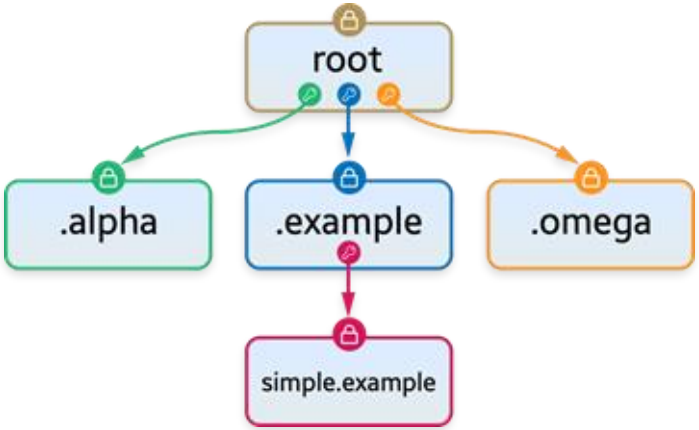
Root Zone KSK Rollover

Champika Wijayatunga, ICANN

26 July 2026

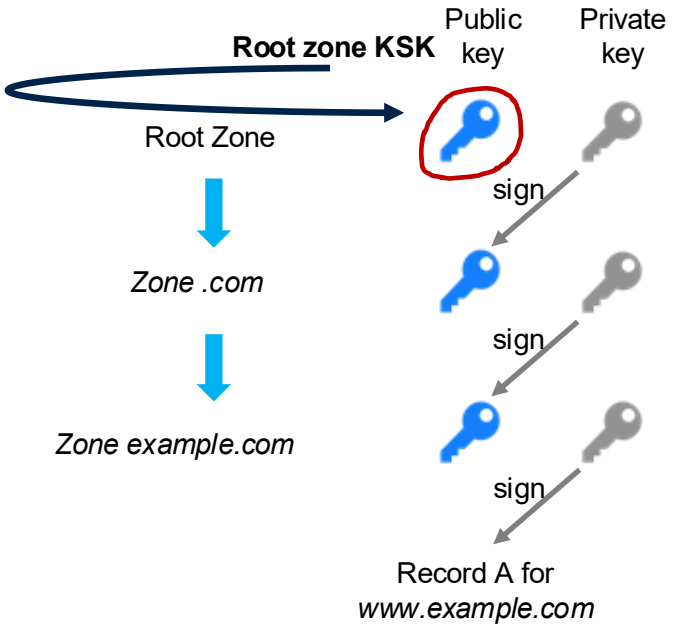
DNSSEC and the Chain of Trust



DNSSEC relies on a chain of trust, where each parent zone authenticates its child zones.

Since the root zone has no parent, its signature must be validated through a trusted mechanism.

Chain of Trust (DS):



Root Signing Process

DNS Security Extensions (DNSSEC) constitute a hierarchical public-key cryptographic system that mirrors the hierarchical delegation of the DNS itself. At the apex of this hierarchy resides the Root Zone Key Signing Key (KSK), the sole anchor of trust for the DNSSEC system.

This key is managed through a highly transparent process, which includes public-key signing ceremonies and an open design model.

Understanding the Root KSK Rollover

Key Reasons

Why this matters:

- Cryptographic keys should be updated periodically
- Planned maintenance is safer than emergency replacement
- Regular updates strengthen long-term DNS security and resilience

What Happens During the Rollover?

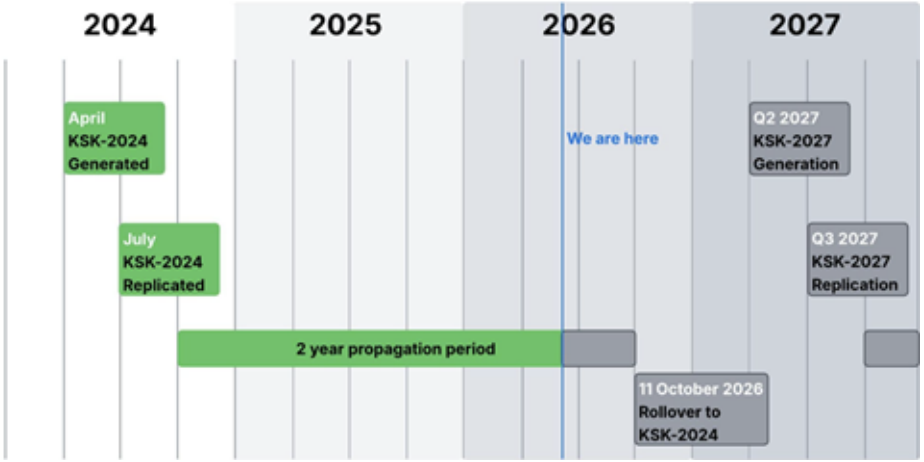
High-level rollover process

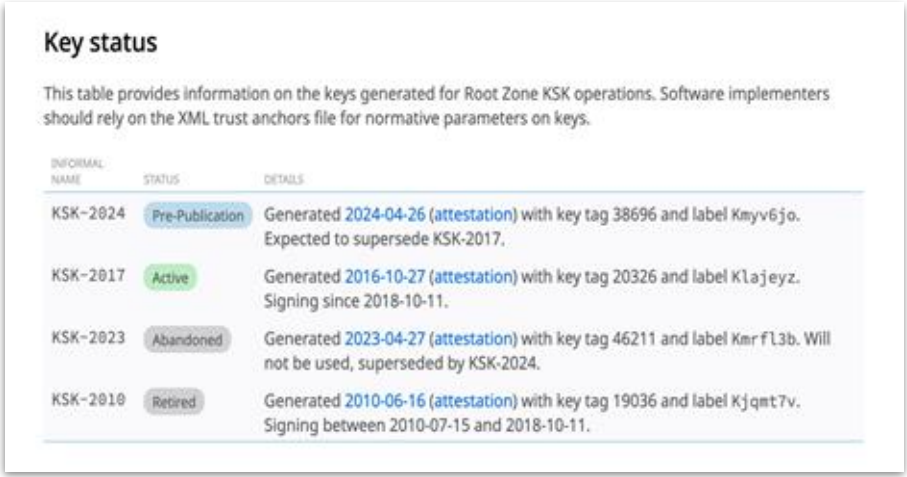
- New KSK is generated
- New KSK is published in the root zone
- Resolvers learn the new trust anchor
- Root zone signatures transition to the new KSK

Root Zone KSK Rollover Timeline

The KSK rollover:

- Introduces a new root zone KSK (KSK-2024)
- Updates the DNS root trust anchor
- Gradually transitions systems to trust the new key





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.

When?

11 OCTOBER

Who Needs to Take Action?

Organizations operating DNSSEC-validating resolvers, including:

- Internet Service Providers (ISPs)
- Enterprise network operators
- DNS service providers
- Software developers

Key action:

Ensure systems trust the new KSK

Recommended Operator Actions

Operators and developers should:

- Verify RFC 5011 support
- Test resolver behavior
- Monitor rollover updates
- Update trust anchors where needed

ICANN also provides:

- Operational testing resources
- Trust anchor publication files
- Technical guidance and outreach

What Could Happen if Systems are Unprepared?

Potential issues:

- Validation failures
- SERVFAIL responses
- DNS lookup failures
- User-facing connectivity problems

To protect stability:

- Rollout may pause
- Phases may be extended
- Changes may be temporarily reversed if necessary

Goal: A seamless transition for Internet users

Trust Anchor Management

Trust anchors are critical for validation

Resolvers using RFC 5011 can:

- Automatically learn new trust anchors
- Update trust anchors without manual intervention

Resolvers not using RFC 5011 may require:

- Manual trust anchor updates
- Configuration validation
- Additional operational testing

Risk: Resolvers without the new trust anchor may return SERVFAIL responses.

What Operators Should Monitor

Expected behavior and operational monitoring

Prepared resolvers should:

- Transition automatically
- Continue validating normally
- Experience no service disruption

Operators should monitor for:

- SERVFAIL increases
- Validation failures
- Resolver log anomalies
- Unexpected traffic patterns

Lessons From the 2018 Rollover

Key lessons learned

The 2018 rollover demonstrated:

- Preparation and outreach matter
- Most operators transitioned successfully
- User impact was minimal
- Monitoring and flexibility are essential

Operator Preparation Checklist

Preparation checklist

- ✓ Verify RFC 5011 support
- ✓ Confirm trust anchor configuration
- ✓ Test validating resolvers
- ✓ Review monitoring and alerting
- ✓ Update operational documentation
- ✓ Follow ICANN and IANA updates

Takeaways and Resources

Takeaways

- The root zone KSK rollover is planned security maintenance
- Prepared resolvers should transition smoothly
- RFC 5011 significantly reduces operational burden
- Monitoring and testing remain essential
- Community coordination supports DNS stability

Resources:

- ICANN root zone KSK rollover page
- IANA trust anchor resources
- KSK rollover mailing list
- globalsupport@icann.org

ICANN Webpage and Social Media Links


icann.org


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin.com/company/icann


instagram.com/icannorg