DNSSEC Policy Statement for .ALIBABA

1. INTRODUCTION

1.1 Overview

Domain Name System Security Extensions (DNSSEC) provide origin authentication and data integrity for DNS data by using digital signatures over DNS resource records. This document describes the DNSSEC practices and controls adopted by Alibaba Cloud in its role as a back-end Registry Service Provider (RSP) for top-level domains (TLDs). This policy statement follows the IETF DNSSEC DPS structure and is intended to inform stakeholders about the level of trust and the protections provided by the system.

1.2 Document Name and Identification

Alibaba Cloud DNSSEC Policy Statement (DPS)
Version 1.01

1.3 Community and Applicability

This policy statement applies to registrars and registrants operating within the Alibaba Cloud registry service ecosystem, and in particular to Registry Operators (ROs) that rely on Alibaba Cloud as a back-end operator.

• For the Registry (RO): Alibaba Cloud operates and maintains DNS zone files based on registry data and provides public DNS/DNSSEC services. This includes management of ZSK/KSK key material, signing of zone data, submission of Delegation Signer (DS) data to ICANN for publication at the root, processing DS data received from registrars, and publishing updated WHOIS/RDDS indications of DNSSEC status.

• For Registrars: Registrars change DNS information for domains via the EPP protocol (and optionally via a web portal). Registrars are responsible for maintaining DS records for their child zones with the Alibaba Cloud registry back end.

• For Registrants: Registrants (or their DNS operators) are responsible for DNS resolution and DNSSEC signing of their second-level domains, generating DS data and submitting it to the registrar, who then submits it to the registry (Alibaba Cloud registry back end).

1.4 Specification Administration

1.4.1 Specification Administration Organization

This statement is administered by the Alibaba Cloud DNS Services organization.

1.4.2 Contact Information

For inquiries regarding DNSSEC policies and practices, contact the Alibaba Cloud DNS Security Team at rspsupport@list.alibaba-inc.com or +86-13810106659.

1.4.3 Specification Change Procedures

Any change to this statement will be approved through internal review and accompanied by training for relevant personnel. The update procedure includes: technical team proposal, security team review, executive approval, and formal publication. Prior to publication, operations staff receive training on the new procedures to ensure full understanding.

2. PUBLICATION AND REPOSITORIES

2.1 Repositories

The Alibaba Cloud DNSSEC Policy Statement is published at https://alidns.com/dsp. Only registry technical and management personnel are authorized to modify this document.

2.2 Publication of Public Keys

The registry's public KSK is published externally via DS records in the parent (root) zone. Alibaba Cloud submits the KSK-derived DS record to the root zone administrator (IANA) for publication at the root. Once published, the DS record at the root forms the trust anchor for DNSSEC validation of the TLD. No additional trust anchors are used; validation relies on the root or officially published DS records.

3. OPERATIONAL REQUIREMENTS

3.1 Meaning of Domain Names

The term “domain name” in this policy follows definitions in RFC 8499 and related standards, referring to the canonical form of fully qualified domain names within the DNS. Legitimacy and constraints (e.g., length, character set) are governed by Alibaba Cloud’s TLD management rules.

3.2 Identification and Authentication of Child Zone Manager

Only entities authorized by the registry may operate on DNSSEC-related records. Typically, only accredited registrars (acting on behalf of their registrants) may activate or modify a child zone’s DNSSEC settings. They submit DS records using either the secure EPP interface (per RFC 5910) or the Alibaba Cloud web management portal. In EPP, each registrar authenticates using unique credentials prior to submitting any transaction. The web portal likewise requires authenticated login. This ensures only legitimate registrars, after verifying control of the domain, can submit or modify DS records.

3.3 Registration of Delegation Signer (DS) Resource Records

Registration process: Registrars (or agents authorized by the registrant) submit DS records via the Alibaba Cloud domain management platform using:

• EPP interface: The registrar uses its EPP account to invoke <add>, <update>, or <delete> operations to write DS data to the registry database (per RFC 5910).

• Web portal: The registrar enters DS information via the UI; the backend executes equivalent EPP operations to the registry.

Once accepted, the registry database update triggers publication of DS data at the parent zone during the next zone update cycle. WHOIS/RDDS is updated accordingly to indicate that the child has DNSSEC enabled (DS present).

3.4 Method to Prove Possession of Private Key

This system does not implement additional cryptographic challenges or domain control validations for DS submission. Operations performed by registrars on behalf of registrants are trusted, and are presumed to be made only when the registrant controls the corresponding private key material. When a registrar submits a DS record, its EPP session uses the domain’s preconfigured AuthInfo, implicitly proving administrative control of the domain. No public- or private-key fragments are required to be submitted to the registry, and no extra validation tests are performed.

3.5 Removal of DS Resource Records

3.5.1 Who Can Request Removal

Only the sponsoring registrar may request removal of a DS record. Typical cases include domain expiry, cessation of DNSSEC signing, or change of DNSSEC provider. The registrar must authenticate using its account (including the domain's AuthInfo where applicable).

3.5.2 Procedure for Removal Request

Removal may be requested via either of the following mechanisms:

• EPP command: Use <delete> to remove secDNS:dsData with proper AuthInfo or equivalent credentials. After validation, the DS will be removed from the parent during the next zone update cycle.

• Web portal: Remove the DS entry in the UI; the backend issues an equivalent EPP delete request.

Once the DS is removed, the parent ceases to authenticate the child's DNSKEY. The chain of trust is broken and the child is considered insecure. WHOIS/RDDS and zone data will reflect the new status.

3.5.3 Emergency Removal Request

Because DS operations are executed through real-time EPP channels, the system can process deletions at any time. Submitting the delete command immediately breaks the chain of trust; no additional special approval is required in emergencies.

4. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

4.1 Physical Controls

Alibaba Cloud DNSSEC infrastructure is deployed in high-security (Tier III) data centers. Site selection and construction follow industry standards and employ strict physical security:

• Site location and construction: Registry (including DNSSEC) services are deployed in data centers located in two cities with active-active redundancy. DNS services remain available should one site fail. All facilities employ rigorous badge access; only background-checked and authorized personnel are permitted entry.

• Power, HVAC, fire and water protection: Both facilities provide redundant and backup power, air conditioning, as well as fire and water protection. Each site backs up the other's DNSSEC services. Sensitive media (e.g., signer backups and secure storage media) are kept in multiple locked safes or rooms accessible only to senior management or designated operators.

• Off-site backup: Critical data for signing systems is regularly backed up and replicated to off-site locations. For example, key-store backups are distributed across data center storage systems, enabling swift switchover in case of any single-point failure. Offline backups are stored in secure off-site locations to mitigate regional disasters and support business continuity.

4.2 Procedural Controls

Trusted roles and defined procedures govern DNSSEC operations. Members of the Alibaba Cloud DNSSEC operations team receive privileged access to signing systems. Each trusted individual authenticates with assigned credentials to access HSMs and signing servers. Routine operations (e.g., scheduled resigning) may be carried out by a single authorized operator for responsiveness, while critical steps (e.g., key generation, emergency rollover) are performed by senior engineers with at least security lead notification to improve oversight and auditability.

Separation of duties is applied so that approval and execution of critical operations are conducted by different personnel. For instance, signing software releases, configuration changes, and certificate management require security team review rather than self-approval by the operator performing the change. Least-privilege principles are enforced throughout.

4.3 Personnel Controls

Personnel engaged in DNSSEC operations must have sufficient DNS security knowledge and relevant experience. New team members undergo internal technical vetting. Alibaba Cloud provides regular DNSSEC training, including operational procedures, security policies, and incident response exercises. Background checks are performed for key roles such as signing system administrators.

To avoid concentration of critical duties, key roles are eligible for rotation according to project needs, reducing the risk of knowledge silos. Policy violations are addressed per corporate procedures, up to and including removal of authorization or termination.

External contractors needing access must sign NDAs and work under the supervision of authorized operations staff. Comprehensive run-books and process manuals are supplied; significant changes are documented and communicated to ensure team-wide awareness and adherence.

4.4 Audit Logging Procedures

Comprehensive logging is used to detect issues and support auditing.

• Types of events recorded: All critical events are logged, including physical facility entry, administrator logins, key operations (generation, activation, deactivation, destruction), and system configuration changes. For example, access control systems record every entry/exit; signing servers log each key generation, signing action, and zone publication.

• Frequency of processing logs: Logs are collected in real time and analyzed by automated monitoring. After each key ceremony, audit logs receive focused review to detect anomalies. If alerts or irregularities are identified, the security team investigates immediately.

• Retention period: Logs are retained online for at least one year and archived offline for no less than ten years.

• Protection of audit logs: The audit logging system is deployed in an isolated secure environment. Logs are immutable to ordinary operators. Write-once media and digital signing are used to prevent tampering. Only a limited set of authorized auditors may access logs in read-only mode.

• Audit log backup procedures: Logs are periodically backed up to off-site storage. For example, following each key ceremony, the log repository is copied to a secure offline facility. Backups are encrypted and stored in safes or dedicated storage systems to prevent loss due to physical damage.

• Audit collection system and vulnerability assessments: Automated log collection and analysis tools are employed. Periodic vulnerability assessments and penetration tests are

conducted on the logging and signing infrastructure. Software and configuration updates undergo security testing prior to production deployment.

4.5 Compromise and Disaster Recovery

• Incident handling: Upon detection or suspicion of a security incident (e.g., unauthorized key access, anomalous logging patterns, or signing errors), the incident response team initiates investigation immediately. If key compromise risk is identified, an emergency key rollover is executed, replacing affected keys and publishing updated trust information.

• Corrupted resources: If signing software, configurations, or hardware are damaged, the business continuity plan is executed to activate standby systems or restore from the latest backup. All sensitive data restoration requires multi-factor authentication and authorized access.

• Private key compromise: In the event of confirmed private key compromise, response follows industry best practices (e.g., rapid replacement and DS updates). New KSKs are generated, minimal continued trust is maintained with old material only as needed, and parent DS updates are expedited. Enhanced monitoring continues until the new chain is effective.

• Business continuity and IT disaster recovery: Critical servers and signers are deployed across multiple availability zones, with regular data replication. Offline backups are maintained and recovery procedures are periodically exercised to ensure rapid failover.

4.6 Entity Termination

If Alibaba Cloud’s DNSSEC service (or relevant entity) is terminated, DNSSEC signing will be disabled, private keys will be destroyed or archived securely, DS records will be removed from the parent to break the chain of trust, and audit logs will be handed over to appropriate authorities or operations teams. The decommissioning process follows legal and contractual obligations.

5. TECHNICAL SECURITY CONTROLS

5.1 Key Pair Generation and Installation

KSK and ZSK key pairs are generated and protected by dedicated Hardware Security Modules (HSMs).

• Key pair generation: Both KSK and ZSK are generated inside cloud HSMs using secure hardware RNGs. The HSMs are FIPS 140-2 Level 3 validated. Generation occurs in controlled environments and only authorized personnel can activate the process via secure channels.

• Public key delivery: Public keys are published as DNSKEY RRs in the zone. The KSK-derived DS hash is submitted through standard processes to the parent (e.g., the root), closing the validation chain. All validation information is distributed via normal parent/child DNSSEC mechanisms; no external trust channels are required.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

• Cryptographic module standards and controls: Alibaba Cloud HSMs meet FIPS 140-2 Level 3. All critical operations (generation, storage, key use) occur within the HSM. Dedicated instances prevent unauthorized access.

• Private key storage and backup: Keys remain within HSMs and benefit from tamper resistance. HSM clusters comprise at least two instances (one primary and at least one backup). Keys are securely replicated within the cluster to avoid single points of failure.

• Private key archival: Retired keys are revoked within the HSM and can be securely deleted or overwritten. Keys are not retained longer than necessary; short-term recovery may be possible from cluster backups before final destruction.

• Private key transfer: Keys are not exported from or imported into HSMs during normal operations. If migration is required (e.g., equipment replacement), new HSM clusters are provisioned and keys are re-established within them under strict authorization.

• Activation/deactivation: Keys are marked online when needed and deactivated when not in use. All such actions are logged.

• Destruction: When a key is no longer required, destruction procedures render the key unrecoverable at the hardware level.

Additional measures include one-key-per-domain usage policies, clear key-purpose scoping (signing only), least-privilege enforcement, and maintaining records of which keys signed which RRsets for auditability.

5.3 Computer Security Controls

Signing systems and HSM management servers run hardened operating systems with timely security updates. Production and development/test environments are segregated. Access is tightly restricted; administrators use MFA and are prohibited from performing critical operations from unauthorized devices. Non-essential services and ports are disabled; firewalls and IDS/IPS are enabled to protect critical servers.

5.4 Network Security Controls

Signing infrastructure resides within Alibaba Cloud's private VPC and is separated from the public Internet by firewalls. Only necessary DNS signing data traverses public networks; management operations are limited to internal connections. All communications use encrypted protocols (e.g., HTTPS/API). HSMs accept connections only from trusted network segments; administrators use VPN for remote maintenance.

5.5 Timestamping

System clocks are synchronized via reliable NTP sources. All signing actions are timestamped to ensure correct signature validity windows. Time synchronization logs are included in audits to detect manipulation.

5.6 Life-Cycle Technical Controls

Mature signing software and tools are used with strict version control. Any software/configuration update is validated for security and stability in staging prior to production rollout. Changes undergo code review, diffing, and impact analysis. Software artifacts are provenance-checked and integrity-verified to prevent supply-chain attacks.

6. ZONE SIGNING

6.1 Key Lengths, Key Types, and Algorithms

The registry uses ECDSA P-256 (algorithm 13, ECDSAP256SHA256) as defined in RFC 6605. This configuration provides a strong balance of security and performance, reducing signature size and improving response efficiency.

6.2 Authenticated Denial of Existence

NSEC3 with Opt-Out is used to provide authenticated denial of existence. NSEC3's hashed chain resists zone-walking, and Opt-Out reduces the number of NSEC3 records where many unsigned delegations exist.

6.3 Signature Format

RRSIG records use SHA-256 hashing with ECDSA P-256 signatures. Signature length and on-the-wire format conform to RFC 4034.

6.4 Key Rollover

• KSK rollover: Double-signature rollover per RFC 6781 §4.1.2 is used to ensure smooth transition.

• ZSK rollover: Pre-Publish rollover per RFC 6781 §4.1.1.1 is used to ensure cryptographic continuity and prevent DNSSEC validation failure.

Typical cadence: KSK every three years; ZSK every three months.
ZSK rollover is carried out every three months. KSK rollover is carried out every 3 years

6.5 Signature Lifetime and Re-signing Frequency

RRSIG validity is 14 days. The signature will be refreshed a period (0.1 * RRSIG validity + propagation-delay(1h) + zone-max-ttl(maximal TTL among all the records in the zone) before its expiration. Additionally, any change to an RRset (add/modify/delete) triggers immediate re-signing with the current ZSK. Thus, updated records are signed immediately.

6.6 Verification of Resource Records

All RRset signatures are verified prior to publication.

6.7 Verification of zone signing key set

Verification of the zone signing key set is performed by validating the public key data contained in the Key Signing Record.

6.8 Resource Records Time-to-Live

DNSKey	15 minutes
NSEC3	SOA minimum (24 hours)
Delegation Signer (DS)	24 hours
RRSIG	varies depending on the RR covered

7. COMPLIANCE AUDIT

7.1 Frequency of Entity Compliance Audit

Annual internal compliance audits are performed against this policy.

7.2 Identity/Qualifications of Auditor

Audits are conducted by internal or external auditors with information security expertise, independent of day-to-day operations, and with appropriate qualifications or experience.

7.3 Auditor's Relationship to Audited Party

Auditors are organizationally independent of the Alibaba Cloud DNSSEC operations team. Reports are submitted directly to senior management to preserve objectivity.

7.4 Topics Covered by Audit

Environmental, network and software controls, DNS/DNSSEC operations, key management practices and operations.

7.5 Actions Taken as a Result of Deficiency

Any nonconformity is recorded and corrective actions are required within set timeframes. Significant issues are reported to management and tracked in subsequent audit cycles.

7.6 Communication of Results

Audit results and remediation progress are communicated internally via reports and meetings. Disclosable information may be shared with stakeholders or regulators where appropriate.

8. LEGAL MATTERS

This DPS is to be construed in accordance with and governed by the internal laws and regulations of the People's Republic of China. Contracts, service agreements, or liability terms involving DNSSEC will reference this policy as the technical specification. In the event of conflict with applicable law, the law prevails; this document serves as a technical implementation guide and does not itself carry legal force.

The following material shall be considered confidential:

- ✓ Private keys
- ✓ Information necessary to retrieve/recover private keys
- ✓ Disaster recovery plans (DRPs)
- ✓ Any operational details relevant to the management and administration of DNS keys, including but not limited to network, software, hardware details.

The Company does not implicitly or explicitly provide any warranty, and assumes no legal responsibility for any procedure or function described in this DPS. The Company shall not be liable for any financial damages, losses arising from the use of keys, or any other liabilities. All legal questions or concerns should be sent to rspsupport@list.alibaba-inc.com.