

# DNSSEC : Mise à jour importante

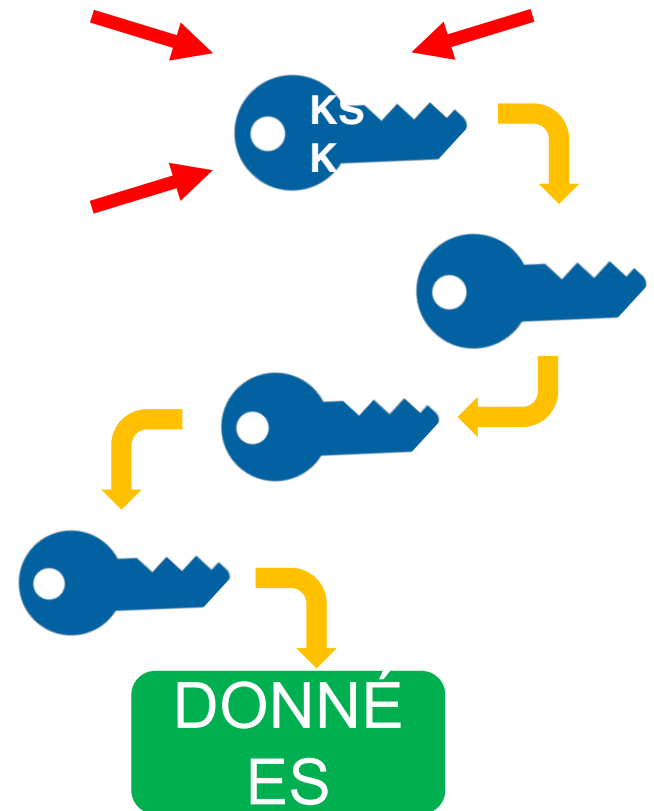
FFGI 2017  
Ouagadougou – Burkina Faso



# Roulement de la KSK : aperçu

## L'ICANN prépare la mise en place d'un roulement de la clé de signature de clé (KSK) des extensions de sécurité du système des noms de domaine (DNSSEC).

- ⊙ La clé de signature de clé « **KSK** » de DNSSEC de la zone racine est la clé cryptographique qui se trouve au-dessus de la hiérarchie de DNSSEC
- ⊙ La KSK est une paire de clés cryptographiques publique-privée :
  - Partie publique : point de départ fiable pour la validation de DNSSEC
  - Partie privée : signe la clé de signature de zone (ZSK)
- ⊙ Construit une « chaîne de confiance » des clés et des signatures successives afin de valider l'authenticité de n'importe quelles données signées de DNSSEC



# Pourquoi l'ICANN fait-elle le roulement de la KSK ?

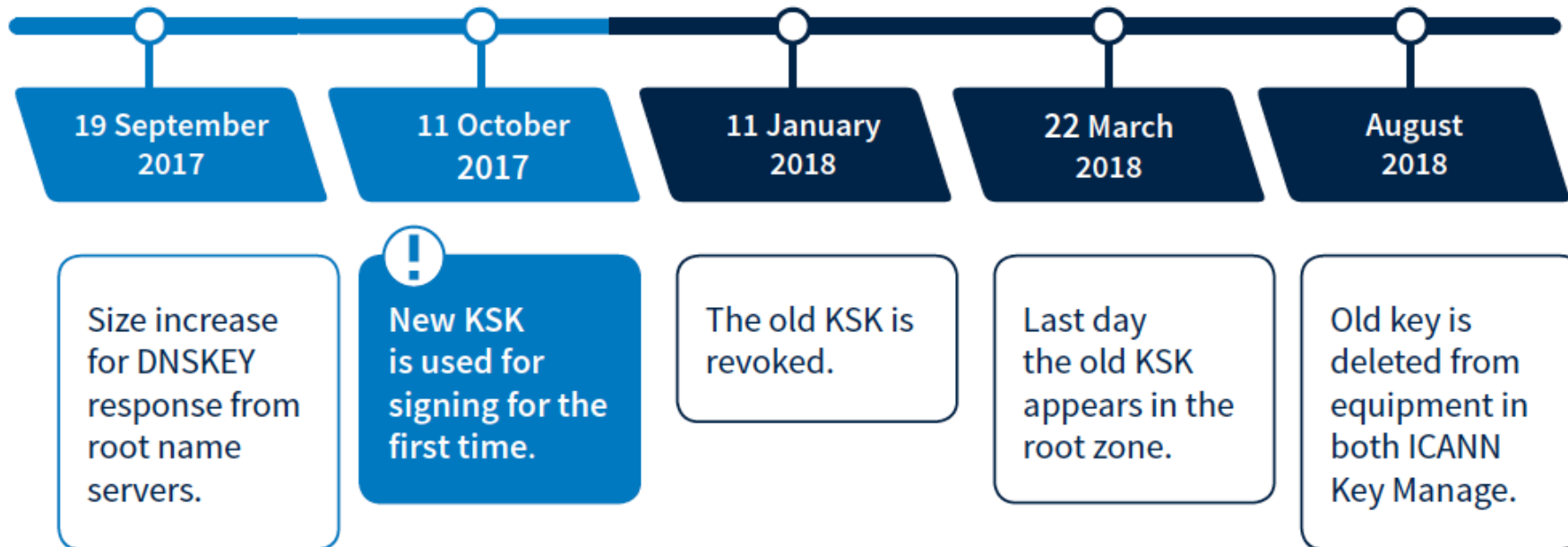
- ⊙ Comme pour les mots de passe, les clés cryptographiques utilisées dans les données DNS pour signer DNSSEC
  - Assure l'infrastructure pouvant supporter le changement de clé en cas d'urgence
- ⊙ Ce type de changement ne s'est jamais produit au niveau de la racine
  - Il existe une même KSK DNSSEC de la zone racine qui est fonctionnelle et opérationnelle depuis 2010
- ⊙ Le roulement doit être largement et soigneusement coordonné pour s'assurer qu'il n'interfère pas avec les opérations normales

# DNSSEC

# Quand le roulement aura-t-il lieu ?

## Le roulement de la KSK est un processus, pas un seul événement

Les dates suivantes sont les jalons clés du processus auxquels les utilisateurs finaux pourraient subir des interruptions des services Internet .



# Qui sera affecté ?

Les  
développeurs  
et distributeurs  
de logiciels  
pour le DNS

Les  
intégrateurs de  
systèmes

Les opérateurs  
de réseau

Opérateurs de  
serveur racine

Les  
fournisseurs  
de services  
Internet

Utilisateurs  
finaux  
*(si les opérateurs du  
résolveur ne prenaient  
aucune mesure)*

# Pourquoi devez-vous être préparé ?



Si vous avez activé la validation du DNSSEC, vous devez mettre à jour vos systèmes avec la nouvelle KSK pour garantir que les utilisateurs Internet pourront accéder à l'Internet sans aucun problème.

- ⦿ À l'heure actuelle, 25 % des utilisateurs mondiaux d'Internet, soit **750 millions de personnes**, utilisent des résolveurs de validation du DNSSEC qui pourraient être affectés par le roulement de la KSK.
- ⦿ Si ces résolveurs n'ont pas la nouvelle clé lors du roulement de la KSK, les utilisateurs finaux qui utilisent ces résolveurs rencontreront des erreurs et **ne pourront pas accéder à l'Internet**



# Que doivent faire les opérateurs ?



**Savoir si DNSSEC est activé dans vos serveurs**



**Savoir comment la confiance est évaluée dans vos opérations**



**Tester/vérifier vos configurations**



**Inspecter les fichiers de configuration, sont-ils (aussi) à jour ?**



**Si la validation de DNSSEC est activée ou prévue dans votre système**

- Avoir un plan pour participer au roulement de la KSK
- Connaître les dates, les symptômes, les solutions



# Comment mettre à jour votre système



Si votre logiciel prend en charge les mises à jour automatisées des ancrs de confiance de DNSSEC (RFC 5011) :

- ◉ La KSK sera mise à jour automatiquement, le moment venu
- ◉ Il n'est pas nécessaire de décider d'autres actions
  - ◉ Les dispositifs qui sont hors ligne au cours du roulement devront être mis à jour manuellement s'ils sont mis en ligne une fois que le roulement est terminé



Si votre logiciel ne prend pas en charge les mises à jour automatisées des ancrs de confiance de DNSSEC (RFC 5011) ou s'il n'est pas configuré pour les utiliser :

- ◉ L'ancre de confiance du logiciel doit être mise à jour manuellement
- ◉ La nouvelle KSK de la zone racine est disponible ici depuis mars 2017 :

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





# Vérifiez si vos systèmes sont prêts

L'ICANN propose un **banc d'essai** pour les opérateurs de réseau et autres parties souhaitant s'assurer que leurs systèmes peuvent gérer correctement le processus de mise à jour automatique.

Vérifiez que vos systèmes  
sont prêts en visitant :  
**[go.icann.org/KSKtest](https://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

# Trois étapes pour la récupération

Si votre validation DNSSEC a une défaillance après le roulement de la clé



## Arrêter les tickets

C'est OK de désactiver la validation de DNSSEC jusqu'à ce que le problème soit résolu (mais n'oubliez pas d'en faire la réactivation !)



## Débogage

Si le problème est l'ancre de confiance, cherchez pourquoi il n'est pas correct

- Le RFC 5011 a-t-il échoué ? Les outils de configuration n'ont pas réussi à mettre à jour la clé ?
- Si le problème est lié à la fragmentation, vérifiez que le TCP est activé et/ou faites d'autres ajustements au transport



## Test de récupération

Assurez-vous que vos corrections fonctionnent

# Pour plus d'information

---

1

Visitez <https://icann.org/kskroll>

2

**Joignez-vous aux conversations en ligne**

- Utilisez le hashtag #KeyRoll
- Inscrivez-vous à la liste de diffusion  
<https://mm.icann.org/listinfo/ksk-rollover>

3

**Posez votre question à [globalsupport@icann.org](mailto:globalsupport@icann.org)**

- Ligne objet : « Roulement de la KSK »

4

**Assistez à un événement**

- Visitez <https://features.icann.org/calendar> pour trouver les prochaines présentations sur le roulement de la KSK dans votre région

# Autres diapos techniques

# Reconnaître la KSK-2017

- ◉ L'étiquette de la clé de la KSK-2017 est

20326

- ◉ L'enregistrement relatif à la signature de délégation (DS) pour la KSK-2017 est

• IN DS 20326 8 2  
E06D44B80B8F1D39A95C0B0D7C65D084  
58E880409BBC683457104237C7F8EC8D

« Racine »

Remarque : licenses prises avec le formattage aux fins de la présentation



# KSK-2017 dans un enregistrement de ressource DNSKEY

⊙ L'enregistrement de ressource DNSKEY sera :

• IN DNSKEY 257 3 8

AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxexF3  
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv  
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF  
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbu7pr+e  
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd  
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN  
R1AkUTV74bU=

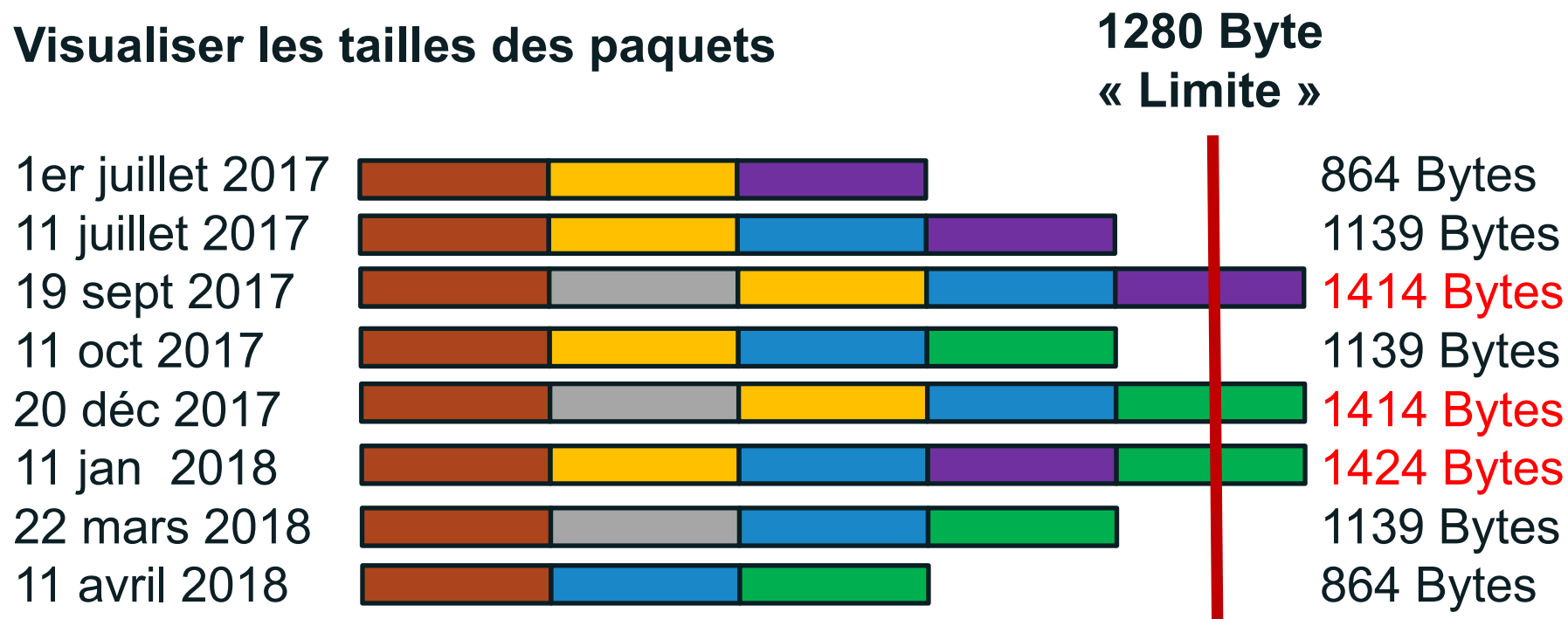
« Racine »

*Remarque : licenses prises avec le formatage aux fins de la présentation*



# Impact sur le processus de roulement de la KSK

## Visualiser les tailles des paquets



## Root Zone Key Signing Key (KSK) Rollover

### KSK rollover at a glance

ICANN is planning to roll, or change, the "top" pair of cryptographic keys used in the Domain Name System Security Extensions (DNSSEC) protocol, commonly known as the [Root Zone KSK](#). This will be the first time the KSK has been changed since it was initially generated in 2010.

Changing these DNSSEC keys is an important security step, in much the same way that regularly changing passwords is considered a prudent practice by any Internet user.

The root zone KSK consists of a private key and a public key. The private component is securely stored by ICANN, but the public component is widely distributed and configured in a large number of devices, possibly numbering in the millions. The multi-step KSK rollover process basically involves generating a new cryptographic key pair and then distributing the new public key.

Internet service providers, enterprise network operators and others performing DNSSEC validation must ensure their systems are updated with the public part of the new KSK in order to assure trouble-free Internet access for their users.

The KSK is an essential component of DNSSEC, a security technology that authenticates the integrity of information within the Domain Name System (DNS), which is the Internet's global phone book. This type of change has never before occurred at the root level, so the rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations. For this reason, ICANN is informing the Internet operator and user communities about the changes now, before the rollover actually occurs.

### What role does the KSK play in DNSSEC?

The KSK plays an important role in protecting Internet users from domain name hijacking by validating DNS data. As the phrase implies, domain name hijacking is taking control of a domain name, often by those with malicious intent who may be seeking illicit financial gain. For example, attempts to access bank account information may result in redirecting users to a site that steals identification and passwords.

## Liens :

- **EN** : <https://www.icann.org/en/system/files/files/ksk-rollover-at-a-glance-22jul16-en.pdf>
- **ES** : <https://www.icann.org/es/system/files/files/ksk-rollover-at-a-glance-22jul16-es.pdf>
- **FR** : <https://www.icann.org/fr/system/files/files/ksk-rollover-at-a-glance-22jul16-fr.pdf>
- **AR** : <https://www.icann.org/ar/system/files/files/ksk-rollover-at-a-glance-22jul16-ar.pdf>
- **PT** : <https://www.icann.org/pt/system/files/files/ksk-rollover-at-a-glance-22jul16-pt.pdf>
- **RU** : <https://www.icann.org/ru/system/files/files/ksk-rollover-at-a-glance-22jul16-ru.pdf>
- **ZH** : <https://www.icann.org/zh/system/files/files/ksk-rollover-at-a-glance-22jul16-zh.pdf>



# Question/Réponses

## KSK Rollover: Questions and Answers

### What is the Key Signing Key?

- The Root Zone Key Signing Key (KSK) is a cryptographic public-private key pair that plays an important role in the Domain Name System Security Extensions (DNSSEC). The Root Zone KSK serves as the trusted starting point for DNSSEC validation, similar to how the root zone serves as the starting point for DNS resolution.
- Just as one starts at the root zone to resolve a domain name anywhere in DNS, software performing DNSSEC validation trusts the root zone KSK and builds a "chain of trust" of successive keys and signatures to validate the authenticity of any signed data in DNS.

### What does the Key Signing Key (KSK) rollover involve?

- The KSK rollover process updates the root zone trust anchor by introducing a new KSK (KSK-2017) into the root zone.

### Why roll the KSK?

- Because it's not good for a cryptographic key to live forever. Like any password, it needs to be changed sometimes.
- Because it's better to make proactive changes during normal operations when things are running smoothly, rather than be reactive in an emergency.
- When DNSSEC was first deployed in 2010, NTIA required that the KSK be rolled and the Root Zone Management Partners subsequently outlined requirements to change the key after five years of operations. The role of NTIA ended on 1 October 2016.

### Who needs to know about the KSK rollover?

- Internet service providers, enterprise network operators and others who operate DNSSEC validation must update their systems with the public part of the new key signing key.

### How will they know?

- ICANN is executing an extensive outreach campaign to ensure that those who currently use the KSK know about the change.
- Interested parties can view a [schedule of events](#) at which the rollover will be discussed on the ICANN website, where they can also follow [KSK updates](#) and join a special mailing list. They can also follow the hashtag #KeyRoll on social media to stay informed.

### What's the impact on Internet users?

- If completed smoothly, there will be no visible change for the end user.

### What could go wrong?


- It's possible that some software performing DNSSEC validation will not be updated with

## Liens :


- **EN :**  
<https://www.icann.org/en/system/files/files/ksk-rollover-questions-answers-31oct16-en.pdf>
- **ES :** <https://www.icann.org/resources/pages/ksk-rollover-2016-07-27-es>
- **FR :** <https://www.icann.org/fr/system/files/files/ksk-rollover-questions-answers-31oct16-fr.pdf>
- **AR :**  
<https://www.icann.org/ar/system/files/files/ksk-rollover-questions-answers-31oct16-ar.pdf>
- **PT :** <https://www.icann.org/pt/system/files/files/ksk-rollover-questions-answers-31oct16-pt.pdf>
- **RU :**  
<https://www.icann.org/ru/system/files/files/ksk-rollover-questions-answers-31oct16-ru.pdf>
- **ZH :**  
<https://www.icann.org/zh/system/files/files/ksk-rollover-questions-answers-31oct16-zh.pdf>

# Petit guide pour les opérateurs

Liens : (à déterminer)




## Quick Guide: Prepare Your Systems for the Root KSK Rollover



### What is the Root KSK Rollover?

The Internet Corporation for Assigned Names and Numbers (ICANN) is planning to roll, or change, the “top” pair of cryptographic keys used in the Domain Name System Security Extensions (DNSSEC) protocol, commonly known as the Root Zone KSK. This will be the first time the KSK has been changed since it was initially generated in 2010, and is considered an important security step, in much the same way that regularly changing passwords is considered a prudent practice by any Internet user.

Changing the key involves generating a new cryptographic key pair and distributing the new public component to DNSSEC-validating resolvers. As every Internet query using DNSSEC depends on the root zone KSK to validate the destination, this will be a significant change. Once the new keys have been generated, web operators, such as ISPs, will need to update their systems with the new key so that when a user attempts to visit a website, it can validate it against the new KSK.




### Why You Need to Prepare

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.

If you don't use DNSSEC, your system will not be affected by the rollover. However, you should know that DNSSEC is an important part of preventing domain name hijacking. [Learn more about implementing DNSSEC here.](#)

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](https://go.icann.org/KSKtest).



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

Designed by ICANN Communications | March 2017Creative Commons Attribution - NonCommercial

# Vidéo d'information



## Liens :

- **EN** : Prepare Your Systems for the Root KSK Rollover  
<https://youtu.be/d7H1AkC9Plw>
- **ES** : Prepare sus Sistemas para el Traspaso de la Clave para la Firma de la Llave de la Zona Raíz (KSK)  
<https://youtu.be/cAPyLI1qowY>
- **PT** : Preparem seus sistemas para a implementação da KSK da raíz  
<https://youtu.be/AysAHXAEJFM>
- **FR** : Préparer vos systèmes pour le roulement de la KSK de la racine  
<https://youtu.be/Lph39UgS7e4>

# Annonce de lancement du banc d'essai de l'ICANN

## ICANN Launches Testing Platform for the KSK Rollover

This page is available in: [Русский](#) | [Español](#) | [Français](#) | [中文](#) | [العربية](#) | [English](#)

in f t d e +

**13 March 2017** – ICANN is offering a testing platform for network operators and other interested parties to confirm that their systems can handle the automated update process for the upcoming Root Zone Domain Name Systems Security Extensions (DNSSEC) Key Signing Key (KSK) rollover. **The KSK rollover is currently scheduled for 11 October 2017.**

"Currently, seven hundred and fifty million people are using DNSSEC-validating resolvers that could be affected by the KSK rollover," said ICANN's Vice President of Research, Matt Larson. "The testing platform is an easy way for operators to confirm that their infrastructure supports the ability to handle the rollover without manual intervention."

Internet service providers, network operators and others who have enabled DNSSEC validation must update their systems with the new KSK. This can be done in one of two ways:

- An operator can configure a new trust anchor *manually* by obtaining the new root zone KSK from the [iana.org](https://www.iana.org/dnssec/files) website at <https://www.iana.org/dnssec/files>.
- An operator can enable a feature available in many validating resolvers that *automatically* detects and configures a new root zone KSK as a trust anchor, in which case they need take no action.

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

The KSK has been widely distributed and configured by every operator performing DNSSEC validation. If the validating resolvers using DNSSEC 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. A careful and coordinated effort is required to ensure that the update does not interfere with normal operations.

More information is available at [www.icann.org/kskroll](https://www.icann.org/kskroll).

## Liens :

- **EN** : <https://www.icann.org/news/announcement-2017-03-13-en>
- **ES** : <http://www.icann.org/news/announcement-2017-03-13-es>
- **FR** : <http://www.icann.org/news/announcement-2017-03-13-fr>
- **AR** : <http://www.icann.org/news/announcement-2017-03-13-ar>
- **RU** : <http://www.icann.org/news/announcement-2017-03-13-ru>
- **ZH** : <https://www.icann.org/news/announcement-2017-03-13-zh>