Afilias / Donuts DNSSEC Practice Statement (DPS)
Version 1.10 2021-10-26

1. INTRODUCTION

1.1. Overview

This document was created using the template provided under the current practicing documentation.[1] Henceforth in this document, the "Company" shall refer to Donuts Inc., as well as Afilias, Inc. Afilias Limited, and Afilias Canada Corporation, and their subsidiaries. This document comprises the practices utilized by the Company 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 the Company's auspice that have been signed.

1.2. Document name and identification

Afilias /Donuts DNSSEC Practice Statement (DPS) Version 1.10

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

The Company 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 Registry Service Provider (RSP), where the Company operates and performs the functions of maintaining the zone, on behalf of another entity (which acts as the RO). In the case where the Company is the RO for a zone, the Company is also acting as the RSP.

The Registry is expected to perform the following functions:
- Generate the Key Signing Keys (KSK) for the zone. Alternatively, the RO may generate their own KSKs.
- Generate the Zone Signing Keys (ZSK) for the zone. If the RO generates their own KSK, then the Company is also expected to generate Key Signing Requests (KSRS) and receive Signed Key Responses (SKRs) to and from the RO, respectively. Materials received from within the SKR are loaded and used as appropriate.
- Sign the apex DNSKEY RRSet 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 a Company 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 the Company 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 the Company).

1.4. Specification Administration

[1] Definitions for many of the terms used in this document are defined in Section 2 of RFC 6841.

1.4.1. Specification administration organization
The Company maintains this specification.

1.4.2. Contact Information
Questions or concerns regarding this DPS, or the operation of a signed TLD should be sent to the Company Customer Support Center.
They can be reached via:
Phone: +1 (425) 298-2200
Email: support@donuts.email

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 https://donuts.domains/dps
Only the Company Operations department has the ability to update the contents of the website. ACLs on the file are Read-Only.

2.2. Publication of public keys
The Company generates DS-record data for zones that fall under the Company's control, either through direct contractual delegation by ICANN, or via contract with a Registry Operator using the Company to provide DNS services. Key Signing Keys (KSKs) are signed with the Secure Entry Point (SEP) bit set. As soon as possible, the Company sends DS-record data pertaining to these KSKs for signed TLD zones to ICANN for publication in the root. No other trust anchors or repositories are used.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names
Generally, domain names are defined in Section 2 of RFC 8499.[2]
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 the Company 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

[2] https://datatracker.ietf.org/doc/html/rfc8499

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 the Company. 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. The Company therefore does not perform any tests to prove possession of a private key.

3.5. Removal of DS resource records

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

The Company uses four 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).

All 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 the Company's systems.

Media with sensitive information is stored within the Company's 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.

The Company 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

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

The Company 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 a Company employee in a comparable position.

The Company 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.

The Company monitors all log entries for alerts based on irregularities and incidents. The Company 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, the Company's 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.

The Company 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

The Company has adopted a DNSSEC termination plan in the event that the roles and responsibilities of the signing services must transition to other entities. The Company 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 2 or higher. 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.

When the RO maintains the KSK offline, ZSKs are installed only after they have been signed via a KSR / SKR transaction with the RO. Only ZSKs and the DNSKEY signatures within the current timeframe are active.

5.2. Private key protection and Cryptographic Module Engineering Controls
All signing modules are FIPS 140-2 level 2 certified or higher. 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. Other Aspects of Key Pair Management

5.3.1. Public key archival
Obsolete public keys are not archived.

5.3.2. Key Usage Periods
Zone Signing Keys (ZSKs) are used in production for approximately one month before being rolled. Key Signing Keys (KSKs) are rolled based on RO policy, but are expected to change at least every five years.

5.4. Activation Data
Activation data is a set of passwords corresponding to user accounts with key-generation privileges. The passwords are “split” to ensure that no single operator can perform these operations.

5.5. Computer Security Controls
The Company ensures that the systems maintaining key software and data files are trustworthy systems secure from unauthorized access. In addition, the Company 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.

5.6. Network Security Controls
The signing systems are placed in the Company’s 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.

5.7. Timestamping
The signer systems securely synchronize their system clocks with a trusted time source inside the Company’s network.

5.8. Life Cycle Technical Controls
Applications developed and implemented by the Company 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. The Company also 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, Key Types and algorithms

6.1.1. Key Signing Key

The Company uses a key length of at least 2048 bits with Algorithm 8[3] as the generation algorithm.

6.1.2. Zone Signing Key

The Company uses a key length of at least 1024 bits with Algorithm 8 as the generation algorithm.

6.2. Authenticated denial of existence

Authenticated denial of existence is provided through the use of NSEC3 records as specified in RFC 5155[4]

6.3. Signature format

SHA-256, using RSA

6.4. Key Rollover

6.4.1. Zone signing key roll-over

The Company rolls the ZSK with a pre-publishing scheme as described in RFC 4641[5], section 4.2.1.1. ZSK roll-over is carried out once a month.

6.4.2. Key signing key roll-over

The Company rolls the KSK with a double-DS scheme, as described in RFC 4641, section 4.2.1.2. There are no planned KSK rollover frequencies defined at this time.

6.5. 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.

6.6. Verification of resource records

All RRset signatures are verified prior to publication.

6.6.1. 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.

6.7. Resource records time-to-live

DNSKey	1 day (86400s)
NSEC3	SOA minimum (1 day)
Delegation Signer (DS)	1 day
RRSIG	varies depending on the RR covered

7. COMPLIANCE AUDIT

[3] As defined in https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

[4] https://datatracker.ietf.org/doc/html/rfc5155

[5] https://datatracker.ietf.org/doc/html/rfc4641

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 is an entity who is proficient in the technologies they are auditing.

7.3. Auditor's relationship to audited party
Auditors are independent of the Company.

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
The Company will communicate internally to resolve any gaps designated by the action map. Should deficiencies be found in this document, it will be augmented to mitigate the issue, and posted with a new revision number.

8. LEGAL MATTERS
This DPS is to be construed in accordance with and governed by the internal laws of the United States 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 the United States.

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 has no legal responsibility for any procedure or function within this DPS. The Company 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@donuts.email.