

# Root Zone KSK Rollover: delay and next steps

**Alexandra Kulikova**  
**Head of Global Stakeholder Engagement**  
**Eastern Europe and Central Asia**

**UADOM, Kiev, Ukraine**  
**1 December, 2017**



# What is DNSSEC?

- ◉ “DNS SECurity enhancements” (DNSSEC) improves the DNS by **digitally signing** DNS data. This provides:
  - ◉ **Data origin authentication**
    - ◉ “I looked up DNS data and I verify which zone the data came from”
  - ◉ **Data integrity**
    - ◉ “I know the data in the zone hasn’t been modified since it was signed”
  - ◉ **Proof of non-existence**
    - ◉ “I can be sure the data I’m looking for is not in the zone”
- ◉ A **public/private key pair** is created for each zone (e.g., *EXAMPLE.COM*).
  - ◉ The **private key** is kept secret
  - ◉ The **public key** is published in the DNS
- ◉ Zone data is signed with the zone’s **private key** to produce **digital signatures**
  - ◉ After a resolver (DNS client) looks up data in a signed zone, that data can be **validated** with the zone’s **public key**

# Chain of Trust

⦿ **Q:** If a zone publishes its public key, how can you trust it?

⦿ **A:** The parent zone uses its **private key** to sign the child zone's public key.

⦿ This process goes all the way to the DNS root zone.

Example:

⦿ *WWW.EXAMPLE.COM* is signed with *EXAMPLE.COM*'s private key

⦿ *EXAMPLE.COM*'s public key signed with *COM*'s private key

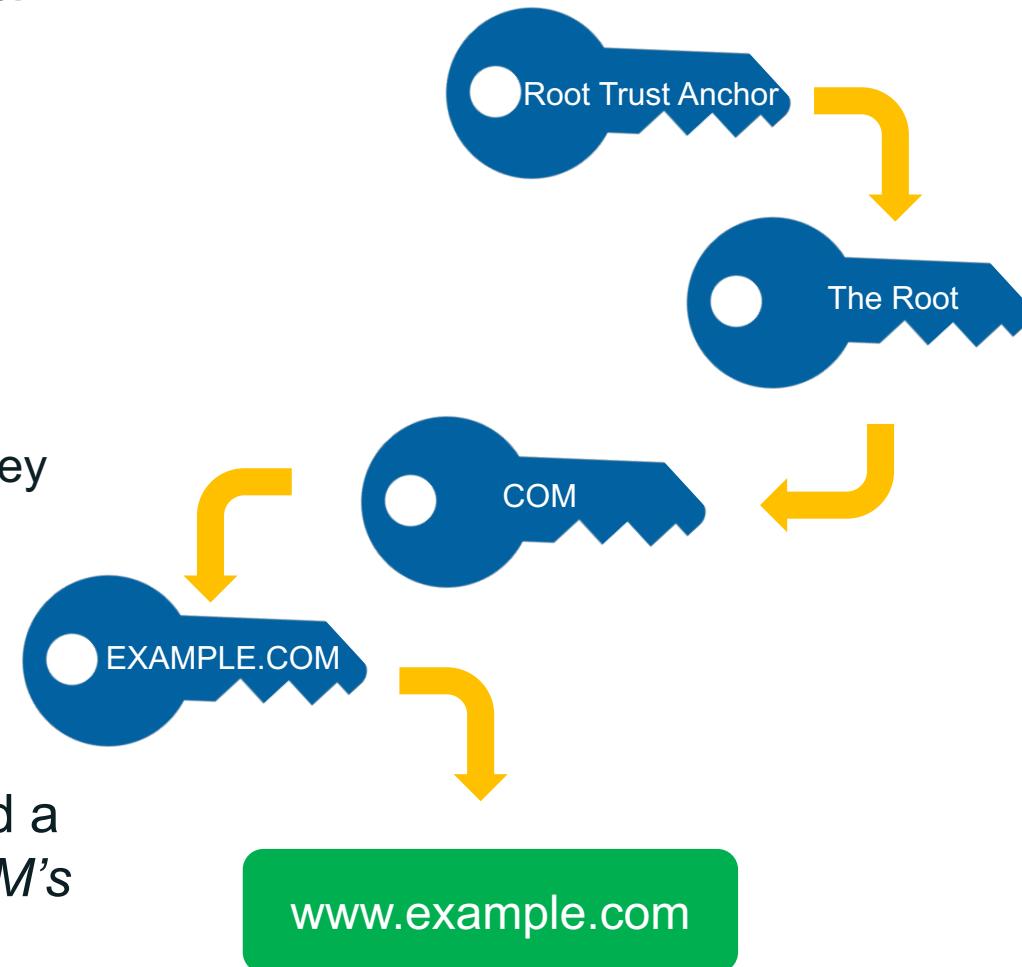
⦿ *COM*'s public key signed by the root's private key

⦿ The root's public key is not signed by anyone: we need to just trust it

⦿ The root zone's public key is called the **root trust anchor**

⦿ To validate *WWW.EXAMPLE.COM*'s DNS data, we build a **chain of trust** from *EXAMPLE.COM*'s public key to *COM*'s public key to the root's public key.

⦿ And the root's public key is distributed with every validating resolver.



# DNSSEC in the Root Zone

---

- DNSSEC in the root zone is managed by ICANN and Verisign
- ICANN, responsible for operating the root KSK
  - KSK lifecycle management, “sign the ZSK”
- Verisign, responsible for operating the root ZSK
  - ZSK lifecycle management, “sign the root zone”
- These activities are coordinated but are operated separately

# Root Zone KSK

- ⦿ The full name for the root zone's public key used as a trust anchor is the **Root Zone Key-Signing Key (KSK)**
- ⦿ The root zone KSK is the most important key in DNSSEC
- ⦿ Any software performing DNSSEC validation **must** have the Root Zone KSK configured as a trust anchor



**Watch video:**

<https://www.youtube.com/watch?v=d7H1AkC9Plw>

# Current Root KSK

---

- The current root KSK was created in 2010
- Stored in hardware security modules (HSMs)
- Two key management facilities (KMFs) have the same data as redundant backups
- (The operation of these is an entirely different talk)

# Getting and Validating the Root KSK

---

- The root KSK comes in the DNS
  - ...but is only as reliable as the data in unprotected DNS
- Get the trust anchor validation from IANA directly
  - <https://data.iana.org/root-anchors/root-anchors.xml>
  - Secured by a PKIX certificate and signature
- Trust anchor validation may also come by other means
  - Might come in the source code of your validating software

# Root Zone KSK Rollover

---

- ◉ Until earlier this year, there was just one Root Zone KSK
  - ◉ Created when the root was first signed in 2010 (KSK-2010)
  - ◉ A second was added earlier this year (KSK-2017)
- ◉ **A new KSK to be used**
  - ◉ This change is known as “Rolling the Key”
  - ◉ A carefully planned, multi-year process to ensure continued smooth operations of the global secured DNS
- ◉ **Resolver operators with DNSSEC enabled had some work to do**
  - ◉ As little as reviewing configurations (and testing)
  - ◉ As much as installing the new KSK (and testing)

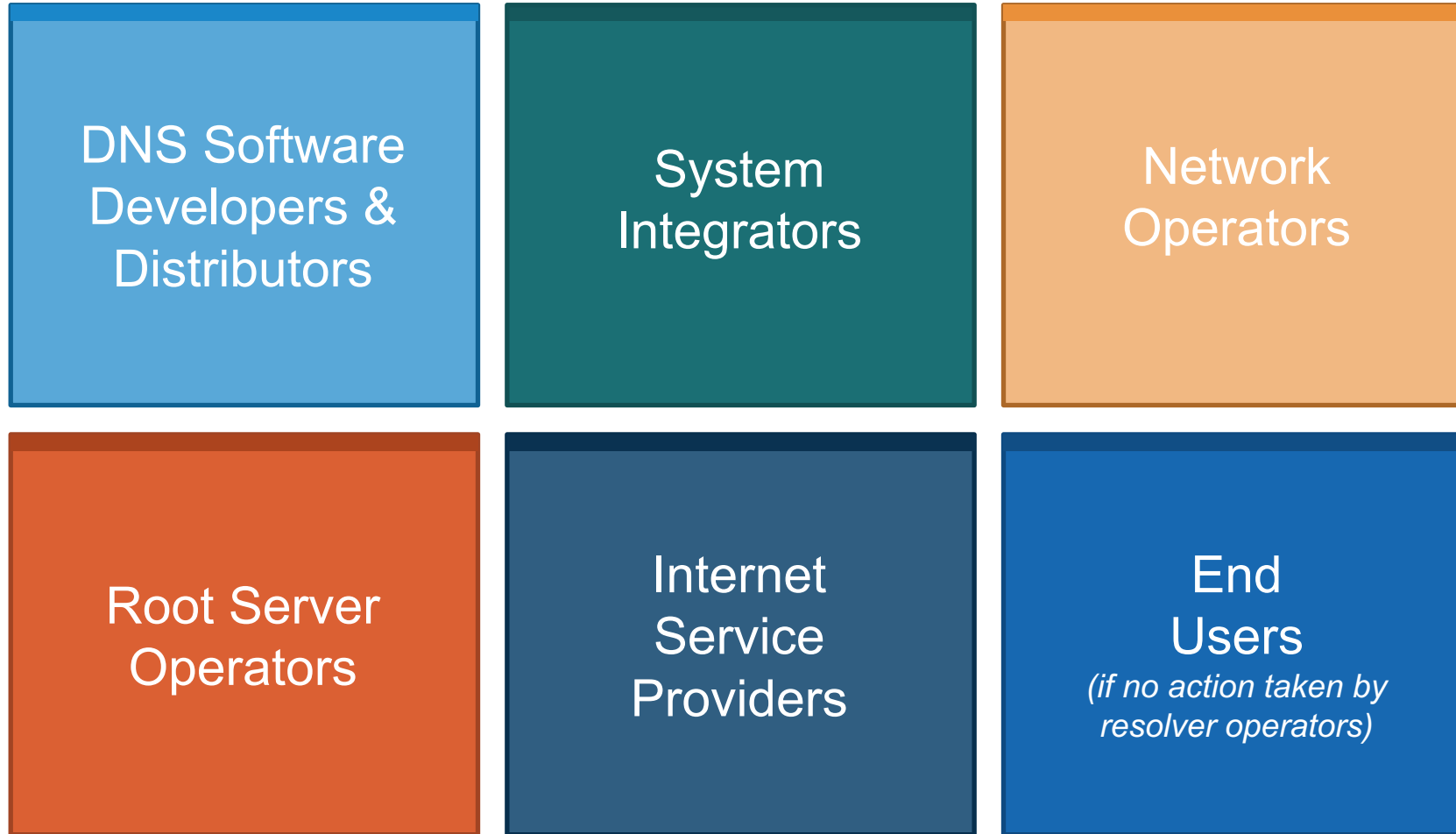


# Why is ICANN Rolling the KSK?

- ⦿ As with passwords, 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
- ⦿ The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations



# Who Will Be Impacted?



# Resolver Operators Need to Work with the New KSK



If you run a resolver and have enabled DNSSEC validation, you must update your configuration with the new Root Zone KSK to help ensure trouble-free Internet access for users

- ⦿ DNSSEC validation usually occurs in **recursive resolvers** (also called **recursive name servers** or **caching name servers**) run by
  - ⦿ Internet service providers (ISPs)
  - ⦿ Enterprise network operators
  - ⦿ Dedicated resolver operators (e.g., Google' Public DNS, OpenDNS, etc.)
- ⦿ 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 are not configured the new root zone KSK which was put into use on 11 October 2017, end users relying on those resolvers **will** encounter errors and be **unable to look up any name on the Internet**.

# How Do Resolver Operators Update Their Trust Anchor?



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

- ◉ The root zone KSK should be updated automatically at the appropriate time
- ◉ You should 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 resolver does **not** 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 available at:

[http://data.iana.org/  
root-anchors/](http://data.iana.org/root-anchors/)

# The KSK Rollover Plan Documents

---

- Available at: <https://www.icann.org/kskroll>

2017 KSK Rollover Operational Implementation Plan

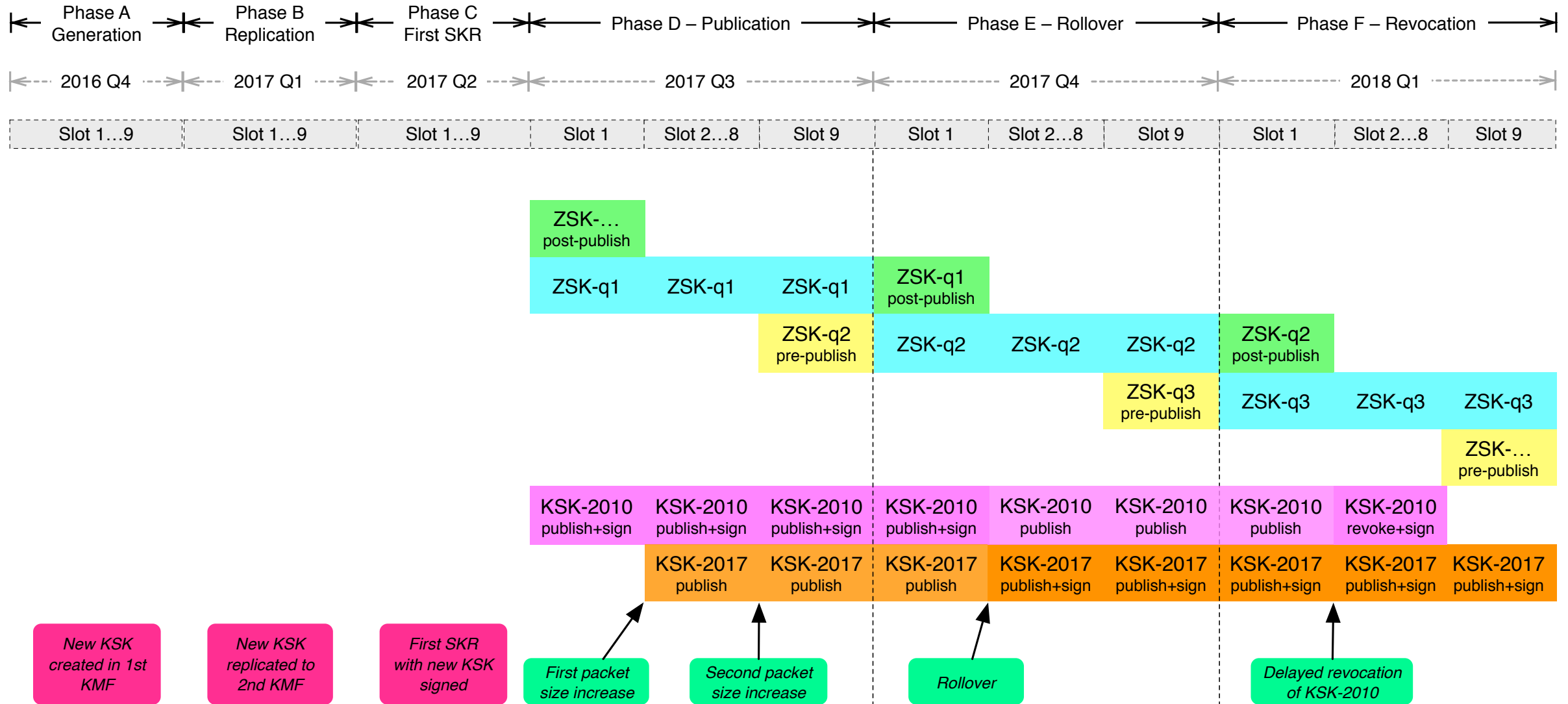
2017 KSK Rollover Systems Test Plan

2017 KSK Rollover Monitoring Plan

2017 KSK Rollover External Test Plan

2017 KSK Rollover Back Out Plan

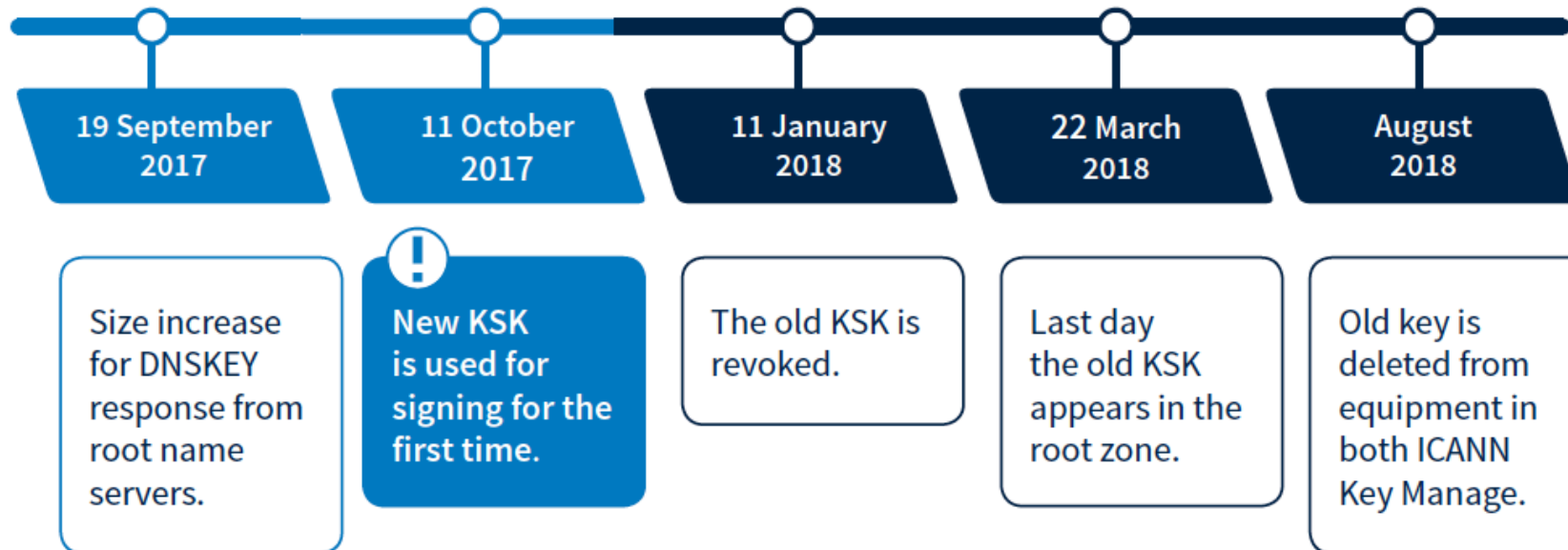
# Operational Implementation Plan Timeline (Original)



# When Does the Rollover Take Place?

## The KSK rollover is a process, not a single event

The following dates are key milestones in the process when end users may experience interruption in Internet services:



# When Does the Rollover Take Place?

---

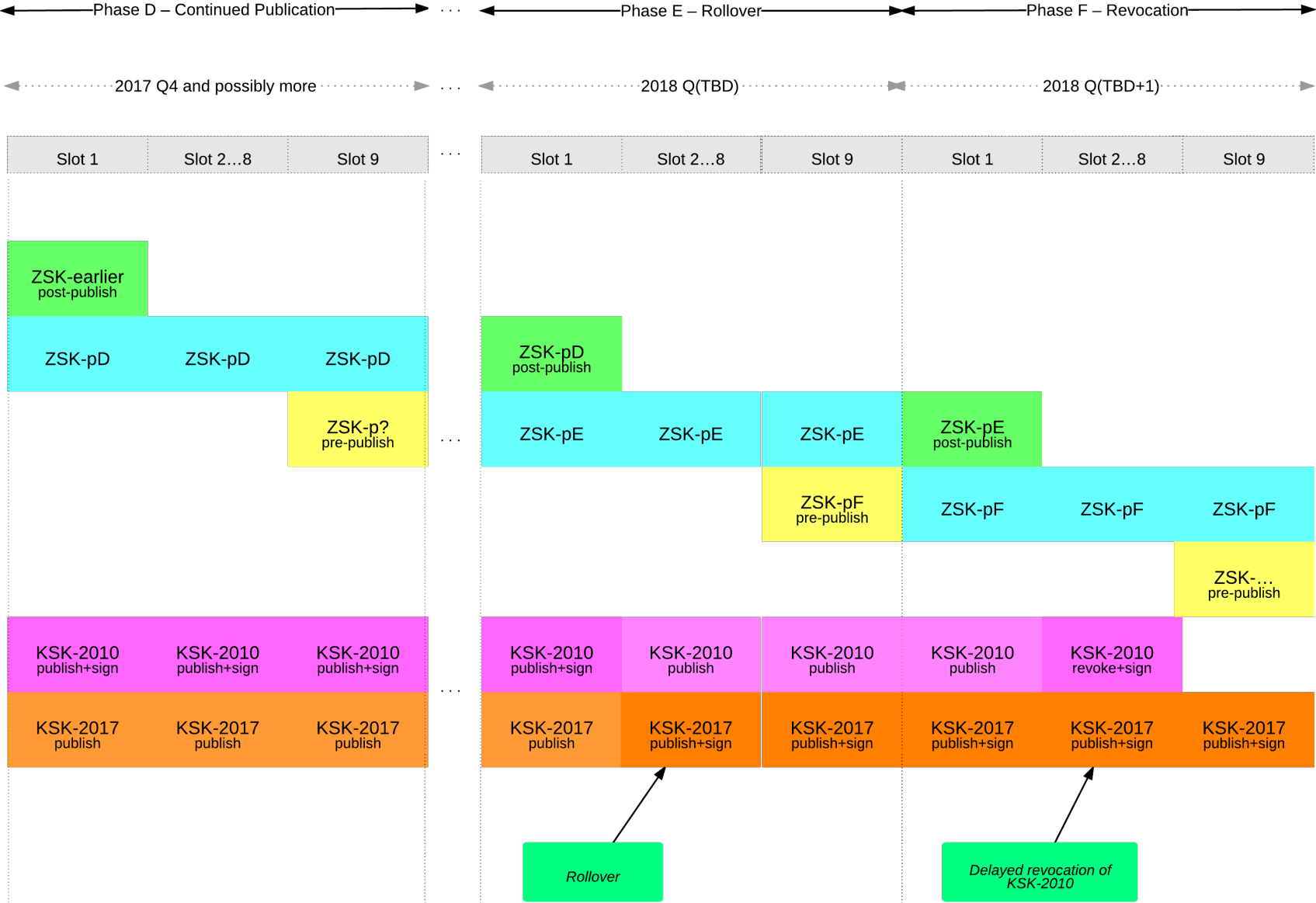
- ◉ The changing or "rolling" of the KSK Key was originally scheduled to occur on **11 October 2017**, but it is being delayed because some recently obtained data shows that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators are not yet ready for the Key Rollover.
- ◉ There may be multiple reasons why operators do not have the new key installed in their systems: some may not have their resolver software properly configured and a recently discovered issue in one widely used resolver program appears to not be automatically updating the key as it should, for reasons that are still being explored.
- ◉ ICANN is tentatively hoping to reschedule the Key Rollover for the **first quarter of 2018** and is encouraging ISPs and Network operators to use this additional time period to be certain that their systems are ready for the Key Rollover.



## **New data obtained in September 2017:**

- Data from Verisign (A, J root servers) on resolvers following RFC 8145, which allows a resolver to indicate which trust anchors it is using: a bigger number of resolvers still had only the current root KSK-2010 as a trust anchor
- The Internet Systems Consortium (ISC): some instances of BIND resolvers reporting trust anchor data were not doing DNSSEC validation: an implementation issue in recent versions caused BIND to not follow the instructions in RFC 8145 correctly
- NLnet Labs (Unbound developer): some users of the Unbound resolver could correctly configure the software to follow automatic KSK update by RFC 5011, but still not have the new key KSK-2017 on the day of the rollover (NLnet Labs recently updated their software to handle this, users of any earlier version would still be affected)
- ISC on earlier problem: some BIND users who believe that their resolver has automatically updated its configuration to trust KSK-2017 were only trusting KSK-2010. In some cases, BIND will start up and be unable to trust KSK-2017 but will provide no visible warning to that effect.

# Operational Implementation Plan Timeline (tentative)



# 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



# Automated Updates of DNSSEC Trust Anchors

- ◉ **Defined in Request For Comments 5011**

- ◉ Use the current trust anchor(s) to learn new
- ◉ To allow for unattended DNSSEC validator operations
- ◉ Based on "time" – if a new one appears and no one complains for some specified time, it can be trusted
- ◉ Highlight: defined "add hold" time is 30 days

- ◉ Operators are not required to follow Automated Updates  
=> <http://data.iana.org/root-anchors/>



# What Should Be Seen

---

- ⦿ **Two listed trust anchors for the root zone**
  - ⦿ KSK-2017, key-id 20326
    - ⦿ If you don't see this, the validator will fail at the rollover moment
  - ⦿ KSK-2010, key-id 19036
    - ⦿ If you don't see this, the validator is not working now!
- ⦿ **Eventually KSK-2010 will "go away"**

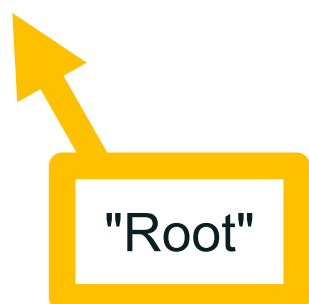
# Recognizing KSK-2017

◎ The KSK-2017's Key Tag (defined protocol parameter) 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 is:

. IN DNSKEY 257 3 8

AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxexF3  
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv  
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF  
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e  
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd  
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN  
R1AkUTV74bU=

"Root"

*Note: liberties taken with formatting for presentation purposes*

# E.g., BIND

```
bind-9.9.5-testconfig $ rndc -c rndc.conf secroots  
bind-9.9.5-testconfig $ cat named.secroots  
05-Sep-2017 09:24:06.361
```

Start view \_default

./RSASHA256/20326 ; managed

./RSASHA256/19036 ; managed

KSK-2017,  
aka 20326

KSK-2010,  
aka 19036



# E.g., Unbound

```
unbound $ cat root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1504239596 ;;Fri Sep  1 00:19:56 2017
;;last_success: 1504239596 ;;Fri Sep  1 00:19:56 2017
;;next_probe_time: 1504281134 ;;Fri Sep  1 11:52:14 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
. 172800 IN DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAYvMgJzkKTOiWlvkIbzxef3/4RgWOq7HrxRixF1ExOLAJr5c
mLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtKROxVQuCaSnIDdD5LKyWh7u2n9WGe2R8PzgCm3EgVLrjyBxWeLF
0jLHwVN8efS3rCj/EWgvIWgb9tarpYDK/b58Da+sqqls3eNbu7pr+eoZG+SrDK6nL3c6H5Apxz7IjVc1
uTIdsIXxuOLYA4/ilBmSVIzuDWfUfhHdY6+cn8HFRm+2h3AnXGXws9555KrUqihylGa8subX2m6UwN
RlAkUTV74bU= ;{id = 20326 (ksk), size = 2048b} ;;state=2 [ VALID ] ;;count=0
;;lastchange=1502438004 ;;Fri Aug 11 03:52:24 2017
. 172800 IN DNSKEY 257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxb0nVVLOyQbSEW008gcCjFFVQUTf6v58fLjwB0YI0EzrAcQqB
GCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaKVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apA7N9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjPJ8LbqF6dsV6DoB
Qzgul0sGICGOYl7OyQdXfZ57relageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBdfwhYB4N7knNnulq
QxA+Uk1ihz0= ;{id = 19036 (ksk), size = 2048b} ;;state=2 [ VALID ] ;;count=0
;;lastchange=1459820836 ;;Mon Apr  4 21:47:16 2016
```

KSK-2017,  
aka 20326

KSK-2010,  
aka 19036

Both are VALID

# Where to Get KSK-2017 Manually

---

- ◉ **Via the official IANA trust anchor XML file at <https://data.iana.org/root-anchors/root-anchors.xml>**
  - ◉ Contains the same information as a DS record for KSK-2017
  - ◉ Validate root-anchors.xml with the detached signature at <https://data.iana.org/root-anchors/root-anchors.p7s>
- ◉ **Via DNS (i.e., ask a root server for “./IN/DNSKEY”)**
  - ◉ Validate the KSK-2017 by comparison with other trusted copies



# Details on Checking Trust Anchors

---

© For further information, consult

<https://www.icann.org/dns-resolvers-checking-current-trust-anchors>

# How does one fix?

---

- ⦿ If one does not see both KSKs as trusted, then adjustments need to be made
- ⦿ "How to's" are tool and environment dependent

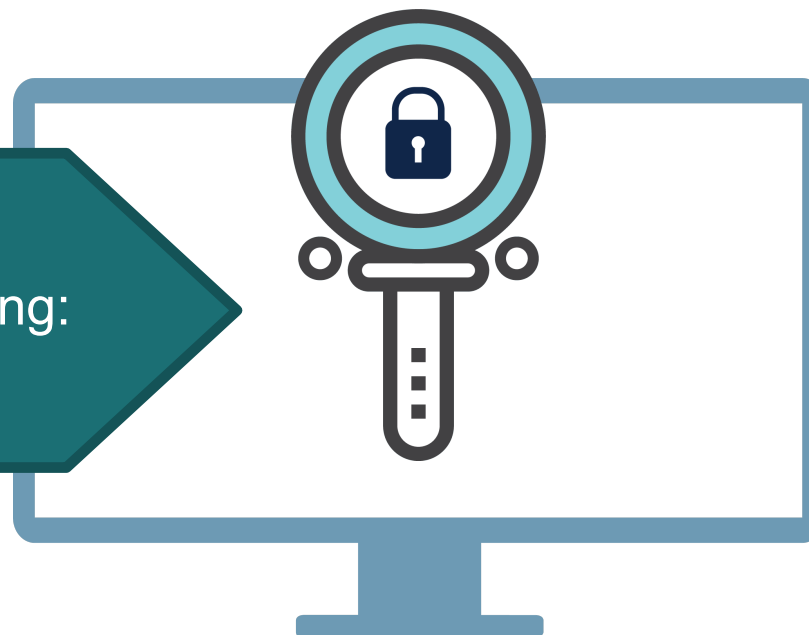
<https://www.icann.org/dns-resolvers-updating-latest-trust-anchor>

# 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:

- ◉ The goal is to test production resolvers with live test zones executing a KSK rollover in real time
- ◉ A full test lasts several weeks

Check to make sure  
your systems are ready by visiting:  
**[go.icann.org/KSKtest](https://go.icann.org/KSKtest)**



# 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](mailto:globalsupport@icann.org)
  - Subject line: “KSK Rollover”

# Engage with ICANN

---

Join the **ksk-rollover@icann.org** mailing list

**Archives:** <https://mm.icann.org/listinfo/ksk-rollover>

**KSK-Roll Website:** <https://www.icann.org/kskroll>



[@icann](https://twitter.com/icann) | **Follow #KeyRoll**



[facebook.com/icannorg](https://facebook.com/icannorg)



[youtube.com/icannnews](https://youtube.com/icannnews)



[flickr.com/icann](https://flickr.com/icann)



[linkedin/company/icann](https://linkedin/company/icann)



[slideshare/icannpresentations](https://slideshare/icannpresentations)

**Thank you!**

---

**And don't get locked out ;)**

**[Alexandra.kulikova@icann.org](mailto:Alexandra.kulikova@icann.org)**  
**[www.icann.org](http://www.icann.org)**