.)
- Data protection
  - Authenticity and Integrity of Data
    - Deployment of DNSSEC (Protect DNS data against cache poisoning, cache impersonations, spoofing etc.)

Technical Requirements

- Networks and Servers (redundant)
- Back office systems.
- Physical and Electronic Security
- Quality of Service (24/ 7 availability!)
- Name Servers
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Name Server Considerations

- Support technical standards
- Handle load multiple times the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively
- Turn off recursion!
- Should “NOT” block access from a valid Internet hosts

Secondary Name Server Choice

Diversity, Diversity and Diversity!

- Don’t place all on the same LAN/building/segment
- Network diversity
- Geographical diversity
- Institutional diversity
- Software and hardware diversity

Security, Stability & Resiliency Considerations

- Physical security
  - Deploy stringent access controls
  - Fire detection and retardation
  - Other environmental sensors (Flood, Humidity etc.)
  - Power continuity for 48 hours (or more)
- Backups
  - Multiple secure copies locally and offsite
  - Test, test and test!!

Know Your SLAs

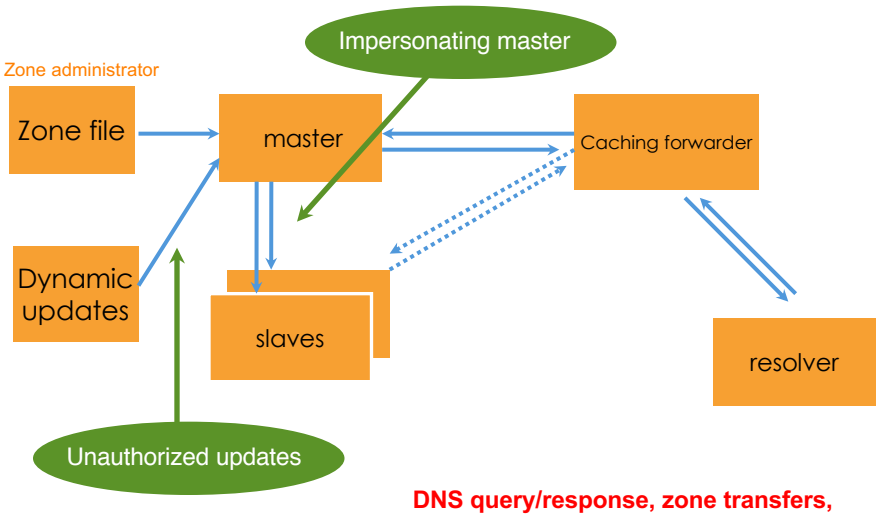
- Functioning name servers are the most critical/visible service
- All other services also need to be considered
  - Billing
  - Whois server, webservers
  - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?

When It All Goes Wrong

- DNS is a known target for hackers.
- You will be targeted at some point!
- Have plans in place to deal with attacks, failures and disasters.
- Test those plans regularly!

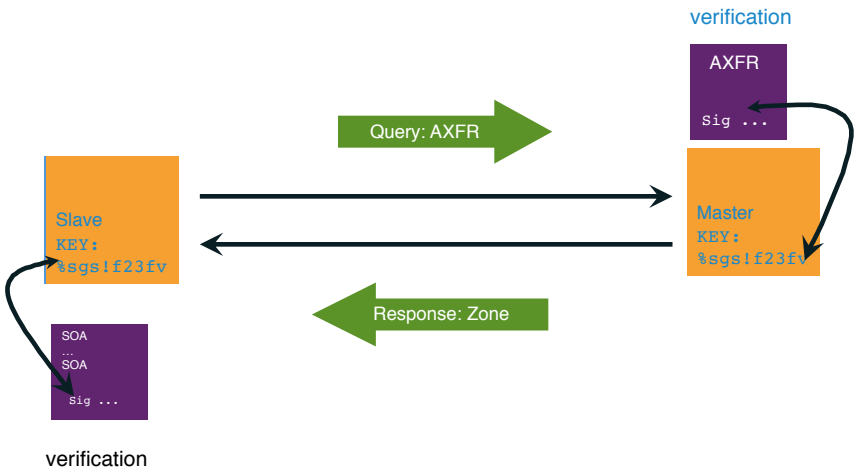
Transaction Signatures

Transactions - Protected Vulnerabilities



DNS query/response, zone transfers, Dynamic updates

TSIG example



TSIG steps

1. Generate secret
2. Communicate secret
3. Configure servers
4. Test

TSIG - Names and Secrets

- TSIG name
  - A name is given to the key, the name is what is transmitted in the message (so receiver knows what key the sender used)
- TSIG secret value
  - A value determined during key generation
  - Usually seen in Base64 encoding

TSIG – Generating a Secret

- dnssec-keygen
  - A simple tool to generate keys
  - Used here to generate TSIG keys

```
dnssec-keygen -a <algorithm> -b <bits> -n host
  <name of the key>
```


TSIG – Generating a Secret

- Example

```
> dnssec-keygen –a HMAC-SHA256 –b 256 –n HOST ns1-ns2.pcx.net

This will generate the key
  Kns1-ns2.pcx.net.+157+15921

>ls
Kns1-ns2.pcx.net.+157+15921.key
Kns1-ns2.pcx.net.+157+15921.private
```

TSIG – Generating a Secret

- TSIG is used in server configuration, not in zone file
- Could be confusing because it looks like RR

```
ns1-ns2.pcx.net. IN KEY 128 3 157 nEfRX9…bbPn7lyQtE=
```


TSIG – Configuring Servers

- Configuring the key

```
key { algorithm ...; secret ...;}
```

- Making use of the key

```
server x { key ...; }
```

where x is the IP address of the other server

Configuration Example – named.conf

Primary server 192.168.1.100

```
key ns1-ns2.pcx. net {
    algorithm hmac-sha1;
    secret "APlaceToBe";
};
server 192.168.1.200 {
    keys {ns1-ns2.pcx.net;};
};
zone "my.zone.test." {
    type master;
    file "db.myzone";
    allow-transfer {
    key ns1-ns2.pcx.net ;};
};
```

Secondary server 192.168.1.200

```
key ns1-ns2.pcx.net {
    algorithm hmac-sha1;
    secret "APlaceToBe";
};
server 192.168.1.100 {
  keys {ns1-ns2.pcx.net;};
};
zone "my.zone.test." {
    type slave;
    file "myzone.backup";
    masters {192.168.1.100;};
};
```

You can save this in a file and refer to it in the named.conf using 'include' statement:

```
include "/var/named/master/tsig-key-ns1-ns2";
```


TSIG Testing - dig

- You can use dig to check TSIG configuration
  - `dig @<server> <zone> AXFR -k <TSIG keyfile>`

```
dig @localhost example.net AXFR \
   -k Kns1-ns2.pcx.net.+157+15921.key
```

- A wrong key will give "Transfer failed" and will be logged on the server's using the security-category

TSIG Testing - Time

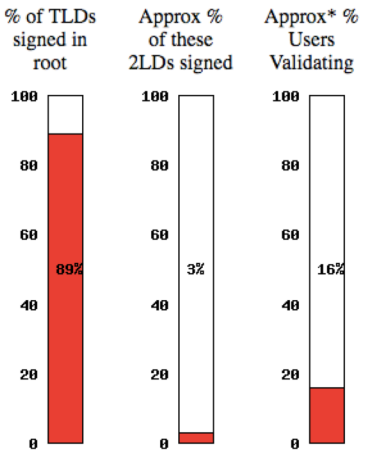
- TSIG is time sensitive
- Message protection expires in 5 minutes
  - Make sure time is synchronized
  - For testing, set the time
  - In operations, (secure) NTP is needed

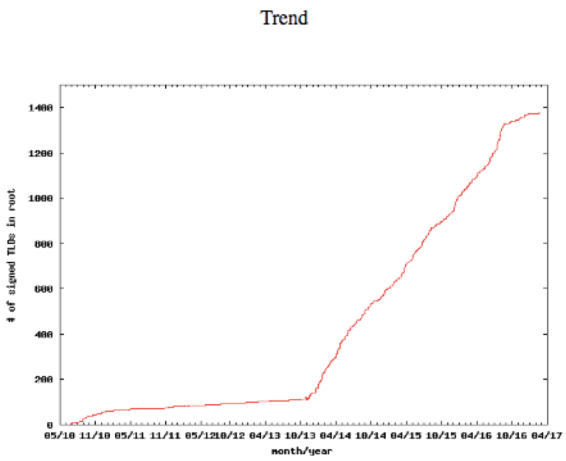
DNSSEC

How DNSSEC Works

DNSSEC ccTLD Map

DNSSEC Deployment





DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.

*but required by new ICANN registrar agreement

What you can do

- For Companies:
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- For Users:
  - Ask ISP to turn on validation on their DNS resolvers
- For All:
  - Take advantage of DNSSEC education and training

New Concepts

- Secure Entry Point and Chain of Trust
  - Delegating Signing Authority
- New packet options (flags)
  - CD, AD, DO
- New RRs
  - DNSKEY, RRSIG, NSEC/NSEC3 and DS
- Signature expiration
- Key Rollovers

Chain of Trust and Secure Entry Point

- Using the existing delegation based model of distribution
- Don't sign the entire zone, sign a RRset
- Parent DOES NOT sign the child zone. The parent signs a pointer (hash) to the key used to sign the data of the child zone (DS record)
- Example with **`www.myzone.net.`**

New RRs

- Adds five new DNS Resource Records:
  1. DNSKEY: Public key used in zone signing operations.
  2. RRSIG: RRset signature
  3. NSEC &
  4. NSEC3: Returned as verifiable evidence that the name and/or RR type does not exist
  5. DS: Delegation Signer. Contains the hash of the public key used to sign the key which itself will be used to sign the zone data. Follow DS RR's until a "trusted" zone is reached (ideally the root).

New RR: DNSKEY

```
                                          PROTOCOL
OWNER                TYPE    FLAGS        ALGORITHM
example.net.  43200  DNSKEY   256    3     7  (
    AwEAAbinasY+k/9xD4MBBa3QvhjuOHIpe319SFbWYIRj
    /nbmVZfJnSw7By1cV3Tm7ZlLqNbcB86nVFMSQ3JjOFMr
    ....) ; ZSK; key id = 23807
```

PUBLIC KEY (BASE64)

KEY ID

- FLAGS determines the usage of the key
- PROTOCOL is always 3 (DNSSEC)
- ALGORITHM can be (3: DSA/SHA-1, 5: RSA/SHA1, 8: RSA/SHA-256, 12: ECC-GOST)
  - http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

DNSKEY: Two Keys, not one…

- There are in practice at least two DNSKEY pairs for every zone
- Originally, one key-pair (public, private) defined for the zone
  - private: key used to sign the zone data (RRsets)
  - public: key published (DNSKEY) in the zone
- DNSSEC works fine with a single key pair
- Problem with using a single key:
  - Every time the key is updated, the DS record must be updated on the parent zone as well
  - Introduction of Key Signing Key (flags=257)

KSK and ZSK

- Key Signing Key (KSK)
  - Pointed to by parent zone in the form of DS (Delegation Signer). Also called Secure Entry Point.
  - Used to sign the Zone Signing Key
  - Flags: 257
- Zone Signing Key (ZSK)
  - Signed by the KSK
  - Used to sign the zone data RRsets
  - Flags: 256
- This decoupling allows for independent updating of the ZSK without having to update the KSK, and involve the parents (i.e. less administrative interaction)

New RR: RRSIG (Resource Record Signature)

```
example.net.   600   A   192.168.10.10
example.net.   600   A   192.168.23.45
```

OWNER	TYPE	TYPE COVERED	ALG	#LABELS	TTL	
example.net.	600	RRSIG	A	7	2	600 (

SIG. EXPIRATION	SIG. INCEPTION	KEY ID	SIGNER NAME
20150115154303	20141017154303	23807	example.net.

SIGNATURE

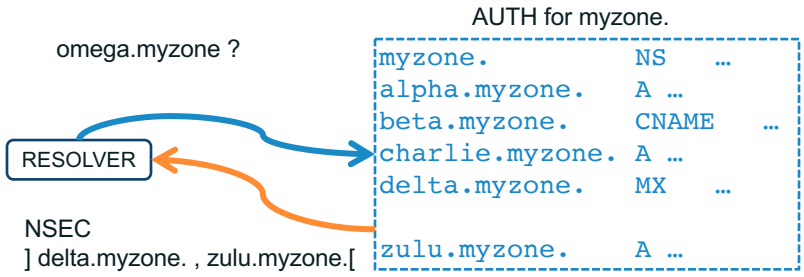
```
CoYkYPqE8Jv6UaVJgRrh7u16m/cEFGtFM8TArbJdaiPu
W77wZhrvonoBEyqYbhQ1yDaS74u9whECEe08gfoe1FGg
. . .
)
```

RRSIG

- Typical default values
  - Signature inception time is 1 hour before.
  - Signature expiration is 30 from now
  - Proper timekeeping (NTP) is required
- What happens when signatures run out?
  - SERVFAIL
  - Domain effectively disappears from the Internet for validating resolvers
- Note that keys do not expire
- No all RRSets need to be resigned at the same time

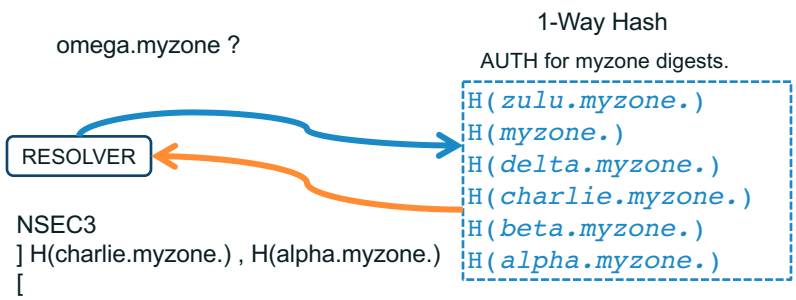
New RR: NSEC

- NXDomains also must be verified
- NSEC provides a pointer to the Next SECure record in the chain of records.



New RR: NSEC3

- To avoid concerns about “zone enumeration”
- To avoid large zone-files: opt-out concept



New RR: DS (Delegation Signer)

- Hash of the KSK of the child zone
- Stored in the parent zone, together with the NS RRs indicating a delegation of the child zone.
- The DS record for the child zone is signed together with the rest of the parent zone data
- NS records are NOT signed (they are a hint/pointer)

Digest type 1 = SHA-1, 2 = SHA-256

```
myzone.    DS  61138   5  1
F6CD025B3F5D0304089505354A0115584B56D683

myzone.    DS  61138   5  2
CCBC0B557510E4256E88C01B0B1336AC4ED6FE08C8268CC1AA5FBF00 5DCE3210
```

Signature Expiration

- Signatures are per default 30 days (BIND)
- Need for regular resigning:
  - To maintain a constant window of validity for the signatures of the existing RRset
  - To sign new and updated Rrsets
  - Use of jitter to avoid having to resign all expiring RRsets at the same time
- The keys themselves do NOT expire…
- But they may need to be rolled over...

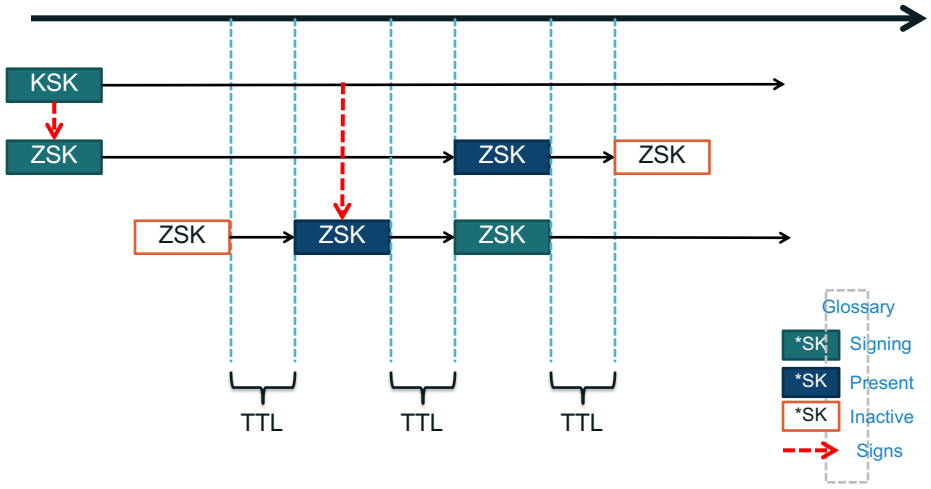
Key Rollovers

- Try to minimise impact
  - Short validity of signatures
  - Regular key rollover
- Remember: DNSKEYs do not have timestamps
  - the RRSIG over the DNSKEY has the timestamp
- Key rollover involves second party or parties:
  - State to be maintained during rollover
  - Operationally expensive

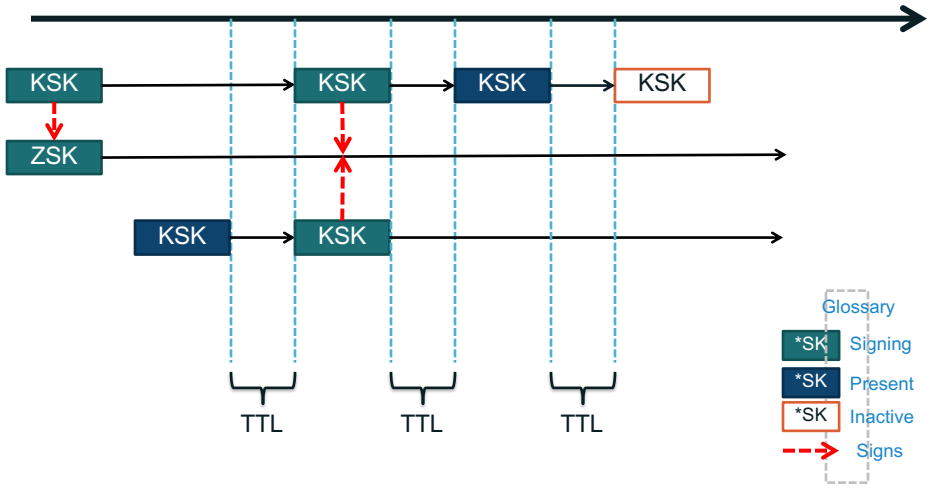
Key Rollovers

- Two methods for doing key rollover
  - Pre-Publish
  - Double Signature
- KSK and ZSK rollover use different methods.
  - Remember that KSK needs to interact with parent zone to update DS record.

Key Rollovers: Pre-Publish method



Key Rollovers: Double Signature



47 ICANN | 47

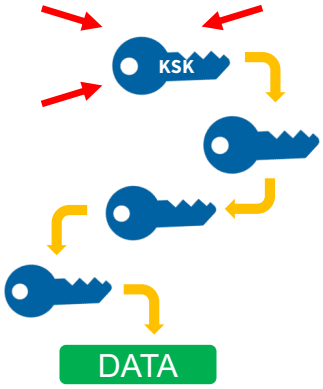
Root Zone DNSSEC KSK Rollover

48 ICANN | 48

KSK Rollover: An Overview

ICANN is in the process of performing a Root Zone DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the topmost cryptographic key in the DNSSEC hierarchy
- The KSK is a cryptographic public-private key pair:
  - Public part: trusted starting point for DNSSEC validation
  - Private part: signs the Zone Signing Key (ZSK)
- Builds a "chain of trust" of successive keys and signatures to validate the authenticity of any DNSSEC signed data



Why is ICANN Rolling the KSK?

- Because it's not good for a cryptographic key to live forever. The cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
  - Ensures infrastructure can support key change in case of emergency
- This type of change has never before occurred at the root level
  - There has been one functional, operational Root Zone DNSSEC KSK since 2010
- Because it's better to make proactive changes during normal operations when things are running smoothly, rather than be reactive in an emergency. The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations

DNSSEC

When Does the Rollover Take Place?

- The changing or "rolling" of the KSK Key was originally scheduled to occur on 11 October 2017, but it was delayed because some data obtained in September 2017 showed that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators were not yet ready for the key rollover.
- There may be multiple reasons why operators do not have the new KSK installed in their systems: some may not have their resolver software properly configured.
- After a preliminary consultation with the community, ICANN posted a plan for starting the rollover process again. That plan was open for community comment at https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en.
- The plan calls for ICANN to roll the root KSK on 11 October 2018 while encouraging ISPs and Network operators to use this additional time period to be certain that their systems are ready for the key rollover.

Why You Need to Prepare

If you have enabled DNSSEC validation, you must update your systems with the new KSK to help ensure trouble-free Internet access for users

- Currently, 25 percent of global Internet users, or **750 million people**, use DNSSEC-validating resolvers that could be affected by the KSK rollover
- If these validating resolvers do not have the new key when the KSK is rolled, end users relying on those resolvers will encounter errors and be **unable to access the Internet**

What Do Operators Need to Do?

- **Be aware whether DNSSEC is enabled in your servers**
- **Be aware of how trust is evaluated in your operations**
- **Test/verify your set ups**
- **Inspect configuration files, are they (also) up to date?**
- **If DNSSEC validation is enabled or planned in your system**
  - Have a plan for participating in the KSK rollover
  - Know the dates, know the symptoms, solutions

How To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- The KSK will be updated automatically at the appropriate time
- You do not need to take additional action
  - Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does <u>not</u> support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- The software's trust anchor file must be manually updated
- The new root zone KSK is now available here:

http://data.iana.org/root-anchors/

Recognizing KSK-2017

- The KSK-2017's Key Tag is

  20326

- The Delegation Signer (DS) Resource Record for KSK-2017 is

```
.      IN   DS     20326 8 2
                     E06D44B80B8F1D39A95C0B0D7C65D084
                     58E880409BBC683457104237C7F8EC8D
```

"Root"

Note: liberties taken with formatting for presentation purposes

KSK-2017 in a DNSKEY Resource Record

- The DNSKEY resource record will be:

```
. IN DNSKEY  257 3 8
     AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
     +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
     ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
     0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
     oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
     RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
     R1AkUTV74bU=
```

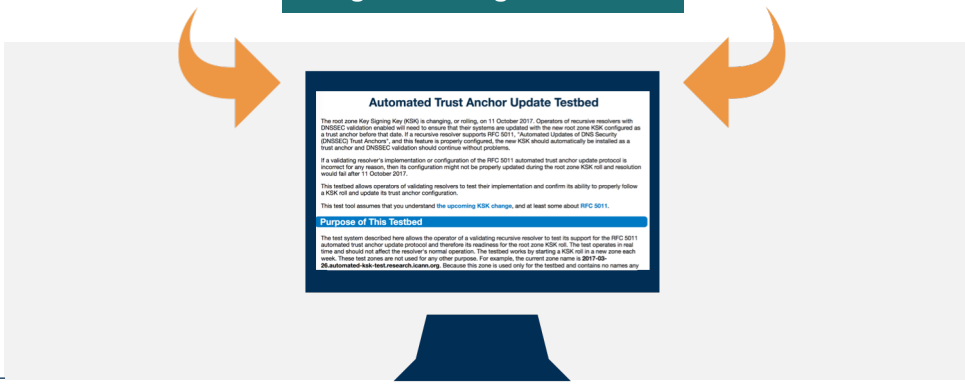
"Root"

Note: liberties taken with formatting for presentation purposes

Check to See If Your Systems Are Ready

ICANN is offering a **test bed** for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure your systems are ready by visiting:
go.icann.org/KSKtest



Automated Trust Anchor Update Testbed

The root zone Key Signing Key (KSK) is changing, or rolling, on 11 October 2017. Operators of recursive resolvers with DNSSEC validation enabled will need to ensure that their systems are updated with the new root zone KSK configured as a trust anchor before that date. If a recursive resolver supports RFC 5011, "Automated Updates of DNS Security (DNSSEC) Trust Anchors", and this feature is properly configured, the new KSK should automatically be installed as a trust anchor and DNSSEC validation should continue without problems.

If a validating resolver's implementation or configuration of the RFC 5011 automated trust anchor update protocol is incorrect for any reason, then its configuration might not be properly updated during the root zone KSK roll and resolution would fail after 11 October 2017.

This testbed allows operators of validating resolvers to test their implementation and confirm its ability to properly follow a KSK roll and update its trust anchor configuration.

This test tool assumes that you understand the upcoming KSK change, and at least some about RFC 5011.

Purpose of This Testbed

The test system described here allows the operator of a validating recursive resolver to test its support for the RFC 5011 automated trust anchor update protocol and therefore its readiness for the root zone KSK roll. The test operates in real time and should not affect the resolver's normal operation. The testbed works by starting a KSK roll in a new zone each week. These test zones are not used for any other purpose. For example, the current zone name is **2017-03-26.automated-ksk-test.research.icann.org**. Because this zone is used only for the testbed and contains no names any

Three Steps to Recovery

If your DNSSEC validation fails after the key role:

Stop the tickets
It's OK to turn off DNSSEC validation while you fix (but remember to turn it back on!)

Debug
If the problem is the trust anchor, find out why it isn't correct
- Did RFC 5011 fail? Did configuration tools fail to update the key?
- If the problem is fragmentation related, make sure TCP is enabled and/or make other transport adjustments

Test the recovery
Make sure your fixes take hold

For More Information

1. **Visit https://icann.org/kskroll**
2. **Join the conversation online**
   - Use the hashtag #KeyRoll
   - Sign up to the mailing list https://mm.icann.org/listinfo/ksk-rollover
3. **Ask a question to globalsupport@icann.org**
   - Subject line: "KSK Rollover"
4. **Attend an event**
   - Visit https://features.icann.org/calendar to find upcoming KSK rollover presentations in your region

Engage with ICANN – Thank You and Questions

ICANN One World, One Internet

Visit us at **icann.org** Email: champika.wijayatunga@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann