From Binary to Maturity: A Five-Level Model for Measuring and Advancing DNSSEC Deployment Across Top-Level Domains

Santosh Pandit
Independent Researcher
ORCID: 0009-0004-5258-8392
Email: contact@santoshpandit.com
LinkedIn: https://www.linkedin.com/in/santoshpandit/

July 2026

Preprint, Version 1, 5 July 2026
DOI: https://doi.org/10.5281/zenodo.21202825

Abstract

DNSSEC deployment is often reported as a binary condition: a top-level domain either has a DS record at its parent zone or it does not. This view hides a wide range of outcomes among nominally signed domains, from delegations that fail chain-of-trust validation, to zones signed with algorithms the IETF has since deprecated, to zones that validate cleanly but deviate from current operational guidance. We measured 201 top-level domains (174 country-code TLDs across Africa, Latin America, Europe, North America, and Asia-Pacific, plus 27 widely used generic and sponsored TLDs) and classified each into a five-level maturity model: Unsigned, Broken/Bogus, Weak Cryptography, Hygiene Gaps, and Fully Conformant. Classification combined chain-of-trust validation status with algorithm, key-size, and NSEC3-parameter checks against RFC 8624, its successor registry regime under RFCs 9904 and 9905, and RFC 9276. We found 48 domains (23.9%) unsigned, 54 (26.9%) signed with cryptography below current recommended strength, 31 (15.4%) cryptographically sound but deviating from NSEC3 hygiene guidance, and 68 (33.8%) fully conformant; no broken chain of trust was observed. The central finding is that the need for improved DNSSEC maturity is global: in every region measured, between 48% and 86% of domains fall short of full conformance. The dominant weakness, a legacy 1024-bit RSA zone-signing key retained alongside a 2048-bit key-signing key, persists in 2026 at the TLD apex itself and appears independent of registry resourcing, affecting major national registries and Google-operated gTLDs alike. We also confirm three zones publishing a must-not-use SHA-1 DS digest and four zones signing with algorithms that current guidance designates MUST NOT or NOT RECOMMENDED. All unusual results were independently re-verified using raw `dig` queries and manual RSA modulus decoding.

1 Introduction

The Domain Name System Security Extensions (DNSSEC) add origin authentication and data integrity to DNS responses through a chain of cryptographic signatures rooted at the DNS root zone. Two decades after the first top-level domains were signed, deployment across the roughly 1,440 top-level domains in the root zone remains uneven, and public reporting on DNSSEC adoption tends to answer only the question of whether a DS record exists at the parent, without examining whether the resulting chain of trust is cryptographically sound by current standards.

This distinction matters. A domain can carry a signed delegation and still present a security posture no better, or in the failure case worse, than an unsigned one. A chain that fails to validate produces resolution failures for every validating resolver on the internet, a condition operationally more severe than simply being unsigned, since an unsigned domain resolves normally for every resolver regardless of validation policy. A chain that validates but relies on a deprecated or undersized algorithm provides a false sense of assurance to any auditor who checks only for the presence of a DS record.

This paper reports a measurement study across 201 top-level domains and proposes a five-level maturity model intended to separate these outcomes: whether a domain is signed at all, whether the signature can be cryptographically trusted, whether the cryptography used meets current recommended strength, and whether the zone follows current operational best practice for enumeration resistance. We apply this model to five geographic regions and to a set of widely used generic top-level domains, and we manually re-verify every result that appeared unusual, including comparisons across major national registries and two large, well-resourced gTLD operators.

2 Background

2.1 DNSSEC chain of trust

A DNSSEC-signed zone publishes a DNSKEY resource record set, and the parent zone publishes a corresponding DS (Delegation Signer) record containing a hash of the child's key-signing key. A validating resolver establishes trust in a child zone by confirming that the DS record at the parent matches a DNSKEY published by the child, and that all relevant resource record sets are covered by a valid RRSIG signature within its validity window. This produces one of three outcomes at any point in the chain: secure (the chain validates), insecure (no DS record exists, so the parent asserts, under a signed NSEC or NSEC3 non-existence proof, that the child is intentionally unsigned), or bogus (a DS record exists but the chain fails to validate, due to a key mismatch, an expired signature, or a similar fault).[1] A bogus result causes SERVFAIL for any resolver enforcing DNSSEC validation, which is a strictly worse outcome for end users than an insecure delegation.

2.2 Algorithm and key-size guidance

RFC 8624 [1] specifies which DNSSEC signing algorithms implementations must, should, or must not support, and updates earlier guidance that had permitted RSA/SHA-1 based algorithms. It distinguishes two tiers of discouragement for signing: algorithms 1 (RSAMD5), 3 (DSA), 6 (DSA-NSEC3-SHA1), and 12 (ECC-GOST) are designated MUST NOT for signing, the strongest level of discouragement, while algorithms 5 (RSASHA1), 7 (RSASHA1-NSEC3-SHA1), and 10 (RSASHA512) are designated NOT RECOMMENDED for signing, a weaker but still explicit discouragement. For algorithm 10 specifically, RFC 8624 bases this designation on limited deployment and comparative operational risk rather than a demonstrated cryptographic weakness of SHA-512 relative to SHA-256; we preserve this distinction throughout the paper and avoid describing NOT RECOMMENDED algorithms as prohibited. Algorithm 13 (ECDSAP256SHA256) is designated MUST for signing and is identified in RFC 8624's own commentary as the recommended algorithm for new DNSSEC deployments; algorithm 15 (Ed25519) is designated RECOMMENDED, with the RFC anticipating it as a future default; algorithm 14 (ECDSAP384SHA384) is designated MAY,

[1] RFC 4033 [8] formally defines a fourth validation state, indeterminate, for portions of the DNS tree not covered by any configured trust anchor. It cannot arise for the delegations measured in this study, all of which sit directly beneath the root trust anchor, and is therefore omitted from this description.

meaning it is permitted but not specifically recommended over the other options. RFC 8624 further designates SHA-1 as a DS record digest algorithm (digest type 1) as MUST NOT for new use, requiring SHA-256 (type 2) instead, with SHA-384 (type 4) permitted; this digest-level prohibition is a separate, stricter designation from the signing-algorithm tiers above.

RFC 8624 has since been obsoleted by RFC 9904 [3], which moves the canonical, continuously updated algorithm implementation guidance into the IANA registries (the DNS Security Algorithm Numbers registry for signing algorithms and the Digest Algorithms registry for DS digest types), rather than a static RFC text. RFC 9904 itself changes no designations; it changes where the guidance is canonically maintained and defines the process by which future documents update it. That process has already been exercised. RFC 9905 [4], published the same month, moves algorithms 5 (RSASHA1) and 7 (RSASHA1-NSEC3-SHA1) from NOT RECOMMENDED to MUST NOT for signing in the current registry, and additionally requires validating resolver operators to treat these signing algorithms as unsupported, so that responses covered only by them are treated as insecure rather than validated. RFC 9906 [5] similarly completes the deprecation of ECC-GOST; no zone in our sample uses a GOST algorithm. We therefore cite RFC 8624 as the historical source of the tiered designations our classification applies, and RFC 9904 and RFC 9905 together with the IANA registries as the current canonical reference. This transition does not alter any level assignment in this study, since MUST NOT and NOT RECOMMENDED signing algorithms both map to Level 2 of our model, but it does sharpen the status of the two algorithm 7 zones we report in Section 6.2.

2.3 NSEC3 parameter guidance

RFC 9276 [2] provides operational guidance for NSEC3 [7], the mechanism many zones use to prove non-existence of a name while resisting zone enumeration through hash-based ordering. It recommends an iteration count of zero and an empty salt. The NSEC3 hash function is, and always has been, attackable offline by an adversary who has obtained the hashed name set, regardless of how many iterations or what salt a zone publishes; RFC 9276's central point is that additional iterations and a non-empty salt do not meaningfully raise the cost of that offline attack, while they do impose real, avoidable computational cost on every validating resolver processing the zone's responses. A non-zero iteration count or non-empty salt is therefore a deviation from current operational guidance rather than a cryptographic break in itself.

3 Related Work

Chung et al. [18] provide the canonical large-scale measurement of DNSSEC key management practice, finding in 2017 that the vast majority (91.7%) of zone-signing keys among signed second-level domains under `.com`, `.net`, and `.org` were weak, most commonly 1024-bit RSA, alongside comparatively stronger key-signing keys, and documenting widespread poor rollover hygiene. The weak-ZSK pattern we report in Section 6.1 is therefore not new as an ecosystem-level observation, nor even as a TLD-apex observation: operator-community surveys by Dukhovni tabulated hundreds of TLD-apex ZSKs at 1024 bits in 2019 [20] and reported in 2022 that 1024-bit RSA still accounted for approximately 92% of RSA zone-signing keys among TLDs [21], and ICANN's Office of the CTO has published per-TLD observations of apex key algorithm and length over time [22]. What our measurement adds is not the discovery of the pattern but evidence of its persistence and a formalization of its assessment: the same legacy convention remains in place in mid-2026, under the successor registry regime of RFCs 9904 and 9905, quantified region by region across five continents, at the registry-operator rather than registrant level, and among named operators whose resourcing rules out capacity as an explanation. An ICANN-commissioned metrics study by Müller et al. [23]

independently recommended key length, signing algorithm, and NSEC3 parameters as DNSSEC deployment-quality metrics; our maturity model can be read as an ordinal packaging of exactly those axes, applied and published as a full per-TLD census. Separately, binary per-TLD signing trackers have long recorded whether each TLD was signed and had a DS record in the root, while the Internet Society's DNSSEC Deployment Maps [19] track top-level domains through six staged levels of deployment progress, from experimentation through automated DS maintenance. The latter model grades a TLD's progress toward operational signing; ours grades the cryptographic strength and operational hygiene of the signed state a TLD has reached. The two are complementary: a domain at the final stage of the deployment-progress model may sit anywhere from Level 2 to Level 4 in ours.

Longitudinal measurement of DNSSEC key management practice has been studied directly by Osterweil et al. [11], who examined key transitions across the first fifteen years of DNSSEC deployment and documented a persistent gap between published best practice and real-world operational behaviour. Our findings are consistent with this gap and extend it geographically: we observe the same divergence between recommended and actual key management independently across five continents and a set of major generic top-level domains, rather than within a single longitudinal dataset. We take the view that this convergence of the same operational shortfall across otherwise unrelated registries, operating under different national policy regimes and different levels of technical resourcing, is itself evidence that the gap Osterweil et al. identify is structural rather than local. A domain cannot be expected to progress through key rollover, algorithm modernisation, or NSEC3 hygiene tuning before it has completed initial signing; a zone must first be brought under a chain of trust before any of the later maturity levels in our model become reachable at all. Every unsigned domain identified in Section 6.3 is, in this sense, one required first step away from being able to reach Level 4, and the governing specifications (RFC 8624, now maintained in the IANA registries per RFC 9904, and RFC 9276) are already published and freely available to any registry regardless of its current resourcing, meaning the remaining gap to full conformance is a matter of operational prioritisation rather than an unsolved technical problem.

Heftrig et al. [12] demonstrate unintended consequences of DNSSEC's algorithm agility in the form of downgrade attacks against validating resolvers. Müller et al. [24] study the DNSSEC algorithm life-cycle directly, documenting at scale how slowly algorithms leave production once deployed, and the case for migrating DNSSEC to elliptic-curve algorithms, on grounds of response size and the RSA key-size dilemma, was made by van Rijswijk-Deij et al. [25]; both underpin the remediation direction our Level 2 implies. We observe a further, distinct consequence of the same property: the agility that permits a zone to publish multiple algorithms simultaneously, typically during a rollover, also permits a deprecated algorithm to remain in production indefinitely once introduced. This is the mechanism visible in the four domains in our dataset still signing with algorithm 7 or algorithm 10 (Section 6.2): the property that makes rollover possible is the same property that allows an algorithm current guidance no longer permits or recommends to persist without operational pressure to remove it.

Gruza et al. [13] demonstrate that a high NSEC3 iteration count can be exploited to exhaust a validating resolver's CPU through repeated hashing of adversary-chosen names. RFC 9276 predates this work, having been published in 2022 with its zero-iteration recommendation already motivated by the computational cost of hash-based enumeration resistance; Gruza et al.'s 2024 result does not underlie that guidance but rather empirically substantiates and sharpens the operational risk RFC 9276 had already warned against, giving concrete measurement to a cost that was previously stated in general terms. We apply RFC 9276's iteration-count guidance directly in our Level 3 classification and cite Gruza et al. as demonstrating the concrete consequence of a zone not following it. We note that this risk is mitigable at the resolver operator's own discretion: rate-limiting facilities

available in widely deployed resolver software (e.g. Unbound) and in general-purpose packet filtering frameworks (e.g. nftables) allow an operator to bound the CPU cost of any single client's query stream, independent of what any authoritative zone publishes. We do not consider this finding to weaken the case for DNSSEC deployment. The alternative to a signed, NSEC3-proven non-existence response is an unauthenticated NXDOMAIN or NODATA response that a validating client has no cryptographic basis to trust, leaving it exposed to on-path or off-path forgery that DNSSEC was designed to prevent. A resolver-side, operator-controlled mitigation for an elevated but bounded CPU cost is, in our view, a materially better position than an unauthenticated answer to a security-relevant query.

Nawrocki et al. [14] observe, in the course of studying DNS amplification, that operators of various `.gov` names do not consistently follow DNSSEC key rollover best practices, a finding we corroborate directly: our own measurement of `.mil`, and of the Google-operated `.app` and `.dev` domains, found a legacy 1024-bit zone-signing key in each case despite these being large, well-resourced operators. Prevalence-style measurement studies by Robinson [15] and Alkinoon et al. [16], both measuring DNSSEC adoption among hospital domains, establish the methodological precedent of reporting DNSSEC as a simple adoption percentage; our maturity model is intended as a finer-grained successor to that style of reporting, separating signed status from chain validity, cryptographic strength, and operational hygiene rather than collapsing all four into one binary figure. Separately, Heftrig et al. [17] demonstrate that a bogus or otherwise mishandled DNSSEC response can itself become a denial-of-service vector against validating resolvers, which reinforces our decision to treat a broken chain of trust (Level 1) as more operationally severe than an unsigned delegation (Level 0) rather than treating all non-conformant states as equally undesirable. Finally, our measurement pipeline builds on DNSViz [10]; Ashiq et al. [26] demonstrate that the same tool's diagnostic logs can drive automated DNSSEC error resolution at scale, and their taxonomy of real-world validation errors is complementary to the Level 1 category of our model.

4 Methodology

4.1 Measurement environment

All measurements were taken on 4 July 2026 from a Debian 13 VPS running a locally operated recursive resolver, using `dig` for direct record queries and `dnsviz` (`probe` and `grok` subcommands) to obtain a structured, per-zone analysis of the DNSSEC chain, including delegation validation status, per-key algorithm and length, and RFC 8624/9276 conformance warnings. Output was parsed with `jq` into a per-domain classification. Table 1 lists the tools used at each stage of measurement and verification.

4.2 Domain selection

We selected 174 country-code TLDs across five regions: Africa (54), Latin America (20), Europe (45), North America (14, limited to territories not already covered under Latin America), and Asia-Pacific (41, spanning East Asia, South Asia, Southeast Asia, and Oceania). We additionally measured 27 widely used generic and sponsored top-level domains (`.com`, `.net`, `.org`, `.edu`, `.gov`, `.mil`, `.int`, `.info`, `.biz`, `.name`, `.pro`, `.coop`, `.museum`, `.aero`, `.jobs`, `.mobi`, `.travel`, `.xyz`, `.online`, `.site`, `.store`, `.tech`, `.app`, `.dev`, `.cloud`, `.io`, `.ai`) for a combined total of 201 top-level domains. Full country groupings are geographic rather than a claim about political status; entries such as Taiwan, Hong Kong, and Macau are included as they carry distinct ccTLD delegations in the root zone. Regional coverage within each continent reflects the countries and territories we

Table 1: Tools used in measurement and verification

Tool	Role in this study
`dig` (BIND9 utils)	Direct queries against authoritative and root servers for DNSKEY, DS, NSEC3PARAM, and NS record sets; primary tool for manual re-verification of automated findings.
`delv` (BIND9 utils)	Independent chain-of-trust validation against a local trust anchor, used in early-stage manual checks to distinguish signed from unsigned responses.
`dnsviz` (`probe` and `grok`)	Structured per-zone analysis of delegation status, per-key algorithm and length, RRSIG validity, and RFC 8624/9276 conformance warnings; primary input to automated classification.
`jq`	Command-line JSON parsing of `dnsviz` output into per-domain classification fields.
`python3` (standard library, `base64`)	Manual decoding of RSA public key modulus length directly from DNSKEY record data per RFC 3110, used to independently confirm key-size findings without relying on `dnsviz`'s reported value.
`kdig` (Knot DNS utils)	Cross-tool corroboration of DNSKEY and RRSIG query results during manual verification.
Bash	Orchestration of per-TLD queries and classification logic across the full domain list.

selected for measurement rather than an exhaustive enumeration of every ccTLD on that continent; for example, Guyana (.gy) and Suriname (.sr) were not included in our Latin America set, and Greenland is included in North America while Bermuda and the Cayman Islands are not. These omissions reflect selection scope rather than any finding about the omitted domains themselves, and extending coverage to the remaining ccTLDs in each region is straightforward future work using the same methodology. Our five regional groupings likewise do not include a Middle East or Central and West Asia region, so ccTLDs such as .tr, .il, .sa, .ae, and .ir also fall outside this measurement's scope.

The 27 generic and sponsored TLDs were selected to span the original unrestricted gTLDs (.com, .net, .org), the legacy sponsored/restricted set introduced between 2000 and 2005 (.info, .biz, .name, .pro, .coop, .museum, .aero, .jobs, .mobi, .travel), government- and institution-restricted TLDs (.edu, .gov, .mil, .int), and a sample of newer generic TLDs launched under ICANN's expansion programs (.xyz, .online, .site, .store, .tech, .app, .dev, .cloud), so that the sample reflects distinct registry eras and governance models rather than an arbitrary or convenience selection. We did not attempt to sample the full space of over 1200 newer generic TLDs delegated since 2013, which we identify as an opportunity for future work.

We additionally include .io and .ai in this comparison set. By IANA delegation type both are ccTLDs, assigned respectively to the British Indian Ocean Territory and to Anguilla, and are not gTLDs; we include them here because both are operated and marketed commercially as generic technology-sector TLDs and are conventionally discussed alongside gTLDs in industry and press coverage. Their inclusion in our 27-domain generic/sponsored comparison set is therefore a grouping choice for comparative purposes, not a claim about their formal delegation type. Under strict IANA delegation type, our overall sample is 176 ccTLDs and 25 gTLDs rather than the 174/27 split used for regional and comparison-set framing throughout this paper.

4.3 Classification procedure

For each domain, we queried the delegation status field reported by dnsviz, which reflects whether the chain from the parent zone validates (secure), is absent (insecure), or fails validation (bogus). We treated any RRSIG reported with a validation status other than valid, for instance an expired or not-yet-valid signature, as equivalent to a bogus delegation for classification purposes, since either condition indicates that a resolver cannot currently trust the zone's signatures. Domains that validated were then checked against two independent criteria groups, corresponding directly to the Level 2 and Level 3 definitions in Section 5. The Level 2 (Weak Cryptography) criteria are: use of a signing algorithm designated MUST NOT or NOT RECOMMENDED by RFC 8624 (designations since maintained and updated in the IANA registries; see Section 2.2); RSA key size below 2048 bits; and presence of a MUST-NOT-use SHA-1 DS digest. The Level 3 (Hygiene Gaps) criterion is a non-zero NSEC3 iteration count or a non-empty NSEC3 salt, present on an otherwise cryptographically conformant zone. A domain triggering any Level 2 criterion is classified Level 2 regardless of its NSEC3 parameters, since weak cryptography is treated as the more severe condition; a domain triggering only Level 3 criteria, with no Level 2 issue present, is classified Level 3. The 2048-bit RSA threshold is not itself a numeric mandate stated in RFC 8624, which defers to general cryptographic strength guidance when specifying minimum key sizes; we adopt 2048 bits as a pragmatic operational cutoff because it is the minimum widely recommended RSA modulus size in contemporary cryptographic guidance (for example, NIST SP 800-57) and is consistent with current registry operational practice.

4.4 Manual verification

Automated tooling can misclassify results, and three errors were identified and corrected during script development: an ordering fault that classified unsigned negative responses as errors; a case-matching fault that failed to detect a combined warning string; and a rule-precedence fault that mapped a non-zero NSEC3 iteration count to Level 2 rather than Level 3, contradicting our own model definition in Section 5. The third fault affected seven domains (Ecuador, Uruguay, Latvia, Luxembourg, Spain, the Philippines, and Brunei), each of which had a non-zero NSEC3 iteration count or non-empty salt as its only flagged issue with no accompanying weak-cryptography finding; these are corrected to Level 3 throughout this paper and its appendix. An independent third-party review that re-measured all 201 domains also identified a data-entry error in the appendix row for Somalia (`.so`), which was recorded as Level 3 based on a stale, zone-side observation of a salted NSEC3PARAM record, when Somalia in fact carries no DS record at the parent zone and is correctly Level 0 under our own definition; this row has been corrected and the appendix and Table 2 were regenerated from a single reconciled dataset to prevent future divergence between them.

Following these corrections, every classification result that appeared unusual, unexpected for the operator in question, or that stacked an unusually high number of issues, was independently re-verified using raw `dig` queries against authoritative and root servers, and, where key size was in question, by decoding the RSA modulus directly from the DNSKEY record according to RFC 3110 [9]. This included re-verification of results for Algeria, Croatia, Grenada, Laos, Guinea-Bissau, Benin, and the United Kingdom, Germany, China, the United States, and Google-operated `.app` and `.dev`, among others. All re-verified results confirmed the automated classification, apart from the corrections described above.

5 A Five-Level Maturity Model

We propose the following five-level model. The number of levels was deliberately bounded at five to keep the model actionable: each level corresponds to a distinct remediation action, and collapsing or expanding the level count would either hide a distinct required action or introduce a distinction without an operational difference.

- **Level 0, Unsigned.** No DS record at the parent zone. Required action: deploy DNSSEC signing from zero, including key generation, zone signing, and DS publication at the parent.
- **Level 1, Broken or Bogus.** A DS record exists but the chain fails validation, or a signature has expired or is not yet valid. This is the most operationally severe state, since validating resolvers return SERVFAIL for the entire zone. Required action: immediate remediation of the key mismatch or re-signing of the zone.
- **Level 2, Weak Cryptography.** The chain validates, but the zone uses a signing algorithm designated MUST NOT or NOT RECOMMENDED (RFC 8624, as since carried into and updated in the IANA registries), an RSA key below 2048 bits, or a MUST-NOT-use SHA-1 DS digest. Required action: algorithm or key rollover to a currently recommended algorithm and key size.
- **Level 3, Hygiene Gaps.** The chain validates using currently recommended cryptography, but NSEC3 parameters deviate from RFC 9276 guidance. Required action: NSEC3 parameter reconfiguration; low operational urgency.

- **Level 4, Fully Conformant.** The chain validates, cryptography meets current recommended strength, and NSEC3 parameters (where used) follow RFC 9276 guidance. Required action: routine monitoring of key rollover schedules and signature expiry windows.

Whether a domain has taken the first step toward maturity at all, that is, whether a DS record exists at the parent zone, is the Level 0/Level 1-and-above boundary. A separate and more consequential question, whether a published signature can actually be relied upon rather than merely whether an algorithm choice looks acceptable on paper, is answered at the Level 1/Level 2 boundary: a secure delegation status places a domain at Level 2 or above for further algorithm-level evaluation, while a bogus status places it at Level 1 regardless of what algorithm or key size the zone uses, since a chain that fails to validate cannot be trusted no matter how strong its unverifiable cryptography claims to be.

6 Results

Table 2 presents the regional breakdown across all 201 domains.

Table 2: Maturity level distribution by region

Region	N	L0	L1	L2	L3	L4
Africa	54	22	0	7	9	16
Latin America	20	7	0	3	6	4
Europe	45	6	0	9	7	23
North America	14	4	0	6	2	2
Asia-Pacific	41	9	0	16	7	9
Common gTLDs	27	0	0	13	0	14
Total	201	48	0	54	31	68

No domain in this sample presented a Level 1 (Broken/Bogus) result at the time of measurement. This is a positive finding in itself: the most operationally dangerous DNSSEC state, in which validation actively breaks resolution, was not observed in any of the 201 domains measured, despite substantial variation in signing maturity elsewhere.

6.1 Weak zone-signing keys are an industry-wide legacy pattern

Across every region, the dominant driver of Level 2 classification was an RSA zone-signing key (ZSK) below 2048 bits, most commonly 1024 bits, coexisting with a 2048-bit key-signing key (KSK). This pattern held for national ccTLD registries of varying size and resourcing (Germany, the United Kingdom, China, Ethiopia, Mauritius) and, notably, for domains operated by well-resourced third parties: `.mil` (operated by the US Department of Defense), and `.app` and `.dev` (both operated by Google). We independently decoded the RSA modulus for all of these to rule out a tooling artifact; in every case the KSK was confirmed at 2048 bits and the ZSK at 1024 bits. This observation is consistent with a legacy 1024-bit ZSK, retained alongside a stronger KSK, being a widespread historical operational convention rather than a signal correlated with an operator's technical resourcing or a country's level of economic development; we present this as an observational pattern across the registries and operators we measured rather than a causally established claim, since we do not have visibility into each operator's internal provisioning history or rollover roadmap. Chung

et al. [18] documented weak ZSKs as the dominant pattern among signed second-level domains in 2017, and Dukhovni's operator-community surveys documented the same pattern at the TLD apex itself in 2019 and 2022 [20, 21]; our measurement shows the convention still in place in mid-2026. We consider this persistence, and its independence from operator resourcing, the most notable finding of the study, since public commentary on DNSSEC key strength often implicitly frames weak keys as a resource or maturity gap specific to smaller or developing-economy registries, a framing our cross-operator observation does not support.

Six domains in our dataset instead carried a non-standard 1280-bit ZSK, confirmed by direct modulus decoding: Chile, Colombia, the United States, Andorra, the generic TLD `.biz`, and `.tv`, formally the ccTLD of Tuvalu and counted under Asia-Pacific in our dataset, though principally marketed and used commercially for purposes unrelated to the country. We interpret this consistent, unusual, non-power-of-two key size as a distinct, deliberate key-size choice rather than the same 1024-bit legacy default discussed above. For four of the six, the public record identifies a common registry-services lineage: `.us` and `.biz` are operated by Registry Services, LLC (GoDaddy Registry), which acquired Neustar's registry business in 2020; Neustar had also provided back-end registry services for `.co`; and GoDaddy Registry took over `.tv` from Verisign in 2022. The 1280-bit convention itself is publicly documented: Dukhovni's 2019 survey already recorded a large 1280-bit ZSK cluster among TLDs [20], Verisign's published DNSSEC practice statements specify 1280-bit ZSKs for the zones it operates, and ICANN's key-lifecycle observations record a large gTLD operator moving its ZSK from 1024 to 1280 bits in late 2019 [22]. Chile (NIC Chile) and Andorra are on separate registry backends; their use of the same size is consistent with published operator guidance recommending at least 1280 bits for RSA ZSKs [21], though we do not claim a causal explanation in those two cases.

Algeria (`.dz`), Croatia (`.hr`), and Laos (`.la`) all publish DS records containing a SHA-1 digest (digest type 1) alongside a SHA-256 digest (digest type 2). RFC 8624 designates new use of the SHA-1 digest type as MUST NOT. We confirmed this directly by querying the root servers for the DS record set of each zone. Since a SHA-256 digest is present in all three cases, resolvers that ignore the weaker digest per RFC 4509 [6] are unaffected in practice, but the continued publication of a prohibited digest type indicates the zone has not fully completed its transition away from legacy signing configuration. Laos's use of a SHA-1 DS digest is discussed further in Section 6.2 alongside its other findings.

6.2 Signing algorithms below current recommended strength in production use

Four domains were found actively signing with algorithms below current recommended strength. Grenada (`.gd`) and Laos (`.la`) use algorithm 7 (RSASHA1-NSEC3-SHA1), designated NOT RECOMMENDED for signing by RFC 8624 and, since RFC 9905 [4], MUST NOT under the current IANA registry. RFC 9905 additionally instructs validating resolver operators to treat algorithm 7 signatures as unsupported. Where algorithm 7 is a zone's only signing algorithm, as we observed for both zones at measurement time, a resolver conforming to RFC 9905 treats the zone's responses as insecure: an effective security posture no better than an unsigned delegation, despite the operational cost of signing having been paid. Guinea-Bissau (`.gw`) and Vanuatu (`.vu`) use algorithm 10 (RSASHA512), which remains NOT RECOMMENDED rather than MUST NOT; as noted in Section 2.2, that designation reflects limited deployment and operational risk rather than a demonstrated weakness of SHA-512 itself. Laos combines algorithm 7 with a 1024-bit key and a coexisting SHA-1 DS digest, the latter a MUST-NOT-use designation, making it the single most severe combination of issues observed in this study. We independently confirmed the algorithm number, key size, and DS digest types for Laos directly against authoritative servers.

6.3 Unsigned domains

48 of 201 domains (23.9%) had no DS record at the parent zone at the time of measurement. This proportion varied substantially by region, from 0 among the common gTLD set (all of which are signed, reflecting policy requirements from their respective registry operators and, for `.gov`, US federal mandate) to over 40% of the African ccTLDs measured (22 of 54, 40.7%).

7 Discussion

The five-level model separates three distinct questions that a binary signed/unsigned metric conflates: whether a domain is signed, whether the resulting chain can be trusted, and whether the cryptography and hygiene of a signed and trusted zone meet current guidance. The absence of any Level 1 result in this sample suggests that, whatever the state of DNSSEC rollout globally, operators that do sign a zone are, at present, not leaving it in an actively broken state. This is a meaningfully different and more reassuring finding than simply reporting an adoption percentage.

The finding that weak zone-signing keys appear across registries of every resourcing level complicates a narrative in which DNSSEC maturity tracks national economic development or registry technical capacity. A large, well-funded operator such as Google retaining a 1024-bit ZSK on `.app` and `.dev` suggests that legacy key-size defaults, once set at zone provisioning time, tend to persist regardless of an operator's capacity to upgrade them, absent an explicit rollover event. This has a practical implication for policy and outreach efforts aimed at improving DNSSEC posture: the appropriate remediation for Level 2 domains is a scheduled key rollover, a comparatively low-cost operational task, rather than a capacity-building intervention.

8 Limitations

This study reflects a single measurement snapshot, taken on 4 July 2026, from a single vantage point using one recursive resolver, and DNSSEC state, particularly signature validity windows and keys mid-rollover, can change on a timescale of days. The classification tool relies on `dnsviz`'s own interpretation of zone state; while we manually re-verified every result that appeared unusual using an independent method, we did not re-verify every one of the 201 results by hand, and a small number of Level 3 or Level 4 classifications rest on the tool's output alone. We measured only the apex of each top-level domain and did not sample second-level delegations beneath it, so this study characterizes registry-operator practice at the TLD level and does not describe DNSSEC deployment among individual domain registrants within each TLD. Finally, the five-level model's thresholds are grounded in current IETF and cryptographic guidance but are not all drawn from a single explicit numeric mandate. The algorithm-tier classification (MUST NOT versus NOT RECOMMENDED) and the SHA-1 DS digest prohibition follow RFC 8624 and its successor registry designations under RFCs 9904 and 9905 directly, while the 2048-bit RSA key-size cutoff is a pragmatic operational threshold consistent with broader contemporary cryptographic strength guidance rather than a number stated explicitly in RFC 8624 itself. All of these thresholds will require revision as guidance evolves, as the recent reclassification of SHA-1-based signing to MUST NOT by RFC 9905 already illustrates. We did not track any domain longitudinally; repeated measurement over time, particularly of the currently unsigned domains identified in Section 6.3, is a natural direction for future work to track remediation progress.

9 Conclusion

We measured DNSSEC deployment and conformance across 201 top-level domains and classified each into a five-level maturity model separating signed status, chain-of-trust validity, cryptographic strength, and NSEC3 hygiene. 23.9% of domains measured were unsigned, 26.9% were signed with cryptography below current recommended strength, 15.4% were cryptographically sound but deviated from NSEC3 operational guidance, and 33.8% were fully conformant, with no broken chains of trust observed. The most notable finding was that weak zone-signing key size, previously documented at scale among second-level domains and in operator-community TLD surveys, persists as a widespread legacy pattern at the TLD apex itself, independent of registry resourcing and observed equally in major national registries and in large third-party gTLD operators.

We view the 48 unsigned domains identified in this study as the highest-priority remediation group, ahead of any of the signed-but-imperfect categories. A registry cannot progress through key modernisation or NSEC3 hygiene tuning before it has completed initial signing; the first mile, publishing a DS record and a validating chain, must be run before any later stage of the maturity model is reachable at all. We consider full conformance to be within reach for every unsigned domain in this dataset, since the governing specifications, the IANA algorithm registries maintained under RFCs 9904 and 9905 for algorithm guidance and RFC 9276 for NSEC3 parameter guidance, are publicly available without cost, and since Level 4 domains already exist in every region we measured, including regions with a high proportion of currently unsigned domains. The remaining gap is one of operational prioritisation and technical assistance rather than an unresolved research problem. We make the full per-domain dataset available in the appendix to support independent verification and longitudinal comparison, and hope it can serve as a baseline against which future remediation, particularly among currently unsigned domains, can be measured.

Data Availability

The complete per-domain classification underlying Table 2 is provided in Appendix A. The measurement scripts used to produce this dataset have been published at `https://github.com/beatquantum/dnssec-maturity`. This paper is archived as a preprint under DOI `https://doi.org/10.5281/zenodo.21202825`.

Suggested Citation

S. Pandit, "From Binary to Maturity: A Five-Level Model for Measuring and Advancing DNSSEC Deployment Across Top-Level Domains," Preprint, Version 1, Zenodo, July 2026. DOI: `https://doi.org/10.5281/zenodo.21202825`.

Declarations

The author received no external funding for this work and declares no competing interests. This research was conducted in the author's personal capacity, and the views expressed are the author's own.

Acknowledgments

Measurement automation and data classification scripts used in this study were developed with the assistance of an AI coding tool, with all classification logic and unusual results independently verified by the author against raw DNS query output prior to inclusion.

References

[1] P. Wouters and O. Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC," RFC 8624, June 2019.

[2] W. Hardaker and V. Dukhovni, "Guidance for NSEC3 Parameter Settings," RFC 9276, August 2022.

[3] W. Hardaker and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process," RFC 9904, November 2025.

[4] W. Hardaker and W. Kumari, "Deprecating the Use of SHA-1 in DNSSEC Signature Algorithms," RFC 9905, November 2025.

[5] W. Hardaker and W. Kumari, "Deprecate Usage of ECC-GOST within DNSSEC," RFC 9906, November 2025.

[6] W. Hardaker, "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)," RFC 4509, May 2006.

[7] B. Laurie, G. Sisson, R. Arends, and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence," RFC 5155, March 2008.

[8] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005.

[9] D. Eastlake 3rd, "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," RFC 3110, May 2001.

[10] C. Deccio, "DNSViz: A DNS Visualization Tool," `https://dnsviz.net/`.

[11] E. Osterweil, P. Fotouhi Tehrani, T. C. Schmidt, and M. Wählisch, "From the Beginning: Key Transitions in the First 15 Years of DNSSEC," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 5265–5283, Dec. 2022. arXiv:2109.08783.

[12] E. Heftrig, H. Shulman, and M. Waidner, "Poster: The Unintended Consequences of Algorithm Agility in DNSSEC," in *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, 2022, pp. 3363–3365. arXiv:2205.10608.

[13] O. Gruza, E. Heftrig, O. Jacobsen, H. Schulmann, N. Vogel, and M. Waidner, "Attacking with Something That Does Not Exist: 'Proof of Non-Existence' Can Exhaust DNS Resolver CPU," in *Proc. USENIX WOOT '24*, 2024. arXiv:2403.15233.

[14] M. Nawrocki, M. Jonker, T. C. Schmidt, and M. Wählisch, "The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core," in *Proc. ACM Internet Measurement Conference (IMC '21)*, 2021. arXiv:2109.01104.

[15] R. Robinson, "Prevalence of DNSSEC for Hospital Websites in Illinois," arXiv:1712.05376, 2017.

[16] M. Alkinoon, A. Alabduljabbar, H. Althebeiti, R. Jang, D. Nyang, and D. Mohaisen, "Understanding the Security and Performance of the Web Presence of Hospitals: A Measurement Study," arXiv:2304.13278, 2023.

[17] E. Heftrig, H. Schulmann, N. Vogel, and M. Waidner, "The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC," in *Proc. ACM CCS '24*, 2024. arXiv:2406.03133.

[18] T. Chung, R. van Rijswijk-Deij, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, "A Longitudinal, End-to-End View of the DNSSEC Ecosystem," in *Proc. 26th USENIX Security Symposium*, 2017, pp. 1307–1322.

[19] Internet Society, "DNSSEC Deployment Maps," `https://www.internetsociety.org/deploy360/dnssec/maps/`.

[20] V. Dukhovni, "TLD key size/stats corrected," dns-operations mailing list, DNS-OARC, 11 July 2019. `https://lists.dns-oarc.net/pipermail/dns-operations/2019-July/019012.html`

[21] V. Dukhovni, "DNSSEC algorithms for TLDs (and everyone else)," APNIC Blog, 24 March 2022. `https://blog.apnic.net/2022/03/24/dnssec-algorithms-for-tlds-and-everyone-else/`

[22] E. Lewis, "Observing DNSSEC Key Lifecycles," ICANN Office of the Chief Technology Officer, OCTO-035, 18 July 2022. `https://www.icann.org/en/system/files/files/octo-035-18jul22-en.pdf`

[23] M. Müller, J. Jansen, M. Davids, and W. Toorop, "DNSSEC Deployment Metrics Research," SIDN Labs and NLnet Labs, commissioned by ICANN, 8 August 2022. `https://www.icann.org/en/system/files/files/dnssec-deployment-metrics-research-08aug22-en.pdf`

[24] M. Müller, W. Toorop, T. Chung, J. Jansen, and R. van Rijswijk-Deij, "The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle," in *Proc. ACM Internet Measurement Conference (IMC '20)*, 2020.

[25] R. van Rijswijk-Deij, A. Sperotto, and A. Pras, "Making the Case for Elliptic Curves in DNSSEC," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 5, pp. 13–19, 2015.

[26] M. I. Ashiq, O. Hureau, C. T. Deccio, and T. Chung, "Decoding DNSSEC Errors at Scale: An Automated DNSSEC Error Resolution Framework using Insights from DNSViz Logs," in *Proc. ACM Internet Measurement Conference (IMC '25)*, 2025, pp. 242–257.

A Full Per-Domain Classification

The following table lists the maturity level classification for all 201 domains measured. L0: Unsigned. L1: Broken/Bogus. L2: Weak Cryptography. L3: Hygiene Gaps. L4: Fully Conformant.

Table 3: Full per-domain classification

Region	Entity	TLD / Level	Issues
Africa	Algeria	.dz / L2	SHA-1 DS digest present
Africa	Angola	.ao / L0	Unsigned
Africa	Benin	.bj / L3	Non-empty NSEC3 salt
Africa	Botswana	.bw / L3	Non-empty NSEC3 salt
Africa	Burkina Faso	.bf / L4	Conformant
Africa	Burundi	.bi / L4	Conformant
Africa	Cabo Verde	.cv / L0	Unsigned
Africa	Cameroon	.cm / L4	Conformant
Africa	Central African Republic	.cf / L0	Unsigned
Africa	Chad	.td / L0	Unsigned
Africa	Comoros	.km / L0	Unsigned
Africa	Congo (Republic)	.cg / L0	Unsigned
Africa	Congo (DRC)	.cd / L0	Unsigned
Africa	Cote d'Ivoire	.ci / L4	Conformant
Africa	Djibouti	.dj / L0	Unsigned
Africa	Egypt	.eg / L0	Unsigned
Africa	Equatorial Guinea	.gq / L0	Unsigned
Africa	Eritrea	.er / L4	Conformant
Africa	Eswatini	.sz / L0	Unsigned
Africa	Ethiopia	.et / L2	Weak RSA key (1024-bit ZSK)
Africa	Gabon	.ga / L4	Conformant
Africa	Gambia	.gm / L0	Unsigned
Africa	Ghana	.gh / L0	Unsigned
Africa	Guinea	.gn / L4	Conformant
Africa	Guinea-Bissau	.gw / L2	Algorithm 10 (not recommended); non-zero NSEC3 iterations; non-empty salt
Africa	Kenya	.ke / L4	Conformant
Africa	Lesotho	.ls / L4	Conformant
Africa	Liberia	.lr / L4	Conformant
Africa	Libya	.ly / L3	Non-empty NSEC3 salt
Africa	Madagascar	.mg / L3	Non-empty NSEC3 salt
Africa	Malawi	.mw / L0	Unsigned
Africa	Mali	.ml / L4	Conformant (Ed25519)
Africa	Mauritania	.mr / L3	Non-empty NSEC3 salt
Africa	Mauritius	.mu / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Africa	Morocco	.ma / L2	Weak RSA key (1024-bit ZSK); non-zero NSEC3 iterations; non-empty salt
Africa	Mozambique	.mz / L0	Unsigned
Africa	Namibia	.na / L3	Non-empty NSEC3 salt
Africa	Niger	.ne / L0	Unsigned
Africa	Nigeria	.ng / L4	Conformant

Table 3 continued

Region	Entity	TLD / Level	Issues
Africa	Rwanda	.rw / L3	Non-empty NSEC3 salt
Africa	Sao Tome and Principe	.st / L0	Unsigned
Africa	Senegal	.sn / L4	Conformant
Africa	Seychelles	.sc / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Africa	Sierra Leone	.sl / L0	Unsigned
Africa	Somalia	.so / L0	Unsigned (no DS at parent; zone still publishes DNSKEY and a salted NSEC3PARAM, but by our L0 definition absence of a DS record classifies it as unsigned)
Africa	South Africa	.za / L2	Weak RSA key (1024-bit ZSK)
Africa	South Sudan	.ss / L4	Conformant
Africa	Sudan	.sd / L0	Unsigned
Africa	Tanzania	.tz / L4	Conformant
Africa	Togo	.tg / L0	Unsigned
Africa	Tunisia	.tn / L4	Conformant
Africa	Uganda	.ug / L3	Non-empty NSEC3 salt
Africa	Zambia	.zm / L3	Non-empty NSEC3 salt
Africa	Zimbabwe	.zw / L0	Unsigned
Latin America	Argentina	.ar / L4	Conformant
Latin America	Bolivia	.bo / L0	Unsigned
Latin America	Brazil	.br / L4	Conformant
Latin America	Chile	.cl / L2	Non-standard 1280-bit ZSK; non-empty salt
Latin America	Colombia	.co / L2	Non-standard 1280-bit ZSK
Latin America	Costa Rica	.cr / L4	Conformant
Latin America	Cuba	.cu / L0	Unsigned
Latin America	Dominican Republic	.do / L0	Unsigned
Latin America	Ecuador	.ec / L3	Non-empty salt; non-zero NSEC3 iterations
Latin America	El Salvador	.sv / L0	Unsigned
Latin America	Guatemala	.gt / L0	Unsigned

Table 3 continued

Region	Entity	TLD / Level	Issues
Latin America	Haiti	.ht / L3	Non-empty NSEC3 salt
Latin America	Honduras	.hn / L3	Non-empty NSEC3 salt
Latin America	Mexico	.mx / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Latin America	Nicaragua	.ni / L0	Unsigned
Latin America	Panama	.pa / L0	Unsigned
Latin America	Paraguay	.py / L3	Non-empty NSEC3 salt
Latin America	Peru	.pe / L3	Non-empty NSEC3 salt
Latin America	Uruguay	.uy / L3	Non-empty salt; non-zero NSEC3 iterations
Latin America	Venezuela	.ve / L4	Conformant
Europe	Albania	.al / L0	Unsigned
Europe	Andorra	.ad / L2	Non-standard 1280-bit ZSK
Europe	Austria	.at / L4	Conformant
Europe	Belarus	.by / L3	Non-empty NSEC3 salt
Europe	Belgium	.be / L4	Conformant
Europe	Bosnia and Herzegovina	.ba / L0	Unsigned
Europe	Bulgaria	.bg / L4	Conformant
Europe	Croatia	.hr / L2	Weak RSA key (1024-bit ZSK); SHA-1 DS digest; non-zero NSEC3 iterations; non-empty salt
Europe	Cyprus	.cy / L4	Conformant
Europe	Czech Republic	.cz / L3	Non-empty NSEC3 salt
Europe	Denmark	.dk / L4	Conformant
Europe	Estonia	.ee / L2	Weak RSA key (1024-bit ZSK)
Europe	Finland	.fi / L4	Conformant
Europe	France	.fr / L4	Conformant
Europe	Germany	.de / L2	Weak RSA key (1024-bit ZSK)
Europe	Greece	.gr / L4	Conformant
Europe	Hungary	.hu / L4	Conformant
Europe	Iceland	.is / L4	Conformant
Europe	Ireland	.ie / L4	Conformant
Europe	Italy	.it / L4	Conformant
Europe	Latvia	.lv / L3	Non-empty salt; non-zero NSEC3 iterations
Europe	Liechtenstein	.li / L4	Conformant

Table 3 continued

Region	Entity	TLD / Level	Issues
Europe	Lithuania	.lt / L4	Conformant
Europe	Luxembourg	.lu / L3	Non-empty salt; non-zero NSEC3 iterations
Europe	Malta	.mt / L0	Unsigned
Europe	Moldova	.md / L4	Conformant
Europe	Monaco	.mc / L2	Weak RSA key (1024-bit ZSK)
Europe	Montenegro	.me / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Europe	Netherlands	.nl / L4	Conformant
Europe	North Macedonia	.mk / L0	Unsigned
Europe	Norway	.no / L4	Conformant
Europe	Poland	.pl / L3	Non-empty NSEC3 salt
Europe	Portugal	.pt / L3	Non-empty NSEC3 salt
Europe	Romania	.ro / L2	Weak RSA key (1024-bit ZSK); non-zero NSEC3 iterations; non-empty salt
Europe	Russia	.ru / L2	Weak RSA key (1024-bit ZSK)
Europe	San Marino	.sm / L0	Unsigned
Europe	Serbia	.rs / L4	Conformant
Europe	Slovakia	.sk / L4	Conformant
Europe	Slovenia	.si / L4	Conformant
Europe	Spain	.es / L3	Non-empty salt; non-zero NSEC3 iterations
Europe	Sweden	.se / L4	Conformant
Europe	Switzerland	.ch / L4	Conformant
Europe	Ukraine	.ua / L4	Conformant
Europe	United Kingdom	.uk / L2	Weak RSA key (1024-bit ZSK)
Europe	Vatican City	.va / L0	Unsigned
North America	Canada	.ca / L4	Conformant
North America	United States	.us / L2	Non-standard 1280-bit ZSK
North America	Bahamas	.bs / L0	Unsigned
North America	Barbados	.bb / L0	Unsigned
North America	Belize	.bz / L2	Weak RSA key (1024-bit ZSK); non-empty salt
North America	Jamaica	.jm / L0	Unsigned
North America	Trinidad and Tobago	.tt / L3	Non-empty NSEC3 salt
North America	Antigua and Barbuda	.ag / L2	Weak RSA key (1024-bit ZSK); non-empty salt

Table 3 continued

Region	Entity	TLD / Level	Issues
North America	Dominica	.dm / L4	Conformant
North America	Grenada	.gd / L2	Algorithm 7 (must not be used for signing); weak RSA key (1024-bit ZSK)
North America	Saint Kitts and Nevis	.kn / L0	Unsigned
North America	Saint Lucia	.lc / L2	Weak RSA key (1024-bit ZSK); non-empty salt
North America	Saint Vincent and the Grenadines	.vc / L2	Weak RSA key (1024-bit ZSK); non-empty salt
North America	Greenland	.gl / L3	Non-empty NSEC3 salt
Asia-Pacific	China	.cn / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Japan	.jp / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	South Korea	.kr / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	North Korea	.kp / L0	Unsigned
Asia-Pacific	Mongolia	.mn / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Asia-Pacific	Taiwan	.tw / L4	Conformant
Asia-Pacific	Hong Kong	.hk / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Macau	.mo / L0	Unsigned
Asia-Pacific	India	.in / L4	Conformant
Asia-Pacific	Pakistan	.pk / L0	Unsigned
Asia-Pacific	Bangladesh	.bd / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Sri Lanka	.lk / L4	Conformant
Asia-Pacific	Nepal	.np / L0	Unsigned
Asia-Pacific	Bhutan	.bt / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Maldives	.mv / L0	Unsigned
Asia-Pacific	Afghanistan	.af / L3	Non-empty NSEC3 salt
Asia-Pacific	Indonesia	.id / L4	Conformant
Asia-Pacific	Malaysia	.my / L4	Conformant
Asia-Pacific	Philippines	.ph / L3	Non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Thailand	.th / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Vietnam	.vn / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Singapore	.sg / L4	Conformant
Asia-Pacific	Myanmar	.mm / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Cambodia	.kh / L0	Unsigned

Table 3 continued

Region	Entity	TLD / Level	Issues
Asia-Pacific	Laos	.la / L2	Algorithm 7 (must not be used for signing); weak RSA key (1024-bit ZSK); SHA-1 DS digest (must-not-use); non-zero NSEC3 iterations
Asia-Pacific	Brunei	.bn / L3	Non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Timor-Leste	.tl / L3	Non-empty NSEC3 salt
Asia-Pacific	Australia	.au / L3	Non-empty NSEC3 salt
Asia-Pacific	New Zealand	.nz / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Papua New Guinea	.pg / L4	Conformant
Asia-Pacific	Fiji	.fj / L4	Conformant
Asia-Pacific	Solomon Islands	.sb / L3	Non-empty NSEC3 salt
Asia-Pacific	Vanuatu	.vu / L2	Algorithm 10 (not recommended)
Asia-Pacific	Samoa	.ws / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Asia-Pacific	Tonga	.to / L0	Unsigned
Asia-Pacific	Kiribati	.ki / L3	Non-empty NSEC3 salt
Asia-Pacific	Micronesia	.fm / L2	Weak RSA key (1024-bit ZSK)
Asia-Pacific	Palau	.pw / L4	Conformant
Asia-Pacific	Marshall Islands	.mh / L0	Unsigned
Asia-Pacific	Nauru	.nr / L0	Unsigned
Asia-Pacific	Tuvalu	.tv / L2	Non-standard 1280-bit ZSK
Generic / Sponsored	Commercial	.com / L4	Conformant
Generic / Sponsored	Network infrastructure	.net / L4	Conformant
Generic / Sponsored	Organization	.org / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	Education (US)	.edu / L4	Conformant
Generic / Sponsored	US Government	.gov / L4	Conformant
Generic / Sponsored	US Military	.mil / L2	Weak RSA key (1024-bit ZSK)
Generic / Sponsored	International organizations	.int / L4	Conformant
Generic / Sponsored	Information	.info / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	Business	.biz / L2	Non-standard 1280-bit ZSK
Generic / Sponsored	Personal names	.name / L4	Conformant
Generic / Sponsored	Professionals	.pro / L2	Weak RSA key (1024-bit ZSK); non-empty salt

Table 3 continued

Region	Entity	TLD / Level	Issues
Generic / Sponsored	Cooperatives	.coop / L4	Conformant
Generic / Sponsored	Museums	.museum / L4	Conformant
Generic / Sponsored	Air transport industry	.aero / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	Human resources	.jobs / L4	Conformant
Generic / Sponsored	Mobile devices	.mobi / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	Travel industry	.travel / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	General use	.xyz / L2	Weak RSA key (1024-bit ZSK)
Generic / Sponsored	General use	.online / L4	Conformant
Generic / Sponsored	General use	.site / L4	Conformant
Generic / Sponsored	Retail	.store / L4	Conformant
Generic / Sponsored	Technology	.tech / L4	Conformant
Generic / Sponsored	Applications (Google)	.app / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Generic / Sponsored	Development (Google)	.dev / L2	Weak RSA key (1024-bit ZSK); non-empty salt; non-zero NSEC3 iterations
Generic / Sponsored	Cloud services	.cloud / L4	Conformant
Generic / Sponsored	Technology (British Indian Ocean Territory)	.io / L2	Weak RSA key (1024-bit ZSK); non-empty salt
Generic / Sponsored	Artificial intelligence (Anguilla)	.ai / L2	Weak RSA key (1024-bit ZSK); non-empty salt