Table of contents

DNSSEC Policies for

.ALIBABA

.ALIPAY

Afilias DNSSEC Practice Statement (DPS)

Version 1.04
2012-04-04

1. INTRODUCTION

1.1. Overview

This document was created using the template provided under the current practicing documentation.[1] This document comprises the practices utilized by Afilias to operate DNS zones as it relates to the DNS Security Extensions. Unless stated otherwise within this document, these statements pertain to all TLD zones under Afilias auspice that have been signed.

1.2. Document name and identification

Afilias DNSSEC Practice Statement (DPS)
Version 1.04

1.3. Community and Applicability

This section describes the various "stakeholders" of the functionality provided by DNSSEC and a signed TLD.

1.3.1. The TLD Registry

Afilias operates in two distinct modes: (1) As a Registry Operator (RO), where the TLD has been directly delegated to Afilias by ICANN, and (2) as a Back End Service Provider (BESP), where Afilias operates and performs the functions of maintaining the zone, on behalf of another entity (which acts as the RO). In the case where Afilias is the RO for a zone, Afilias is also acting as the BESP.

The Registry is expected to perform the following functions:

- Generate the Key Signing Keys (KSK) for the zone.
- Generate the Zone Signing Keys (ZSK) for the zone.
- Sign the ZSK using the KSK.
- Sign the relevant Resource Records of the zone using the ZSK.
- Update the ZSK and KSK as needed.
- Send Delegation Signer (DS) Resource records to ICANN for inclusion into the root zone.
- Receive DS Resource Records from accredited registrars, and update the zone accordingly.
- Update the WHOIS information accordingly.

1.3.2. Accredited Registrars

Registrars that are accredited by a given TLD RO are required to make changes to the zone using one of two mechanisms: (1) via EPP, or (2) via a Web Administration Tool. The Web Administration Tool is an Afilias provided front end to EPP, so, in effect, all changes to the registry are made via EPP. For DNSSEC, registrars are expected to maintain Delegation Signer (DS) records with Afilias on behalf of their customer, the registrant.

1.3.3. Registrants

Registrants are responsible for ensuring that their second level zones are properly signed and maintained. They must also generate and upload DS records for their signed zones to their registrar (who, in turn, sends these into Afilias).

1.4. Specification Administration

1.4.1. Specification administration organization

Afilias maintains this specification.

1 Definitions for many of the terms used in this document are defined in Section 2 of the current Internet Draft from which this work was derived (as of this revision, that document is draft-ietf-dnsop-dnssec-dps-framework-07.txt. References will be changed as needed as that document changes, or is published as an RFC.

1.4.2. Contact Information

Questions or concerns regarding this DPS, or the operation of a signed TLD should be sent to the Afilias Customer Support Center. They can be reached via:

Phone: +1 416.646.3306
Email: support@afilias.info

1.4.3. Specification change procedures

The DPS is reviewed periodically and updated as appropriate.

All changes are reviewed by operations and security teams and submitted to executive management for approval. Once accepted, procedures are updated, and appropriate personnel are trained on any new or changed practice. Once all preparatory work has been completed, the DPS is published and becomes effective as of its publication.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

This DPS can be found at http://www.afilias.info/dps
Only the Afilias Operations department has the ability to update the contents of the website. ACLs on the file are Read-Only.

2.2. Publication of key signing keys

The "chain of trust" is maintained for Afilias TLD zones by sending DS records to ICANN for inclusion in the root zone delegation of the TLD. These DS records correspond to at least one active KSK in the zone. As such, no publication of an additional trust anchor is required.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

Policies regarding restrictions on domain names within a given zone are specified by the registry operator, and vary from TLD to TLD.

3.2. Identification and authentication of child zone manager

Registry Operators must first give express permission to Afilias to permit DNSSEC for child zones in a given TLD. Only registrars (on behalf of their registrants) are permitted to activate DNSSEC for a child zone. To activate DNSSEC, a registrar must submit a Delegation Signer (DS) record either via the Web Administration Tool, or via EPP (according to RFC 5910).

For EPP, each registrar has unique credentials to access the TLD registry, which are verified before EPP transactions of any kind can be conducted. For the Web Administration Tool, certificates are used to uniquely identify each registrar.

3.3. Registration of delegation signer (DS) resource records

DS records are sent to the registry by the registrar via EPP (specifically, according to RFC 5910). Once submitted to the TLD registry, the WHOIS data is changed, and the zone changes are automatically propagated out to the DNS infrastructure.

3.4. Method to prove possession of private key

It is the responsibility of the accredited registrar to ensure the integrity of the data submitted to Afilias. There is no requirement that a corresponding DNSKEY already be published in a zone before a DS record is submitted to the parent. This makes proof of possession of a private key unpredictable.

Afilias therefore does not perform any tests to prove possession of a private key.

3.5. Removal of DS record

3.5.1. Who can request removal

Only the sponsoring registrar for a domain name can add, change, or delete DS records for that domain name. Registrars must provide an Auth-Info code to verify any change for this domain name.

3.5.2. Procedure for removal request

DS records are removed using the appropriate EPP command, as specified by RFC 5910. Only the Sponsoring Registrar can request a DS record be removed, and then only if they include the correct Auth-Info code.

3.5.3. Emergency removal request

Because this is facilitated via EPP, and the system is updated continuously, there is no additional procedure required for an emergency removal request.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

Afilias uses two geographically separate sites located in different countries that are not part of our offices. Both sites are physically protected environments that deter, prevent, and detect unauthorized use of, access to, and disclosure of sensitive information and systems. Both facilities limit access to authorized personnel. Visitors are only permitted by escort from Authorized personnel, and for a specific purpose (such as hardware repair by a technician).

Both facilities provide redundant and backup power, air conditioning, and fire suppression and protection services. The sites provide redundant and backup DNSSEC services for each other. Reasonable precautions have been taken to minimize the impact of water exposure to Afilias systems.

Media with sensitive information is stored within Afilias facilities with appropriate physical and logical access controls designed to limit access to authorized personnel.

Sensitive documents, materials, and media are shredded or rendered unreadable before disposal.

Afilias performs routine backups of critical system data and maintains an off-site backup with a bonded third party storage facility.

4.2. Procedural Controls

There are at least two operational teams with access to and responsibility for the signer systems. Each team member holds a part of the password necessary to grant access to the signer systems. Any task performed on a signer system requires an authorized representative from each team to be present.

4.3. Personnel Controls

Afilias requires that all personnel taking part in a trusted role have to have been working for Afilias for at least one year and must have the qualifications necessary for the job role.

Afilias provides training to all personnel upon hire as well as requisite training needed to perform job responsibilities. Refresher training and updates are provided as needed. Personnel and rotated and replaced as needed.

In limited circumstances, contractors may be permitted to occupy a trusted role. Any such contractor is required to meet the same criteria applied to an Afilias employee in a comparable position.

Afilias provides all employees with the materials and documentation necessary to perform their job responsibilities.

4.4. Audit Logging Procedures

All key life cycle events, including but not limited to generation, activation, rollover, destruction, and use, whether successful or unsuccessful, are logged with a system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

Access to physical facilities is logged by the facility and the log is only accessible to authorized personnel.

Afilias monitors all log entries for alerts based on irregularities and incidents. The Afilias security team reviews all audit logs at least weekly for suspicious or unusual activity.

4.5. Compromise and Disaster Recovery

In the event of a key compromise or disaster, Afilias' incident response team would be notified. The response team has documented procedures for investigation, escalation, and response. The team is responsible for assessing the situation, developing an action plan, and implementing the action plan with approval from executive management.

Afilias maintains redundant facilities to ensure immediate availability of a disaster recovery site should one site become unavailable. Key data is cloned, encrypted, and sent to a hot spare in the same facility, and to two spares in the redundant facility. The ability to encrypt and decrypt the key data resides entirely within each system's High Security Module, and exists nowhere external to the signing systems.

4.6. Entity termination

Afilias has adopted a DNSSEC termination plan in the event that the roles and responsibilities of the signing services must transition to other entities. Afilias will coordinate with all required parties in order to execute the transition in a secure and transparent manner.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

All key pairs are generated on the signer systems according to parameters set by the operational team. The signer systems meet the requirements of FIPS 140-2 level 3. The public key is automatically inserted in the TLD zone file as a DNSKEY resource record as part of the signing process. A DS record is made available for submission to the parent (root) zone.

The signer system maintains the separation of the KSK from the ZSK and manages the use of each key pair as appropriate. Each key is used for only one zone.

5.2. Private key protection and Cryptographic Module

Engineering Controls

All signing systems are FIPS 140-2 level 3 certified. No unencrypted access to the private key is permitted. Access to the signer system is specified in the Procedural and Personnel Control sections.

Multiple redundant signing systems are maintained. The systems include a mechanism to backup key pairs and other operational parameters to each other in a secure manner. Private keys are not

otherwise backed up, escrowed, or archived. When a private key is deactivated it is destroyed by the signing system.

A trusted team has the authority to create, activate, and deactivate key pairs, and executes the responsibility according to documented policies and procedures.

5.3. Computer Security Controls

Afilias ensures that the systems maintaining key software and data files are trustworthy systems secure from unauthorized access. In addition, Afilias limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

5.4. Network Security Controls

The signing systems are placed in Afilias' production systems, which are logically separated from all other systems. Use of normal network security mechanisms such as firewalls mitigate intrusion threats; only restricted role users are allowed access to production systems, and their work is logged.

5.5. Timestamping

The signer systems securely synchronize their system clocks with a trusted time source inside the Afilias network.

5.6. Life Cycle Technical Controls

Applications developed and implemented by Afilias conform to its development and change management procedures. All software is traceable using version control systems. Software updates in production are part of a package update mechanism, controlled via restricted role access and updated via automated recipes. All updates and patches are subject to complete verification prior to deployment.

Afilias uses a third-party solution on its signer systems, where updates are tested in a secure lab environment prior to deployment.

6. ZONE SIGNING

6.1. Key lengths and algorithms

Key Signing Key
Afilias uses a key length of 2048 bits with RSA as the generation algorithm.
Zone Signing Key
Afilias uses a key length of 1024 bits with RSA as the generation algorithm.

6.2. Authenticated denial of existence

Authenticated denial of existence will be provided through the use of NSEC3 records as specified in RFC 5155 [RFC5155].

6.3. Signature format

SHA1, using RSA

6.4. Zone signing key roll-over

Afilias will roll the ZSK with a pre-publishing scheme as described in RFC 4641, section 4.2.1.1. ZSK roll-over is carried out once a month.

6.5. Key signing key roll-over

Afilias will roll the KSK with a double-signing scheme as described in RFC 4641, section 4.2.1.2. There are no planned KSK rollover frequencies defined at this time.

6.6. Signature life-time and re-signing frequency

Zones are signed once every 8 or 9 days (4 times a month), with a signature life-time of 20 days. Jitter is introduced to avoid presumptive attacks during signing.

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. Verification of resource records

All RRset signatures are verified prior to publication.

6.9. 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

Compliance Audits are intended to be conducted at least biennially.

7.2. Identity/qualifications of auditor

The auditor will be an entity who is proficient in the technologies they are auditing, and are independent from Afilias.

7.3. Auditor's relationship to audited party

Auditors must be independent to Afilias.

7.4. Topics covered by audit

Environmental, network and software controls, operations, key management practices and operations.

7.5. Actions taken as a result of deficiency

Any gaps identified in the audit will result in the creation of an action map, which lists what actions are necessary for the resolution of each gap. Management will design and implement mitigating steps to close the gaps identified.

7.6. Communication of results

Afilias will publish results at http://www.afilias.info/dps.

8. LEGAL MATTERS

This DPS is to be construed in accordance with and governed by the internal laws of Ireland without giving effect to any choice of law rule that would cause the application of the laws of any jurisdiction other than the internal laws of Ireland.

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.

Afilias does not implicitly or explicitly provide any warranty, and has no legal responsibility for any procedure or function within this DPS. Afilias shall not be liable for any financial damages or losses arising from the use of keys, or any other liabilities. All legal questions or concerns should be sent to legal@afilias.info.

DNSSEC Policy for

.TAOBAO

DNSSEC Practice Statement

26 September 2017

neustar

This document is provided pursuant to the disclaimer provided on the last page.

Contact

Name	Customer Support
Address	Neustar Inc. 21575 Ridgetop Circle Sterling, Virginia, 20166 United States of America
Phone	+1 844 677 2878 +1 571 434 6700
Email	reg@support.neustar

Classification

Public

Definitions

In this document:

DNS means the 'Domain Name System' that is a distributed database and hierarchical global infrastructure deployed on the Internet and private IP-based networks used to resolve domain names into IP addresses.

DNSKEY means the Domain Name System KEY, a Resource Record that contains the cryptographic keys used to sign records in a Zone.

DNSSEC means Domain Name System Security Extensions which are a suite of specifications for securing certain kinds of information provided by the DNS.

End Users means those accessing services supplied on the domain name in the TLD.

EPP means Extensible Provisioning Protocol.

Key Rollover means the process of generating new cryptographic keys and replacing the keys in use.

KSK means the 'Key Signing Key' used to sign DNSKEY records.

Recursive Name Server Providers means providers who provide their customers with name servers to use.

Registrant means a natural or legal person, company or organization in whose name a domain name is assigned in the TLD.

Registrar means an entity that is authorized to offer domain name registration services in relation to the TLD

Registry Operator means the entity that is a party to the Registry Agreement with ICANN for the TLD.

Registry means the systems used to record, store and maintain details of domain names in the TLD.

Registry Service Provider means the technical services provider providing Registry functions to the Registry Operator.

Resource Record means the basic data element in the DNS that define the structure and content of the DNS.

TLD means Top Level Domain and for the purpose of this policy refers to .TAOBAO

We, **us** and **our** means any or all of the Neustar Inc. group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Zone means a sub-section of the DNS hierarchy for which administrative responsibility has been delegated.

Zone File means a data file which describes a Zone.

ZSK means the 'Zone Signing Key' used to sign records.

Purpose

This document is our DNSSEC Practice Statement for the TLD Zone. It states the considerations that we follow in providing DNSSEC services for the Zone.

Scope

This document covers only that information required to outline the DNSSEC Practices standpoint as it relates to the Zone as required by the DNSSEC Policy & Practice Statement Framework RFC.

Audience

ICANN, Registrars, Registrants and the general public.

Contents

1 Introduction

This document details the practices we use on behalf of the Registry Operator in our capacity as a Registry Service Provider.

This document is our DNSSEC Practice Statement for the TLD. It states the considerations that we follow in providing DNSSEC services for the TLD. The Zone File data, including DNSSEC keys used to sign the Zone File remain the property of the Registry Operator of the TLD.

1.1 Overview

DNSSEC was proposed to add data integrity and authentication to the DNS. The DNSSEC system asserts trustworthiness of data using a chain of public-private keys. For End Users wanting to use DNSSEC enabled name servers, DNSSEC aware resolvers will be necessary to take advantage of the system.

1.2 Document Name and Identification

Document Name	DNSSEC Practice Statement
Version	2.0
Date Created	12 May 2011
Date Modified	23 August 2017

1.3 Community and Applicability

The following stakeholders of this DNSSEC implementation have been identified:

- End Users
- Recursive Name Server Providers
- Registrant
- Registrar
- Registry Operator

Relationship between different entities is regulated through the following agreements:

Relationship	Agreement
Registry Operator and Registry Service Provider	Registry Operator – Registry Service Provider Agreement
Registry Operator and Registrar	Registrar – Registry Agreement
Registry Operator and Registrant	Registrant – Registrar Agreement

1.4 Specification Administration

1.4.1 Specification Administration Organization

Organization	Neustar Inc.
Website	www.registry.neustar

1.4.2 Contact Information

Name	Customer Support
Address	Neustar Inc. 21575 Ridgetop Circle Sterling, Virginia, 20166 United States of America
Phone	+1 844 677 2878 +1 571 434 6700
Email	reg@support.neustar

1.4.3 Specification Change Procedures

Queries with regards to the content of this document may be made directly in writing via email, postal mail or telephone to the contact listed above. Some requests may only be made in writing via email or postal mail and requestors may be notified to do so should they place the initial request via telephone.

We reserve the right to amend the DNSSEC Practice Statement without notification. Updated or new DNSSEC Practice Statements will be published as specified in Section 2.

2 Publication Repositories

2.1 Repositories

This DNSSEC Practice Statement will be published on the Registry Operator's website.

2.2 Publication of Public Keys

Delegation Signing (DS) records of SEP keys are made available by publication in the root Zone. We maintain a website, as described in Section 1.4.1, on which we publish notifications of policy changes specific to DNSSEC, and alerts in the event of an emergency Key Rollover.

2.3 Access Controls on Repositories

Information that the organization deems publically viewable is published on the Registry Operator's website. Other information may be requested by writing to the contact specified in Section 1.4.2. Provision of requested information is at our sole discretion.

This document may refer to documents that are confidential in nature, or considered for our internal use. These documents may be made available on request after consideration on a case by case basis. We reserve the right to deny access to confidential documents or documents classified for internal use only.

We will take all the necessary measures to protect information and material that is of a secure nature with respect to DNSSEC. These measures will be commensurate with the nature of such information and material being secured.

3 Operational Requirements

3.1 Meaning of Domain Names

Restrictions and policy of naming of child Zones is determined by the appropriate policy in place governing the TLD.

3.2 Identification and Authentication of Child Zone Manager

We do not conduct any identification or authentication of the child Zone manager. This is the responsibility of the Registrar of Record.

3.3 Registration of Delegation Signing (DS) Resource Records

The chain-of-trust to the child Zone is established by publishing a signed DS record into the Zone.

The submission of a DS record is carried out by the Registrar of Record using the Registry interface, that is, the EPP service.

We will sign the DS record using the Zone's ZSK(s) and publish the resulting signature along with the DS record to build the chain-of-trust.

3.4 Method to Prove Possession of Private Key

Registrars are mandated by agreements they are subject to, as specified in Section 1.3, to authenticate Registrants before accepting any changes from the Registrant that they may choose to submit to the Registry.

The need for Registrants to explicitly prove the possession of a private key is invalidated due to workings of DNSSEC, as the Registrant submits a DS record using interfaces provided by the Registrar. A chain of trust is established when the Registrant signs their Zone using the private key corresponding to the DS submitted.

In the case where the Registrant does not possess the private component corresponding to the DS, they will not be able to create valid signatures for records in their Zone and the chain of trust culminating at their records will be invalidated.

3.5 Removal of DS Resource Record

The Registrar of Record uses the Registry interface to remove the DS record.

We may remove a DS record and re-delegate the child-Zone in consultation with the Registry Operator, Registrar and Registrant if it is deemed that the child Zone has been compromised. Such a removal may be initiated by the Registry Operator, Registrar, Registrant or us.

4 Facility, Management and Operational Controls

4.1 Physical Controls

4.1.1 Site Location and Construction

The Registry architecture consists of a primary site, a secondary site, and geographically dispersed DNS sites. The components at the secondary site are identical to those at the primary site.

We choose data centers for Registry operations after carrying out stringent checks and visits on a large number of available providers. Each data center provides the following minimum set of requirements:

- Redundant Power Feeds
- Un-interruptible Power Supply (minimum 30 minutes)
- Backup Power Source (generator)
- Fire Detection System (High Sensitivity Smoke Detectors)
- Fire Suppression System
- Water Detection System
- Multiple (Diverse) Internet Links
- Stringent Physical Security (On-site security personnel, bio-metric access control)
- 24/7 Access Availability
- Robust Cooling System (HVAC)
- Real Time/Pro-active Power and Environmental Monitoring

4.1.2 Physical Access

Access to all Registry systems at each data center is restricted. Equipment is located in private locked racks and keys to these are only given out to authorized administrators as part of stringent data center security procedures.

Remote environment surveillance is employed, including cameras and entry alarms.

In addition, direct physical access to equipment is monitored and controlled as an un-trusted interface, login sessions are not permitted to idle for long periods, and network port security is employed to minimize the opportunity for a direct network connection to be used as a security threat vector.

4.1.3 Power and Air Conditioning

N+1 power is utilized at all selected Registry data centers to maximize uptime availability. Uninterruptible Power Supply (UPS) systems are used to prevent power spikes, surges, and brownouts, and redundant backup diesel generators provide additional runtime. Alerts are set on all power provision systems to allow us to begin failover preparation in the event of a potential power provision issue to ensure a smooth and controlled failover if required.

Similarly N+1 monitored air conditioning at Registry data centers is configured to provide maximum temperature control for the installed equipment in order to provide a stable operating environment.

4.1.4 Water Exposures

We have implemented reasonable measures for flood detection and protection at its sites, as well as having a key selection criterion for Registry and DNS sites that they be in areas which are not likely to suffer flooding.

4.1.5 Fire Prevention and Protection

Fire protection in each data centre is world-class, with very early smoke detection apparatus installed and set as one element of a multi-stage, human controlled multi-zone dry-pipe, double-interlock, pre-action fire suppression system in a configuration that complies with local regulations and industry best practice.

4.1.6 Media Storage

Sensitive media is stored offsite securely and is protected by access restrictions. Such media is reasonably protected from fire, water and other disastrous environmental elements.

4.1.7 Waste Disposal

Sensitive documents are shredded before disposal. Where sensitive data is stored electronically, appropriate means are used to render the data unsalvageable prior to disposal.

4.1.8 Off-site Backup

DNSSEC components and necessary data are stored off-site regularly as part of backup and disaster recovery. Such data is protected by reasonably secure means and has access restrictions that are similar to those implemented for online systems and data.

4.2 Procedural controls

4.2.1 Trusted Roles

The following table presents all procedures that we have implemented for providing DNSSEC services for the TLD. These procedures require corresponding roles as below:

Procedure	Roles
Key Rollover	▪ System Administrator ▪ Security Officer
Key Creation	▪ System Administrator ▪ Security Officer
Disposal of old Key	▪ System Administrator ▪ Security Officer
KSK Rollover	▪ System Administrator ▪ Security Officer

4.2.2 Number of Persons Required Per Task

The number of persons required varies per task or procedure. Please refer to Section 4.2.1 for further information.

4.2.3 Identification and Authentication for Each Role

We require all personnel dealing with secure DNSSEC material and systems to have completed security checks. We reserve the right to interpret the findings of the security check equitably with respect to the secure nature of this DNSSEC implementation as covered by our Human Resources policy.

4.2.4 Tasks Requiring Separation of Duties

Tasks that are part of a Key Rollover require separation of duties. Please refer to Section 4.2.1 for further information.

4.3 Personnel Controls

4.3.1 Qualifications, Experience and Clearance Requirements

Each person who fulfils a DNSSEC role must:

- Be employed full time by us;
- Not be within their initial employment probation period; and
- Have completed a security check.

4.3.2 Background Check Procedures

A security check must be completed prior to taking part in DNSSEC tasks.

4.3.3 Training Requirements

Each person who is responsible for DNSSEC tasks must have attended our DNSSEC training session and be fully qualified to perform that function.

We provide frequent retraining to our employees to assist them with keeping their skills current and enabling them to perform their job proficiently.

4.3.4 Job Rotation Frequency and Sequence

We rotate the responsibility for DNSSEC related tasks between staff that satisfy the skill set required to execute those tasks.

4.3.5 Sanctions for Unauthorized Actions

We will conduct investigations where we detect or are made aware of unauthorized actions on the DNSSEC environment. We will take necessary disciplinary action should such action be warranted.

4.3.6 Contracting Personnel Requirements

Contractors and consultants are not authorized to participate in secure DNSSEC tasks.

4.3.7 Documentation Supplied to Personnel

We provide requisite training and support material to our employees to enable them to proficiently perform their duties. Supplied documentation is provided to staff under security controlled guidelines to ensure operational security.

4.4 Audit Logging Procedures

All systems deployed utilize audit log functionality which is coordinated centrally. Logging is used to monitor the health of systems, trace any issues and conduct diagnosis.

4.4.1 Types of Events Recorded

A high level categorization of events that are recorded is as follows:

Zone File Activity	Addition and removal of domain names. Changes in Resource Records associated with domain names in the TLD.
Hardware Failures	Failure of server and network infrastructure or their components.
Access To Hardware	Changes in access controls granting physical, console and network access to infrastructure.
Security Profile	Changes in settings and configuration that determine the security of infrastructure or the services it provides.
System Updates	Updates to operating environment and packages on servers and firmware on network appliances.
Network Activity	Divergences from observed patterns of network activities.
Redundancy Failure	Failure in backups, Disaster Recovery or transitions between primary and secondary site.
Incident Management	Incidents being raised, allocated, acted upon and resolved.
Failure In Event Monitoring	Failure of event monitoring system. This would be detected using a secondary event monitoring system.

4.4.2 Frequency of Processing Log

Audit logs and event monitoring feed into our monitoring system that raises alerts based on states that are not normal in regular operations.

4.4.3 Retention Period for Audit Log Information

Audit log information is securely archived for a period of 7 years.

4.4.4 Protection of Audit Log

Audit logs are only available to our staff with appropriate privileges. Audit logs do not contain private keys or other sensitive information that may lead to a compromise by using existing and known methods.

4.4.5 Audit Log Backup Procedures

Audit logs are backed up as part of the backup procedures in place for production systems. Those logs containing sensitive data are stored in a secure manner. Disposal of audit logs is carried out in accordance with Section 4.1.7.

4.4.6 Audit Collection System

In addition to information recorded manually by staff while conducting operations, Audit information is collected in Audit logs automatically. Methods specific to applications and operating environments are used to record audit logs.

Manual logs are scanned and the original documents archived in a fireproof safe.

4.4.7 Notification to Event-causing Subject

No notification is issued to the event-causing subject as part of automatic event logging. However, selected events are monitored and alerts delivered to our employees that may choose to notify event-causing subjects.

During execution of manual procedures the participants are informed that logging is taking place.

4.4.8 Vulnerability Assessments

We engage an external entity to perform a vulnerability audit annually. This is in addition to monitoring and analysis that is in place for production systems. A broader annual compliance audit is also performed as discussed in Section **Error! Reference source not found.**.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and Compromise Handling Procedures

Any event that may cause or has caused an outage, damage to the Registry, or disruption to service is classified as an incident. Any event that is an incident and has resulted in exposure of private DNSSEC components is classified as a compromise. Incidents are addressed using our incident management procedures.

Should we detect or be notified of a compromise, we will conduct an investigation in order to determine the nature and seriousness of the compromise. Following the investigation we will take the necessary measures to re-instate a secure state. This may involve rolling over the ZSK(s), KSK(s) or both.

Incident management is conducted in accordance with our Incident Management Process.

4.5.2 Corrupted Computing Resources, Software and/or Data

Detection or notification of corrupted computing resources will be responded to with appropriate incident management procedures and escalation procedures as necessary.

4.5.3 Entity Private Key Compromise Procedures

An emergency ZSK and KSK rollover will be carried out in the event that we detect or are notified of a private key compromise of either key. On suspicion of a compromise, we will instigate an investigation to determine the validity of such suspicions. We will notify the public through an update that will be published in accordance with Section 2.2.

4.5.4 Business Continuity and IT Disaster Recovery Capabilities

Business continuity planning and disaster recovery for DNSSEC is carried out in accordance with our Business Continuity and Disaster Recovery Policies, and contracts in place with the Registry Operator.

4.6 Entity Termination

We will ensure that should our responsibilities to manage DNS for the TLD be terminated, we will co-ordinate with all required parties in order to execute a transition.

Should it be decided to return the TLD to an unsigned position, we will endeavor to carry it out in an orderly manner.

5 Technical Security Controls

This section provides an overview of the security policies and procedures we have in place for the operation of DNSSEC within the TLD, presented as a summary for purposes of this DNSSEC Practice Statement.

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

The generation of KSK and ZSK is carried out by following the relevant procedure to generate keys of the strength required for the TLD.

Key Pair Generation is an audited event and audit logs are recorded and kept in accordance with relevant policies.

5.1.2 Public Key Delivery

The DS is delivered to the parent Zone using a secure and authenticated system provided by IANA.

The DNSKEY is published in the DNS.

5.1.3 Public Key Parameters Generation and Quality Checking

In accordance with Section 4.2.1, one of our employees carries out the public key generation. Quality of the parameters is examined as part of our standard change control procedures.

5.1.4 Key Usage Purposes

Keys will be used in accordance with the DNSSEC implementation defined in this DNSSEC Practice Statement and other relevant documents such as agreements stated in Section 1.3. The keys are not exported from the signing system in an unencrypted form and are only exported for backup and disaster recovery purposes.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are carried out within the signing system. The private components of keys stored on the signing system are exported in encrypted forms only for backup and disaster recovery purposes.

5.2.1 Cryptographic Module Standards and Controls

Systems used for cryptographic functions must be able to generate acceptable level of randomness.

5.2.2 Private Key (m-of-n) Multi-person Control

Procedures for KSK generation and key signing implement an M-of-N multi-person approach. Out of N authorized persons that can participate in key generation or key signing, at least M need to be present.

5.2.3 Private Key Escrow

Private components of keys used for the Zone are escrowed in an encrypted format in accordance with ICANN specifications.

5.2.4 Private Key Backup

Private components of keys used for the Zone are backed up in an encrypted format in accordance with our backup and disaster recovery policies.

5.2.5 Private Key Storage a Cryptographic Module

Private keys are stored on the signer system and restricted to be only accessible to signing functions.

5.2.6 Private Key Archival

Old keys are archived for a period of seven years in an encrypted form.

5.2.7 Private Key Transfer into or from a Cryptographic Module

There are no circumstances under which a private key would be transferred into the signing systems.

In accordance with Section 4.6 and in consultation with the relevant stakeholders, a private key can be transferred out of these systems. The private key will be transferred to the relevant stakeholder in encrypted form unless specifically requested otherwise by that stakeholder.

5.2.8 Method of Activating a Private Key

Keys are activated during a Key Rollover with the appropriate employee executing the rollover procedure.

5.2.9 Method of Deactivating a Private Key

A private key is deactivated by removing all signatures that deem the key valid and subsequently removing the DNSKEY record from the Zone. In the case of a KSK, the DS is removed from the root Zone. The exact order of this is dependent on the rollover method being used. Rollover methods are detailed further in Section 6.

5.2.10 Method of Destroying a Private Key

We destroy keys by securely removing them from the signing system. However, encrypted backups of the keys are not destroyed but rather archived as described in Section 5.2.3.

The signing system may be de-activated following pre-configured triggers that indicate suspicious activity for example, a reboot of the signing system.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

Public components of keys are archived as part of backups and disaster recovery procedures.

5.3.2 Key Usage Periods

Item	Value
KSK	1 year
ZSK	3 months
Signature Validity Periods	30 days

Note: Keys that have been superseded are not used to sign Resource Records.

5.4 Activation Data

Activation data is securely generated and is protected by a confidentiality agreement between us and stakeholders that hold activation data. Activation data is decommissioned by destroying, invalidating or by using another suitable method applicable to the type of data.

5.5 Computer Security Controls

We limit access to production servers and only authorized staff members from our IT department are allowed privileged access. Access may be extended to other personnel for valid business reasons.

Authentication methods are complimented with network security measures. Passwords are rotated regularly and best practices such as tiered authentication and two factor authentication are implemented where appropriate.

5.6 Network Security Controls

Networks for secure DNSSEC infrastructure are segregated using firewalls. Audit logs are kept for all sensitive DNSSEC operations and archived for investigative purposes should security breaches be suspected or detected. Systems are divided into their applicability (e.g. frontend and backend) and user and application access to them is restricted using appropriate means. Production infrastructure is logically separated from non-production infrastructure to limit access at a network level in accordance with our security policies.

5.7 Time Stamping

Timestamps are used for:

- Audit logs generated manually and automatically; and
- DNSSEC signatures.

We synchronize our timeservers with stratum 2 or 3 timeservers. All manually recorded times are stated in time that is local to the location of record. All automatically recorded times are in UTC.

5.8 Life Cycle Technical Controls

5.8.1 System Development Controls

All software deployed on production systems is maintained in version controlled repositories. We implement rigorous change control systems for production infrastructure.

5.8.2 Security Management Controls

We monitor our system for access, configuration changes, package installs and network connections in addition to other critical metrics that can be used to detect suspicious activities. Detailed audit logs enable us to trace any transaction on our systems and analyze events.

5.8.3 Life Cycle Security Controls

We implement fully redundant signing infrastructure and contracts with hardware manufacturers to provide 4 hour business day turnaround on support.

All production infrastructure and software is thoroughly tested before being deployed. Source code of all software deployed to production systems is authenticated and verified.

6 Zone Signing

6.1 Key Lengths, Key Types and Algorithms

We use a split key signing method. The RSA algorithm with a key length of 2048 bits is used for the KSK and 1280 bits is used for the ZSK.

6.2 Authenticated Denial of Existence

NSEC3 (RFC 5155) is used to provide authenticated denial of existence. The hash algorithm SHA1 is used. Salt values or iterations are not changed.

6.3 Signature Format

Signatures are generated using SHA256 hashes.

6.4 Key Rollover

ZSK rollover is every 3 months.

KSK rollover is every year using Double RRset KSK Rollover Method.

6.5 Signature Lifetime and Re-signing Frequency

Signatures are valid for 30 days. Signatures are automatically regenerated every 7½ days.

6.6 Verification of Resource Records

Validity checks are made against the Zone as part of our standard monitoring process. This includes verifying DNSSEC material.

All Resource Records are validated by the Registry before delivery to be signed and distributed into the Zone File.

6.7 Resource Records Time-to-live

The time-to-live (TTL) for each DNSSEC Resource Record, in seconds, is as follows:

DNSKEY	3600
DS	3600
NSEC3	1800
RRSIG	Same as covered Resource Record

7 Compliance Audit

7.1 Frequency of Entity Compliance Audit

Compliance audits are conducted annually at our sole expense.

7.2 Identity/Qualifications of Auditor

Our compliance audits are performed a qualified entity which is independent from us and the Registry Operator.

7.3 Auditor's Relationship to Audited Party

Compliance audits of our operations are performed by a qualified entity that is independent from us. Third party auditors do not participate in the multi-person control for any tasks, as stated in Section 4.2.1.

7.4 Topics Covered by Audit

The scope of our annual Compliance Audit includes all DNSSEC tasks as stated in Section 4.2.1.

7.5 Actions Taken as a Result of Deficiency

Action items that are raised as a result of compliance audits are presented to management for consideration. Management will investigate and implement corrective actions should they determine them to be necessary.

7.6 Communication Results

A report of the audit results will be provided to authorized personnel no later than thirty (30) days after the audit.

8 Legal Matters

8.1 Fees

Not applicable.

8.2 Financial Responsibility

Not applicable.

8.3 Confidentiality of Business Information

8.3.1 Scope of Confidential Information

The following information is kept confidential and requires privileged access as controlled by our policy:

- Secure DNSSEC information
- Audit logs
- Reports created by auditors
- Procedures
- Policies that relate to security

8.3.2 Types of Information not Considered Confidential

Information that is classified as public as part of the DNSSEC extensions to DNS are considered to be public by us and will not be subject to access restriction.

8.3.3 Responsibility to Protect Confidential Information

We are committed to the confidentiality of information and takes all measures reasonably possible to prevent the compromise of such information.

8.4 Privacy of Personal Information

8.4.1 Information Treated as Private

Not applicable.

8.4.2 Information not Deemed Private

Not applicable.

8.4.3 Responsibility to Protect Private Information

Not applicable.

8.4.4 Disclosure Pursuant to Judicial or Administrative process

We shall be entitled to disclose confidential/private information if we believe that disclosure is necessary in response to judicial, administrative, or other legal processes.

8.5 Limitations of Liability

We, to the extent permitted by law, exclude liability for any losses, direct or indirect, punitive, special, incidental or consequential damage, in connection with or arising out of this DNSSEC Practice Statement or the actions of us or any third party (including for loss of profits, use, data, or other economic advantage), however it arises, and even if we have been previously advised of the possibility of such.

8.6 Term and Termination

8.6.1 Term

This DNSSEC Practice Statement becomes effective upon publication with the most current version being published.

8.6.2 Termination

This DNSSEC Practice Statement will be amended as required and will remain in force until it is replaced by a new version.

8.6.3 Dispute Resolution Provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

With the exception of injunctive or provisional relief, disputes involving us require an initial negotiation period of no less than 60 days prior to the commencement of legal action.

Subject to the foregoing, any legal action in relation to this DNSSEC Practice Statement against any party or its property may be brought in any court of competent jurisdiction in the Commonwealth of Virginia, United States of America and the parties irrevocably, generally and unconditionally submit to the nonexclusive jurisdiction of any court specified in this provision in relation to both itself and its property.

8.6.4 Governing Law

This DNSSEC Practice Statement shall be governed by and construed under the law in the Commonwealth of Virginia, United States of America.

8.6.5 Registry Jurisdiction

The Registry Service Provider operates in the Commonwealth of Virginia, United States of America.

Definitions

We, us and our means any or all of the Neustar Inc. group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Disclaimer

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

Confidentiality Notice

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

Trademarks Notice

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.

Pricing Notice

Any information or pricing provided in this document is subject to change without notice. Whilst we have compiled this document in good faith, based on what we believe is accurate and up-to-date information, it is possible that the pricing or other information contained in this document may require amendment due to changing market or other circumstances (including product discontinuation, manufacturer price changes, errors, or insufficient or inaccurate information having been provided by the recipient of this document or others, and other external circumstances). Additional charges may also apply for work that is out of scope.

The pricing in this document is based on our standard terms and conditions and is valid for a period of thirty (30) days from the date of this document.

DNSSEC Policy for

.TMALL

DNSSEC Practice Statement

26 September 2017

neustar

This document is provided pursuant to the disclaimer provided on the last page.

Contact

Name	Customer Support
Address	Neustar Inc. 21575 Ridgetop Circle Sterling, Virginia, 20166 United States of America
Phone	+1 844 677 2878 +1 571 434 6700
Email	reg@support.neustar

Classification

Public

Definitions

In this document:

DNS means the 'Domain Name System' that is a distributed database and hierarchical global infrastructure deployed on the Internet and private IP-based networks used to resolve domain names into IP addresses.

DNSKEY means the Domain Name System KEY, a Resource Record that contains the cryptographic keys used to sign records in a Zone.

DNSSEC means Domain Name System Security Extensions which are a suite of specifications for securing certain kinds of information provided by the DNS.

End Users means those accessing services supplied on the domain name in the TLD.

EPP means Extensible Provisioning Protocol.

Key Rollover means the process of generating new cryptographic keys and replacing the keys in use.

KSK means the 'Key Signing Key' used to sign DNSKEY records.

Recursive Name Server Providers means providers who provide their customers with name servers to use.

Registrant means a natural or legal person, company or organization in whose name a domain name is assigned in the TLD.

Registrar means an entity that is authorized to offer domain name registration services in relation to the TLD

Registry Operator means the entity that is a party to the Registry Agreement with ICANN for the TLD.

Registry means the systems used to record, store and maintain details of domain names in the TLD.

Registry Service Provider means the technical services provider providing Registry functions to the Registry Operator.

Resource Record means the basic data element in the DNS that define the structure and content of the DNS.

TLD means Top Level Domain and for the purpose of this policy refers to .TMALL

We, **us** and **our** means any or all of the Neustar Inc. group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Zone means a sub-section of the DNS hierarchy for which administrative responsibility has been delegated.

Zone File means a data file which describes a Zone.

ZSK means the 'Zone Signing Key' used to sign records.

Purpose

This document is our DNSSEC Practice Statement for the TLD Zone. It states the considerations that we follow in providing DNSSEC services for the Zone.

Scope

This document covers only that information required to outline the DNSSEC Practices standpoint as it relates to the Zone as required by the DNSSEC Policy & Practice Statement Framework RFC.

Audience

ICANN, Registrars, Registrants and the general public.

Contents

1 Introduction

This document details the practices we use on behalf of the Registry Operator in our capacity as a Registry Service Provider.

This document is our DNSSEC Practice Statement for the TLD. It states the considerations that we follow in providing DNSSEC services for the TLD. The Zone File data, including DNSSEC keys used to sign the Zone File remain the property of the Registry Operator of the TLD.

1.1 Overview

DNSSEC was proposed to add data integrity and authentication to the DNS. The DNSSEC system asserts trustworthiness of data using a chain of public-private keys. For End Users wanting to use DNSSEC enabled name servers, DNSSEC aware resolvers will be necessary to take advantage of the system.

1.2 Document Name and Identification

Document Name	DNSSEC Practice Statement
Version	2.0
Date Created	12 May 2011
Date Modified	23 August 2017

1.3 Community and Applicability

The following stakeholders of this DNSSEC implementation have been identified:

- End Users
- Recursive Name Server Providers
- Registrant
- Registrar
- Registry Operator

Relationship between different entities is regulated through the following agreements:

Relationship	Agreement
Registry Operator and Registry Service Provider	Registry Operator – Registry Service Provider Agreement
Registry Operator and Registrar	Registrar – Registry Agreement
Registry Operator and Registrant	Registrant – Registrar Agreement

1.4 Specification Administration

1.4.1 Specification Administration Organization

Organization	Neustar Inc.
Website	www.registry.neustar

1.4.2 Contact Information

Name	Customer Support
Address	Neustar Inc. 21575 Ridgetop Circle Sterling, Virginia, 20166 United States of America
Phone	+1 844 677 2878 +1 571 434 6700
Email	reg@support.neustar

1.4.3 Specification Change Procedures

Queries with regards to the content of this document may be made directly in writing via email, postal mail or telephone to the contact listed above. Some requests may only be made in writing via email or postal mail and requestors may be notified to do so should they place the initial request via telephone.

We reserve the right to amend the DNSSEC Practice Statement without notification. Updated or new DNSSEC Practice Statements will be published as specified in Section 2.

2 Publication Repositories

2.1 Repositories

This DNSSEC Practice Statement will be published on the Registry Operator's website.

2.2 Publication of Public Keys

Delegation Signing (DS) records of SEP keys are made available by publication in the root Zone. We maintain a website, as described in Section 1.4.1, on which we publish notifications of policy changes specific to DNSSEC, and alerts in the event of an emergency Key Rollover.

2.3 Access Controls on Repositories

Information that the organization deems publically viewable is published on the Registry Operator's website. Other information may be requested by writing to the contact specified in Section 1.4.2. Provision of requested information is at our sole discretion.

This document may refer to documents that are confidential in nature, or considered for our internal use. These documents may be made available on request after consideration on a case by case basis. We reserve the right to deny access to confidential documents or documents classified for internal use only.

We will take all the necessary measures to protect information and material that is of a secure nature with respect to DNSSEC. These measures will be commensurate with the nature of such information and material being secured.

3 Operational Requirements

3.1 Meaning of Domain Names

Restrictions and policy of naming of child Zones is determined by the appropriate policy in place governing the TLD.

3.2 Identification and Authentication of Child Zone Manager

We do not conduct any identification or authentication of the child Zone manager. This is the responsibility of the Registrar of Record.

3.3 Registration of Delegation Signing (DS) Resource Records

The chain-of-trust to the child Zone is established by publishing a signed DS record into the Zone.

The submission of a DS record is carried out by the Registrar of Record using the Registry interface, that is, the EPP service.

We will sign the DS record using the Zone's ZSK(s) and publish the resulting signature along with the DS record to build the chain-of-trust.

3.4 Method to Prove Possession of Private Key

Registrars are mandated by agreements they are subject to, as specified in Section 1.3, to authenticate Registrants before accepting any changes from the Registrant that they may choose to submit to the Registry.

The need for Registrants to explicitly prove the possession of a private key is invalidated due to workings of DNSSEC, as the Registrant submits a DS record using interfaces provided by the Registrar. A chain of trust is established when the Registrant signs their Zone using the private key corresponding to the DS submitted.

In the case where the Registrant does not possess the private component corresponding to the DS, they will not be able to create valid signatures for records in their Zone and the chain of trust culminating at their records will be invalidated.

3.5 Removal of DS Resource Record

The Registrar of Record uses the Registry interface to remove the DS record.

We may remove a DS record and re-delegate the child-Zone in consultation with the Registry Operator, Registrar and Registrant if it is deemed that the child Zone has been compromised. Such a removal may be initiated by the Registry Operator, Registrar, Registrant or us.

4 Facility, Management and Operational Controls

4.1 Physical Controls

4.1.1 Site Location and Construction

The Registry architecture consists of a primary site, a secondary site, and geographically dispersed DNS sites. The components at the secondary site are identical to those at the primary site.

We choose data centers for Registry operations after carrying out stringent checks and visits on a large number of available providers. Each data center provides the following minimum set of requirements:

- Redundant Power Feeds
- Un-interruptible Power Supply (minimum 30 minutes)
- Backup Power Source (generator)
- Fire Detection System (High Sensitivity Smoke Detectors)
- Fire Suppression System
- Water Detection System
- Multiple (Diverse) Internet Links
- Stringent Physical Security (On-site security personnel, bio-metric access control)
- 24/7 Access Availability
- Robust Cooling System (HVAC)
- Real Time/Pro-active Power and Environmental Monitoring

4.1.2 Physical Access

Access to all Registry systems at each data center is restricted. Equipment is located in private locked racks and keys to these are only given out to authorized administrators as part of stringent data center security procedures.

Remote environment surveillance is employed, including cameras and entry alarms.

In addition, direct physical access to equipment is monitored and controlled as an un-trusted interface, login sessions are not permitted to idle for long periods, and network port security is employed to minimize the opportunity for a direct network connection to be used as a security threat vector.

4.1.3 Power and Air Conditioning

N+1 power is utilized at all selected Registry data centers to maximize uptime availability. Uninterruptible Power Supply (UPS) systems are used to prevent power spikes, surges, and brownouts, and redundant backup diesel generators provide additional runtime. Alerts are set on all power provision systems to allow us to begin failover preparation in the event of a potential power provision issue to ensure a smooth and controlled failover if required.

Similarly N+1 monitored air conditioning at Registry data centers is configured to provide maximum temperature control for the installed equipment in order to provide a stable operating environment.

4.1.4 Water Exposures

We have implemented reasonable measures for flood detection and protection at its sites, as well as having a key selection criterion for Registry and DNS sites that they be in areas which are not likely to suffer flooding.

4.1.5 Fire Prevention and Protection

Fire protection in each data centre is world-class, with very early smoke detection apparatus installed and set as one element of a multi-stage, human controlled multi-zone dry-pipe, double-interlock, pre-action fire suppression system in a configuration that complies with local regulations and industry best practice.

4.1.6 Media Storage

Sensitive media is stored offsite securely and is protected by access restrictions. Such media is reasonably protected from fire, water and other disastrous environmental elements.

4.1.7 Waste Disposal

Sensitive documents are shredded before disposal. Where sensitive data is stored electronically, appropriate means are used to render the data unsalvageable prior to disposal.

4.1.8 Off-site Backup

DNSSEC components and necessary data are stored off-site regularly as part of backup and disaster recovery. Such data is protected by reasonably secure means and has access restrictions that are similar to those implemented for online systems and data.

4.2 Procedural controls

4.2.1 Trusted Roles

The following table presents all procedures that we have implemented for providing DNSSEC services for the TLD. These procedures require corresponding roles as below:

Procedure	Roles
Key Rollover	▪ System Administrator ▪ Security Officer
Key Creation	▪ System Administrator ▪ Security Officer
Disposal of old Key	▪ System Administrator ▪ Security Officer
KSK Rollover	▪ System Administrator ▪ Security Officer

4.2.2 Number of Persons Required Per Task

The number of persons required varies per task or procedure. Please refer to Section 4.2.1 for further information.

4.2.3 Identification and Authentication for Each Role

We require all personnel dealing with secure DNSSEC material and systems to have completed security checks. We reserve the right to interpret the findings of the security check equitably with respect to the secure nature of this DNSSEC implementation as covered by our Human Resources policy.

4.2.4 Tasks Requiring Separation of Duties

Tasks that are part of a Key Rollover require separation of duties. Please refer to Section 4.2.1 for further information.

4.3 Personnel Controls

4.3.1 Qualifications, Experience and Clearance Requirements

Each person who fulfils a DNSSEC role must:

- Be employed full time by us;
- Not be within their initial employment probation period; and
- Have completed a security check.

4.3.2 Background Check Procedures

A security check must be completed prior to taking part in DNSSEC tasks.

4.3.3 Training Requirements

Each person who is responsible for DNSSEC tasks must have attended our DNSSEC training session and be fully qualified to perform that function.

We provide frequent retraining to our employees to assist them with keeping their skills current and enabling them to perform their job proficiently.

4.3.4 Job Rotation Frequency and Sequence

We rotate the responsibility for DNSSEC related tasks between staff that satisfy the skill set required to execute those tasks.

4.3.5 Sanctions for Unauthorized Actions

We will conduct investigations where we detect or are made aware of unauthorized actions on the DNSSEC environment. We will take necessary disciplinary action should such action be warranted.

4.3.6 Contracting Personnel Requirements

Contractors and consultants are not authorized to participate in secure DNSSEC tasks.

4.3.7 Documentation Supplied to Personnel

We provide requisite training and support material to our employees to enable them to proficiently perform their duties. Supplied documentation is provided to staff under security controlled guidelines to ensure operational security.

4.4 Audit Logging Procedures

All systems deployed utilize audit log functionality which is coordinated centrally. Logging is used to monitor the health of systems, trace any issues and conduct diagnosis.

4.4.1 Types of Events Recorded

A high level categorization of events that are recorded is as follows:

Zone File Activity	Addition and removal of domain names. Changes in Resource Records associated with domain names in the TLD.
Hardware Failures	Failure of server and network infrastructure or their components.
Access To Hardware	Changes in access controls granting physical, console and network access to infrastructure.
Security Profile	Changes in settings and configuration that determine the security of infrastructure or the services it provides.
System Updates	Updates to operating environment and packages on servers and firmware on network appliances.
Network Activity	Divergences from observed patterns of network activities.
Redundancy Failure	Failure in backups, Disaster Recovery or transitions between primary and secondary site.
Incident Management	Incidents being raised, allocated, acted upon and resolved.
Failure In Event Monitoring	Failure of event monitoring system. This would be detected using a secondary event monitoring system.

4.4.2 Frequency of Processing Log

Audit logs and event monitoring feed into our monitoring system that raises alerts based on states that are not normal in regular operations.

4.4.3 Retention Period for Audit Log Information

Audit log information is securely archived for a period of 7 years.

4.4.4 Protection of Audit Log

Audit logs are only available to our staff with appropriate privileges. Audit logs do not contain private keys or other sensitive information that may lead to a compromise by using existing and known methods.

4.4.5 Audit Log Backup Procedures

Audit logs are backed up as part of the backup procedures in place for production systems. Those logs containing sensitive data are stored in a secure manner. Disposal of audit logs is carried out in accordance with Section 4.1.7.

4.4.6 Audit Collection System

In addition to information recorded manually by staff while conducting operations, Audit information is collected in Audit logs automatically. Methods specific to applications and operating environments are used to record audit logs.

Manual logs are scanned and the original documents archived in a fireproof safe.

4.4.7 Notification to Event-causing Subject

No notification is issued to the event-causing subject as part of automatic event logging. However, selected events are monitored and alerts delivered to our employees that may choose to notify event-causing subjects.

During execution of manual procedures the participants are informed that logging is taking place.

4.4.8 Vulnerability Assessments

We engage an external entity to perform a vulnerability audit annually. This is in addition to monitoring and analysis that is in place for production systems. A broader annual compliance audit is also performed as discussed in Section **Error! Reference source not found.**.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and Compromise Handling Procedures

Any event that may cause or has caused an outage, damage to the Registry, or disruption to service is classified as an incident. Any event that is an incident and has resulted in exposure of private DNSSEC components is classified as a compromise. Incidents are addressed using our incident management procedures.

Should we detect or be notified of a compromise, we will conduct an investigation in order to determine the nature and seriousness of the compromise. Following the investigation we will take the necessary measures to re-instate a secure state. This may involve rolling over the ZSK(s), KSK(s) or both.

Incident management is conducted in accordance with our Incident Management Process.

4.5.2 Corrupted Computing Resources, Software and/or Data

Detection or notification of corrupted computing resources will be responded to with appropriate incident management procedures and escalation procedures as necessary.

4.5.3 Entity Private Key Compromise Procedures

An emergency ZSK and KSK rollover will be carried out in the event that we detect or are notified of a private key compromise of either key. On suspicion of a compromise, we will instigate an investigation to determine the validity of such suspicions. We will notify the public through an update that will be published in accordance with Section 2.2.

4.5.4 Business Continuity and IT Disaster Recovery Capabilities

Business continuity planning and disaster recovery for DNSSEC is carried out in accordance with our Business Continuity and Disaster Recovery Policies, and contracts in place with the Registry Operator.

4.6 Entity Termination

We will ensure that should our responsibilities to manage DNS for the TLD be terminated, we will co-ordinate with all required parties in order to execute a transition.

Should it be decided to return the TLD to an unsigned position, we will endeavor to carry it out in an orderly manner.

5 Technical Security Controls

This section provides an overview of the security policies and procedures we have in place for the operation of DNSSEC within the TLD, presented as a summary for purposes of this DNSSEC Practice Statement.

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

The generation of KSK and ZSK is carried out by following the relevant procedure to generate keys of the strength required for the TLD.

Key Pair Generation is an audited event and audit logs are recorded and kept in accordance with relevant policies.

5.1.2 Public Key Delivery

The DS is delivered to the parent Zone using a secure and authenticated system provided by IANA.

The DNSKEY is published in the DNS.

5.1.3 Public Key Parameters Generation and Quality Checking

In accordance with Section 4.2.1, one of our employees carries out the public key generation. Quality of the parameters is examined as part of our standard change control procedures.

5.1.4 Key Usage Purposes

Keys will be used in accordance with the DNSSEC implementation defined in this DNSSEC Practice Statement and other relevant documents such as agreements stated in Section 1.3. The keys are not exported from the signing system in an unencrypted form and are only exported for backup and disaster recovery purposes.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are carried out within the signing system. The private components of keys stored on the signing system are exported in encrypted forms only for backup and disaster recovery purposes.

5.2.1 Cryptographic Module Standards and Controls

Systems used for cryptographic functions must be able to generate acceptable level of randomness.

5.2.2 Private Key (m-of-n) Multi-person Control

Procedures for KSK generation and key signing implement an M-of-N multi-person approach. Out of N authorized persons that can participate in key generation or key signing, at least M need to be present.

5.2.3 Private Key Escrow

Private components of keys used for the Zone are escrowed in an encrypted format in accordance with ICANN specifications.

5.2.4 Private Key Backup

Private components of keys used for the Zone are backed up in an encrypted format in accordance with our backup and disaster recovery policies.

5.2.5 Private Key Storage a Cryptographic Module

Private keys are stored on the signer system and restricted to be only accessible to signing functions.

5.2.6 Private Key Archival

Old keys are archived for a period of seven years in an encrypted form.

5.2.7 Private Key Transfer into or from a Cryptographic Module

There are no circumstances under which a private key would be transferred into the signing systems.

In accordance with Section 4.6 and in consultation with the relevant stakeholders, a private key can be transferred out of these systems. The private key will be transferred to the relevant stakeholder in encrypted form unless specifically requested otherwise by that stakeholder.

5.2.8 Method of Activating a Private Key

Keys are activated during a Key Rollover with the appropriate employee executing the rollover procedure.

5.2.9 Method of Deactivating a Private Key

A private key is deactivated by removing all signatures that deem the key valid and subsequently removing the DNSKEY record from the Zone. In the case of a KSK, the DS is removed from the root Zone. The exact order of this is dependent on the rollover method being used. Rollover methods are detailed further in Section 6.

5.2.10 Method of Destroying a Private Key

We destroy keys by securely removing them from the signing system. However, encrypted backups of the keys are not destroyed but rather archived as described in Section 5.2.3.

The signing system may be de-activated following pre-configured triggers that indicate suspicious activity for example, a reboot of the signing system.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

Public components of keys are archived as part of backups and disaster recovery procedures.

5.3.2 Key Usage Periods

Item	Value
KSK	1 year
ZSK	3 months
Signature Validity Periods	30 days

Note: Keys that have been superseded are not used to sign Resource Records.

5.4 Activation Data

Activation data is securely generated and is protected by a confidentiality agreement between us and stakeholders that hold activation data. Activation data is decommissioned by destroying, invalidating or by using another suitable method applicable to the type of data.

5.5 Computer Security Controls

We limit access to production servers and only authorized staff members from our IT department are allowed privileged access. Access may be extended to other personnel for valid business reasons.

Authentication methods are complimented with network security measures. Passwords are rotated regularly and best practices such as tiered authentication and two factor authentication are implemented where appropriate.

5.6 Network Security Controls

Networks for secure DNSSEC infrastructure are segregated using firewalls. Audit logs are kept for all sensitive DNSSEC operations and archived for investigative purposes should security breaches be suspected or detected. Systems are divided into their applicability (e.g. frontend and backend) and user and application access to them is restricted using appropriate means. Production infrastructure is logically separated from non-production infrastructure to limit access at a network level in accordance with our security policies.

5.7 Time Stamping

Timestamps are used for:

- Audit logs generated manually and automatically; and
- DNSSEC signatures.

We synchronize our timeservers with stratum 2 or 3 timeservers. All manually recorded times are stated in time that is local to the location of record. All automatically recorded times are in UTC.

5.8 Life Cycle Technical Controls

5.8.1 System Development Controls

All software deployed on production systems is maintained in version controlled repositories. We implement rigorous change control systems for production infrastructure.

5.8.2 Security Management Controls

We monitor our system for access, configuration changes, package installs and network connections in addition to other critical metrics that can be used to detect suspicious activities. Detailed audit logs enable us to trace any transaction on our systems and analyze events.

5.8.3 Life Cycle Security Controls

We implement fully redundant signing infrastructure and contracts with hardware manufacturers to provide 4 hour business day turnaround on support.

All production infrastructure and software is thoroughly tested before being deployed. Source code of all software deployed to production systems is authenticated and verified.

6 Zone Signing

6.1 Key Lengths, Key Types and Algorithms

We use a split key signing method. The RSA algorithm with a key length of 2048 bits is used for the KSK and 1280 bits is used for the ZSK.

6.2 Authenticated Denial of Existence

NSEC3 (RFC 5155) is used to provide authenticated denial of existence. The hash algorithm SHA1 is used. Salt values or iterations are not changed.

6.3 Signature Format

Signatures are generated using SHA256 hashes.

6.4 Key Rollover

ZSK rollover is every 3 months.

KSK rollover is every year using Double RRset KSK Rollover Method.

6.5 Signature Lifetime and Re-signing Frequency

Signatures are valid for 30 days. Signatures are automatically regenerated every 7½ days.

6.6 Verification of Resource Records

Validity checks are made against the Zone as part of our standard monitoring process. This includes verifying DNSSEC material.

All Resource Records are validated by the Registry before delivery to be signed and distributed into the Zone File.

6.7 Resource Records Time-to-live

The time-to-live (TTL) for each DNSSEC Resource Record, in seconds, is as follows:

DNSKEY	3600
DS	3600
NSEC3	1800
RRSIG	Same as covered Resource Record

7 Compliance Audit

7.1 Frequency of Entity Compliance Audit

Compliance audits are conducted annually at our sole expense.

7.2 Identity/Qualifications of Auditor

Our compliance audits are performed a qualified entity which is independent from us and the Registry Operator.

7.3 Auditor's Relationship to Audited Party

Compliance audits of our operations are performed by a qualified entity that is independent from us. Third party auditors do not participate in the multi-person control for any tasks, as stated in Section 4.2.1.

7.4 Topics Covered by Audit

The scope of our annual Compliance Audit includes all DNSSEC tasks as stated in Section 4.2.1.

7.5 Actions Taken as a Result of Deficiency

Action items that are raised as a result of compliance audits are presented to management for consideration. Management will investigate and implement corrective actions should they determine them to be necessary.

7.6 Communication Results

A report of the audit results will be provided to authorized personnel no later than thirty (30) days after the audit.

8 Legal Matters

8.1 Fees

Not applicable.

8.2 Financial Responsibility

Not applicable.

8.3 Confidentiality of Business Information

8.3.1 Scope of Confidential Information

The following information is kept confidential and requires privileged access as controlled by our policy:

- Secure DNSSEC information
- Audit logs
- Reports created by auditors
- Procedures
- Policies that relate to security

8.3.2 Types of Information not Considered Confidential

Information that is classified as public as part of the DNSSEC extensions to DNS are considered to be public by us and will not be subject to access restriction.

8.3.3 Responsibility to Protect Confidential Information

We are committed to the confidentiality of information and takes all measures reasonably possible to prevent the compromise of such information.

8.4 Privacy of Personal Information

8.4.1 Information Treated as Private

Not applicable.

8.4.2 Information not Deemed Private

Not applicable.

8.4.3 Responsibility to Protect Private Information

Not applicable.

8.4.4 Disclosure Pursuant to Judicial or Administrative process

We shall be entitled to disclose confidential/private information if we believe that disclosure is necessary in response to judicial, administrative, or other legal processes.

8.5 Limitations of Liability

We, to the extent permitted by law, exclude liability for any losses, direct or indirect, punitive, special, incidental or consequential damage, in connection with or arising out of this DNSSEC Practice Statement or the actions of us or any third party (including for loss of profits, use, data, or other economic advantage), however it arises, and even if we have been previously advised of the possibility of such.

8.6 Term and Termination

8.6.1 Term

This DNSSEC Practice Statement becomes effective upon publication with the most current version being published.

8.6.2 Termination

This DNSSEC Practice Statement will be amended as required and will remain in force until it is replaced by a new version.

8.6.3 Dispute Resolution Provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

With the exception of injunctive or provisional relief, disputes involving us require an initial negotiation period of no less than 60 days prior to the commencement of legal action.

Subject to the foregoing, any legal action in relation to this DNSSEC Practice Statement against any party or its property may be brought in any court of competent jurisdiction in the Commonwealth of Virginia, United States of America and the parties irrevocably, generally and unconditionally submit to the nonexclusive jurisdiction of any court specified in this provision in relation to both itself and its property.

8.6.4 Governing Law

This DNSSEC Practice Statement shall be governed by and construed under the law in the Commonwealth of Virginia, United States of America.

8.6.5 Registry Jurisdiction

The Registry Service Provider operates in the Commonwealth of Virginia, United States of America.

Definitions

We, us and our means any or all of the Neustar Inc. group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Disclaimer

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

Confidentiality Notice

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

Trademarks Notice

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.

Pricing Notice

Any information or pricing provided in this document is subject to change without notice. Whilst we have compiled this document in good faith, based on what we believe is accurate and up-to-date information, it is possible that the pricing or other information contained in this document may require amendment due to changing market or other circumstances (including product discontinuation, manufacturer price changes, errors, or insufficient or inaccurate information having been provided by the recipient of this document or others, and other external circumstances). Additional charges may also apply for work that is out of scope.

The pricing in this document is based on our standard terms and conditions and is valid for a period of thirty (30) days from the date of this document.