Root KSK Rollover 2026

An Operator’s Readiness Checklist

Roy Arends, ICANN

NOG.FI --- 16 June 2026

DNSSEC overview

- A hierarchical public key cryptography system that matches the hierarchical delegation of the DNS itself.
- At the top of this hierarchy is the Root Zone Key Signing Key (KSK), the single trust anchor for the DNSSEC system.
- ICANN manages this key through a highly transparent process, including public key signing ceremonies and an open design model.

Why You Should Care

- DNSSEC validation depends on **root trust anchor**
  - The root has been signed since 2010
  - First rollover since 2018
  - Second root KSK rollover overall
- Automated root KSK rollover depends on RFC5011 processes
- This is a planned, routine event
- Your job: make sure your resolvers follow along

What is Rolling Over

- Root zone **KSK (Key Signing Key)**
- Managed by ICANN
- Part of the DNSSEC chain of trust
- Since it happens infrequently, it is easy to forget operational details.
- We plan to do this every 3 years

Timeline

- 2016: 1st rollover prep: generated KSK-2017

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- 2017: 1st rollover with KSK-2017

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- 2020: 2nd rollover prep (for ‘21 roll)

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- 2021: 2nd rollover prep (for '21 roll)

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- ~~2021: 2nd rollover prep (for '21 roll)~~ Still covid

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- ~~2021: 2nd rollover prep (for '21 roll)~~ Still covid
- 2022: resumption of normal operations (face to face ceremonies again)

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- ~~2021: 2nd rollover prep (for '21 roll)~~ Still covid
- 2022: resumption of normal operations (face to face ceremonies again)
- 2023: 2nd rollover, generated KSK-2023

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- ~~2021: 2nd rollover prep (for '21 roll)~~ Still covid
- 2022: resumption of normal operations (face to face ceremonies again)
- ~~2023: 2nd rollover, generated KSK-2023~~ Abandoned KSK due to HSM EOL

Timeline

- 2016: 1st rollover prep: generated KSK-2017
- ~~2017: 1st rollover with KSK-2017~~ Extended to 2018 due to noisy metrics
- 2018: 1st rollover with KSK-2017 Success
- ~~2020: 2nd rollover prep (for '21 roll)~~ TCRs could not travel due to covid
- ~~2021: 2nd rollover prep (for '21 roll)~~ Still covid
- 2022: resumption of normal operations (face to face ceremonies again)
- ~~2023: 2nd rollover, generated KSK-2023~~ Abandoned KSK due to HSM EOL
- 2024: 2nd rollover, generated KSK-2024 Success

Timeline

• 2016: 1st rollover prep: generated KSK-2017	
~~• 2017: 1st rollover with KSK-2017~~	Extended to 2018 due to noisy metrics
• 2018: 1st rollover with KSK-2017	Success
~~• 2020: 2nd rollover prep (for '21 roll)~~	TCRs could not travel due to covid
~~• 2021: 2nd rollover prep (for '21 roll)~~	Still covid
• 2022: resumption of normal operations	(face to face ceremonies again)
~~• 2023: 2nd rollover, generated KSK-2023~~	Abandoned KSK due to HSM EOL
• 2024: 2nd rollover, generated KSK-2024	Success
• 2025: published KSK-2024 in the root zone	(on 11th January)

Timeline

• 2016: 1st rollover prep: generated KSK-2017	
~~• 2017: 1st rollover with KSK-2017~~	Extended to 2018 due to noisy metrics
• 2018: 1st rollover with KSK-2017	Success
~~• 2020: 2nd rollover prep (for '21 roll)~~	TCRs could not travel due to covid
~~• 2021: 2nd rollover prep (for '21 roll)~~	Still covid
• 2022: resumption of normal operations	(face to face ceremonies again)
~~• 2023: 2nd rollover, generated KSK-2023~~	Abandoned KSK due to HSM EOL
• 2024: 2nd rollover, generated KSK-2024	Success
• 2025: published KSK-2024 in the root zone	(on 11th January)
• 2025: RFC5011 resolvers trust KSK2024	(from 10th February)

Timeline

• 2016: 1st rollover prep: generated KSK-2017	
~~• 2017: 1st rollover with KSK-2017~~	Extended to 2018 due to noisy metrics
• 2018: 1st rollover with KSK-2017	Success
~~• 2020: 2nd rollover prep (for '21 roll)~~	TCRs could not travel due to covid
~~• 2021: 2nd rollover prep (for '21 roll)~~	Still covid
• 2022: resumption of normal operations	(face to face ceremonies again)
~~• 2023: 2nd rollover, generated KSK-2023~~	Abandoned KSK due to HSM EOL
• 2024: 2nd rollover, generated KSK-2024	Success
• 2025: published KSK-2024 in the root zone	(on 11th January)
• 2025: RFC5011 resolvers trust KSK2024	(from 10th February)
• 2026: October 11th (Sunday, sorry)	KSK2024 first use

Timeline

- 2018: 1st rollover with KSK-2017 Success

If you want to make the Gods laugh, show him your plans.

How RFC5011 works

- A new KSK is published, the current KSK signs the keyset
  - A keyset contains zone and key signing keys
- After a while, resolvers trust the new KSK
  - Since they trust the old KSK
- After a while, the new KSK signs the set of keys
  - It becomes the current key, while the old key will still be present
- After a while, the old KSK will have the “revoke” bit set
  - This is a signal to validators that the old KSK is invalid
- After a while, the old KSK will be removed from the set of keys

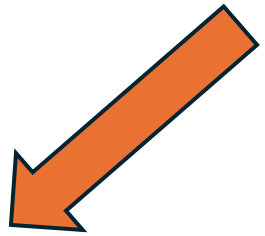
How long is “a while”

- A new KSK is published, the current KSK signs the keyset
  - January 11, 2025; KSK-2024 published in the root zone
- After a while, resolvers trust the new KSK
  - February 10, 2025; KSK-2024 trusted via 5011
- After a while, the new KSK signs the set of keys
  - October 11, 2026; KSK-2024 will start signing, KSK-2017 will stop
- After a while, the old KSK will have the “revoke” bit set
  - January 11, 2027; KSK-2017 will have the revoke bit set.
- After a while, the old KSK will be removed from the set of keys
  - March 22, 2027; KSK-2017 will be removed

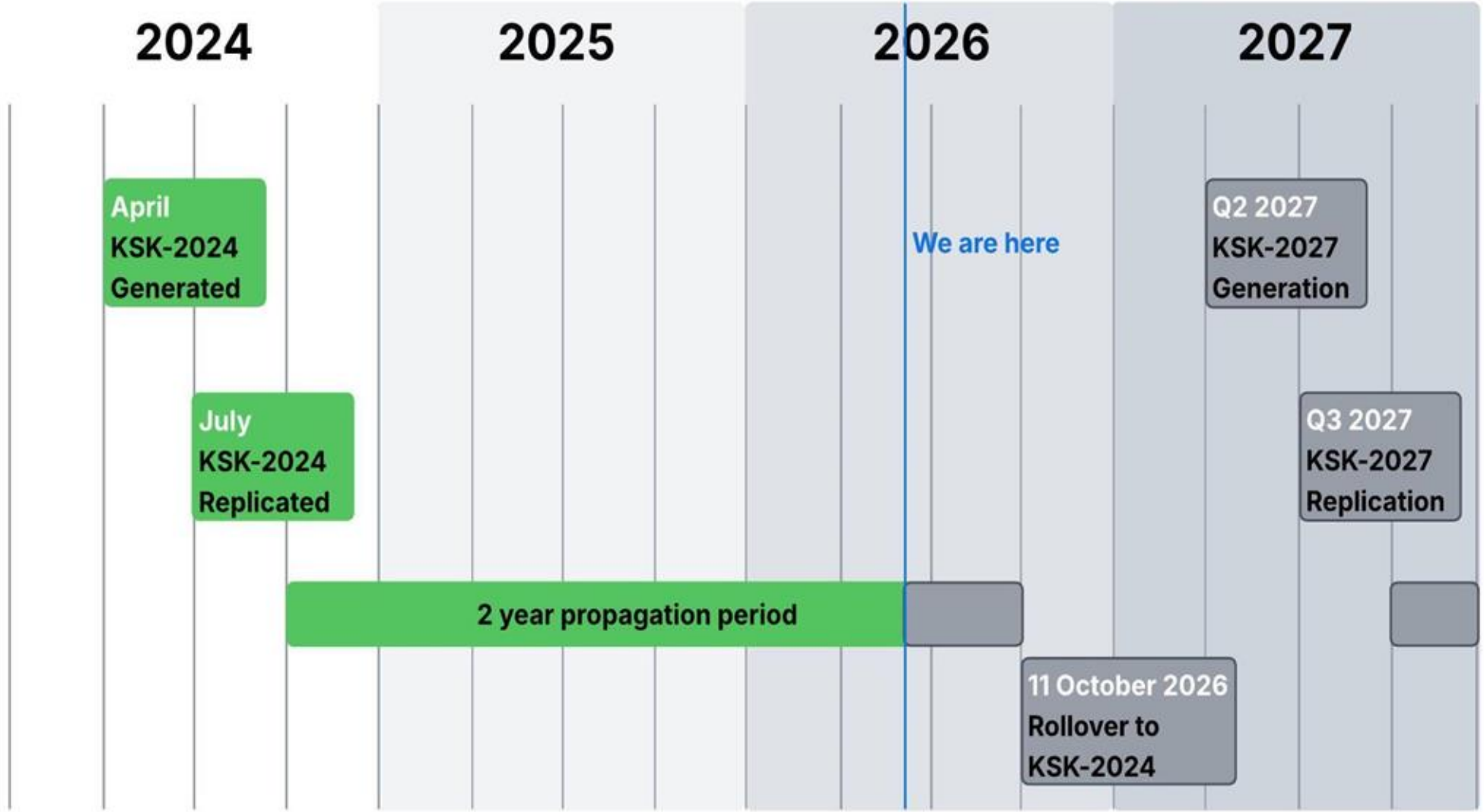
How long is “a while”

- A new KSK is published, the current KSK signs the keyset
  - January 11, 2025; KSK-2024 published in the root zone
- After a while, resolvers trust the new KSK
  - February 10, 2025; KSK-2024 trusted via 5011
- After a while, the new KSK signs the set of keys
  - October 11, 2026; KSK-2024 will start signing, KSK-2017 will stop
- After a while, the old KSK will have the “revoke” bit set
  - January 11, 2027; KSK-2017 will have the revoke bit set.
- After a while, the old KSK will be removed from the set of keys.
  - March 22, 2027; KSK-2017 will be removed

This is why I’m here!

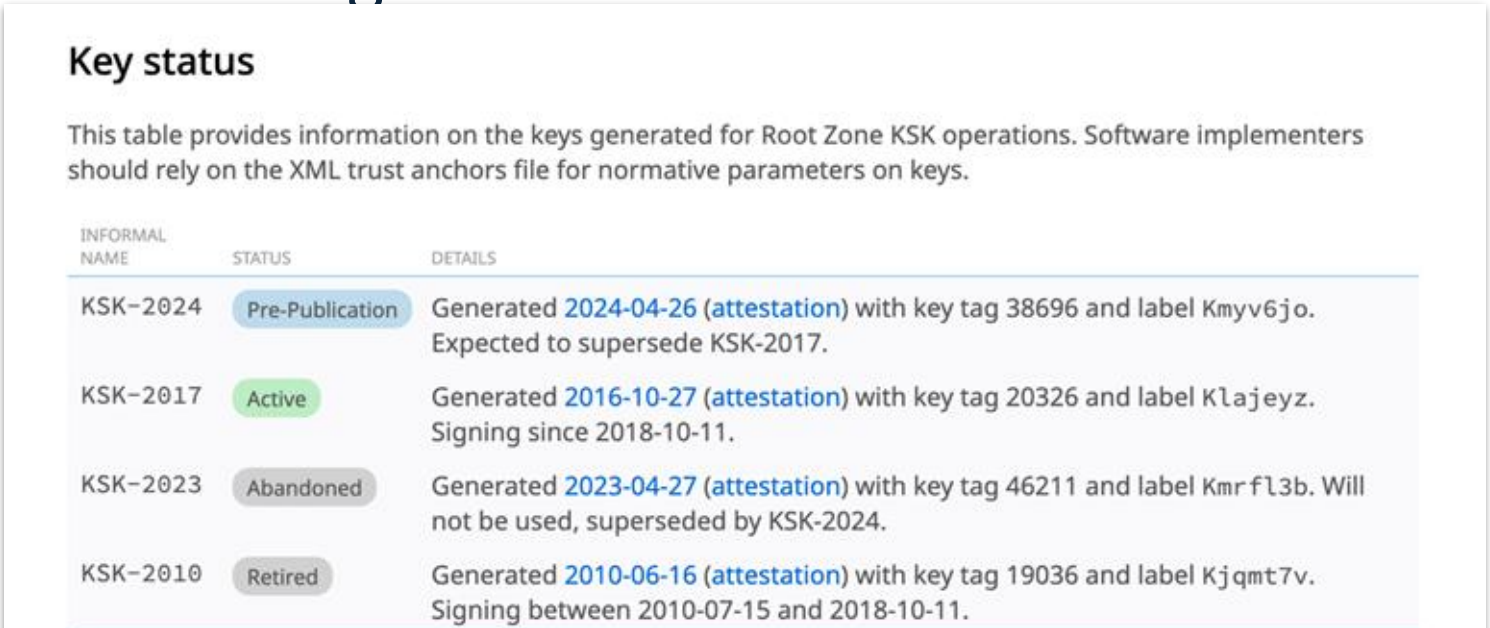


Timeline


2024
2025
2026
2027
April
KSK-2024
Generated
July
KSK-2024
Replicated
We are here
Q2 2027
KSK-2027
Generation
Q3 2027
KSK-2027
Replication
2 year propagation period
11 October 2026
Rollover to
KSK-2024

DNS Trust Anchor Availability

- The trust anchor is available for distribution (XML file)
  - Most users adopt it automatically via software updates
  - Published in the root zone since 11 January 2025
  - See RFC7958
- https://www.iana.org/dnssec/files



Key status

This table provides information on the keys generated for Root Zone KSK operations. Software implementers should rely on the XML trust anchors file for normative parameters on keys.

INFORMAL NAME	STATUS	DETAILS
KSK-2024	Pre-Publication	Generated 2024-04-26 (attestation) with key tag 38696 and label Kmyv6jo. Expected to supersede KSK-2017.
KSK-2017	Active	Generated 2016-10-27 (attestation) with key tag 20326 and label Klajeyz. Signing since 2018-10-11.
KSK-2023	Abandoned	Generated 2023-04-27 (attestation) with key tag 46211 and label Kmrfl3b. Will not be used, superseded by KSK-2024.
KSK-2010	Retired	Generated 2010-06-16 (attestation) with key tag 19036 and label Kjqmt7v. Signing between 2010-07-15 and 2018-10-11.

If your software is up to date: BIND

- BIND validates and uses RFC5011 by default.
- Included since BIND 9.18.33+, BIND 9.20.4+
- Check your status:
  - “rndc managed-keys status”
- You should see:

```
$ rndc managed-keys status
view: _default
next scheduled event: …
    name: .
    keyid: 20326
       algorithm: RSASHA256
       flags: SEP
       …
    keyid: 38696
       algorithm: RSASHA256
       flags: SEP
       …
```

If your software is up to date: Unbound

- Unbound validates and uses RFC5011 by default.
- Included since Unbound 1.21.0
- Check your status:
  - “unbound-anchor -l”
- You should see:

```
$ unbound-anchor -l
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
. IN DS 38696 8 2 683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16
```

If your software is up to date: knot-resolver

- knot Resolver (kresd) validates and uses RFC5011 by default.
- Included since 5.7.4 / 6.0.8
- Check your status:
  - “trust_anchors.summary()”
- You should see:

```
> trust_anchors.summary()
'.                      86400     DNSKEY    257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8
Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3
eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihy
lGa8subX2Nn6UwNR1AkUTV74bU= ; Valid: ; KeyTag:20326
.                       86400     DNSKEY    257 3 8
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJNnOAlFNKF2jBosZBU5eeHspaQWOmOElZsjICMQMC
3aeHbGiShvZsx4wMYSjH8e7Vrhbu6irwCzVBApESjbUdpWWmEnhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge71M
3ej2/7CPqpdVwuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxPvYLw4z9mR7K2v
aF18UYH9Z9GNUUeayffKC73PYc= ; Valid: ; KeyTag:38696
```

If your software is up to date: pdns-recursor

- pdns-recursor validates by default
- Included since 5.2.0
- Does not use RFC5011
- Check your keys:
  - “rec_control get-tas”
- You should see:

```
$rec_control get-tas
Configured Trust Anchors:
.
            20326 8 2 e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d
            38696 8 2 683d2d0acb8c9b712a1948b27f741219298d0a450d612c483af444a4c0fb2b16
```

Check if your software is up to date

Resolver	First Release with KSK-2024	RFC 5011	Key File
Unbound	1.21.0 (August 15, 2024)	Yes	root.key
Knot Resolver	5.7.4 / 6.0.8 (Late 2024)	Yes	root.keys
BIND	9.18.33 / 9.20.4 (January 2025)	Yes	bind.keys / managed-keys.bind
PowerDNS Recursor	5.2.0-alpha1 (Nov 11, 2024) / 5.2.0 (Jan 14, 2025)	No	root.key

In summary

- 11 October 2026, KSK roll
- Subsequently every 3 years
  - 2029, 2032, 2035 etc
- The ZSK rolls every 3 months
  - Independent of the KSK roll
  - You don’t have to do anything for this

In summary

- 11 October 2026, KSK roll
- Subsequently every 3 years
  - 2029, 2032, 2035 etc
- The ZSK rolls every 3 months
  - Independent of the KSK roll
  - You don’t have to do anything for this

- Oh, and we have a plan for Algorithm roll as well

Algorithm Roll

- Different beast altogether
  - A future rollover (potentially 2029) may include an algorithm rollover
- We’re rolling to Algorithm 13 (ECDSAP256SHA256)
- We need to roll the ZSK at the same time
- This causes an increase in DNS message size
  - Over the 1232 EDNS response size default
  - Which causes a significant fallback to TCP
- So the RSA ZSK will be reduced to 1536 bits
  - Which keeps TCP fallback at a manageable level for root server operators

Questions?

- roy.arends@icann.org