

Root KSK Rollover 2026

An Operator's Readiness Checklist

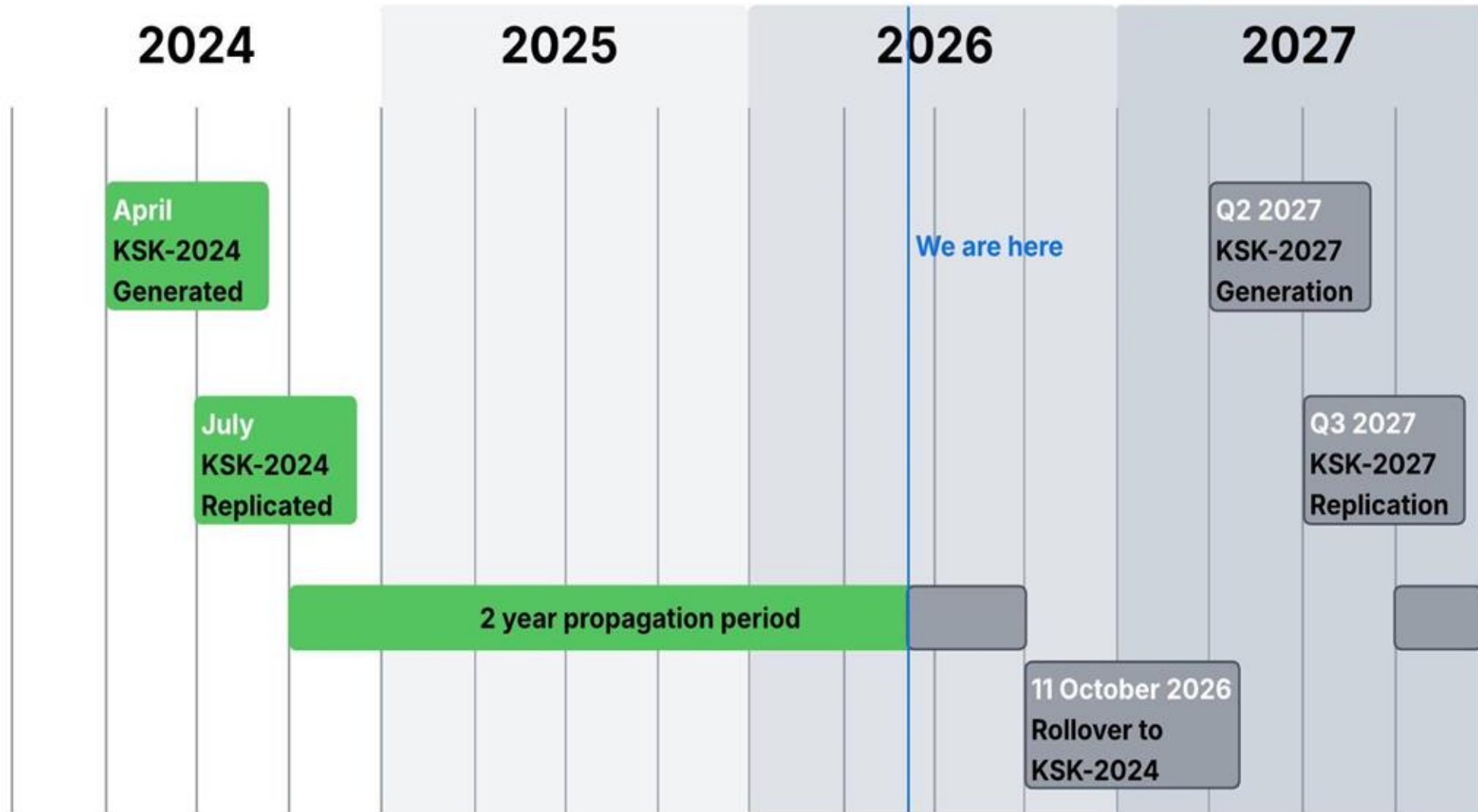
Roy Arends, ICANN

DNS-OARC May 2026

Why You Should Care

- DNSSEC validation depends on **root trust anchor**
 - The root has been signed since 2010
 - First rollover since 2018
 - Second rollover since the start
- Automated root KSK rollover depends on RFC5011 processes
- This is a planned, routine event
- Your job: make sure your resolvers follow along
- Our intent is to rollover ever 3 years.

Timeline



How does “5011” work

- A new KSK is published, the current KSK signs the set of keys
 - A set contains zone and key signing keys
- After a while the new KSK signs the set of keys
 - It becomes the current key
 - 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”

- January 11, 2025: DNSKEY “KSK-2024” in the root zone
- February 10, 2025: KSK-2024 should be trusted via 5011
- October 11, 2026: KSK-2024 will start signing
KSK-2017 will stop signing
- January 11, 2027: KSK-2017 is scheduled to be revoked

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 K1ajeyz. 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 Will not be used, superseded by KSK-2024.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.

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	Built-in only

Questions