

Root KSK Rollover — Resolver Evidence Worksheet

One row per validating endpoint, forwarders included. Record three separate results: **Configured** (KSK-2024, key tag 38696, is in the trust-anchor source), **Runtime** (the running process loaded it), **Behavioral** (RFC 8509 sentinel three-query test and a known-signed name returned with the ad flag). A row is PASS only when all three are recorded with evidence, plus a UTC timestamp and an owner. Unchecked = FAIL until evidenced.

Endpoint (resolver / forwarder)	Software + version	Validates on	Anchor mgmt	Config-ured Y/N/—	Runtime Y / N / —	Behavioral Pass / Fail / Indet.	Evidence (command, output ref, query path)	Checked (UTC)	Owner	Verdict

Validates on: this host / upstream / both. Anchor mgmt: RFC 5011 managed / static file / firmware / image-baked / unknown. Schedule: KSK-2017 revocation 2027-01-11 and removal 2027-03-22 are IANA-scheduled dates; re-run this worksheet at both.

Command reference — verify against your software version

Checks marked (tested) were run on Ubuntu 24.04 packages: BIND 9.18.39, Unbound 1.19.2, PowerDNS Recursor 4.9.3, Knot Resolver 5.7.2. None of those hosts could reach the root servers, so initialization-dependent output was not observed.

Result	Software	Check	Note
Configured	BIND	Inspect bind.keys for <i>initial-ds 38696</i> , or your trust-anchors statement (tested)	bind.keys carried initial-key 20326 and initial-ds 38696 on 9.18.39.
Configured	Unbound	Inspect auto-trust-anchor-file (commonly root.key) for a DNSKEY with tag 38696 (tested)	Ubuntu dns-root-data file held tags 20326 and 38696. File content is not runtime state.
Configured	Knot Resolver	Inspect the file given to trust_anchors.add_file (commonly root.keys)	Runtime listing not confirmed. Check your build.
Runtime	BIND	rndc managed-keys status (tested)	Without root reachability it reported keyid 0 / no trust for '.'. Look for 38696 in trusted state once initialized.
Runtime	PowerDNS Recursor	rec_control get-tas (tested)	4.9.3 listed only 20326: the stale-anchor condition this sheet exists to find.
Runtime	Unbound / others	Compare process start or reload time to the anchor file's modification time	Unbound 1.19.2 has no unbound-control command listing trust anchors.
Behavioral	Any sentinel-aware resolver	Query a bogus name, then root-key-sentinel-is-ta-38696.<signed-zone> and root-key-sentinel-not-ta-38696.<signed-zone>	RFC 8509 sec. 2.2: trusted key: is-ta answers, not-ta SERVFAIL; untrusted: the reverse. Record indeterminate combinations as indeterminate.
Behavioral	Any validating resolver	dig @resolver known-signed-name A +dnssec — look for the ad flag	A forwarder in front changes which resolver answered.
Differentiate	Any	Repeat the failing query with +cd; query an unsigned name; compare a second resolver known to hold KSK-2024	Evidence of a validation problem, not proof of a root anchor failure by itself. Read EDE (RFC 8914) where returned.

Sources: IANA Trust Anchors and Rollovers (iana.org/dnssec/files); APNIC, Rolling the root key (2026-10-09); RFC 5011; RFC 8509; RFC 8914.