DNSSEC Practice Statement

1. Introduction

1.1. Overview

Background: This document describes DNSGuru's practices for DNSSEC operations and management.

Purpose: To provide a clear understanding of how DNSGuru manages and operates DNSSEC for its zones.

1.2. Document and Identification

Document Name: DNSGuru DNSSEC Practice Statement
Version: 1.0
Date: 2023-08-28

1.3. Community and Applicability

DNSGuru: DNSGuru (a division of Kiwazo CommV) provides Enterprise DNS services. DNSGuru will host own zones and customer zones using a network of DNS services. This policy applies to DNSGuru managed zones.

Customers: Enterprise or MSP customers such as ISPs, hosting providers or service companies. These Customers typically manage their own zones, but outsource distribution, analytics and other services to DNSGuru. Customers can (as part of the services) ask DNSGuru to sign the zone. This policy only applies to Customer zones if they opt-in to this signing service.

1.4. Specification Administration

Specification administration organization: DNSGuru maintains this specification and will review it periodically.

Questions or concerns regarding this DPS, or the operation of a signed zone should be sent to the DNSGuru Customer Support Center. They can be reached via email at support@dnsguru.cloud.

Any changes to this document need to be signed off by the CTO of DNSGuru.

The most recent version of this DPS will be published on the website of DNSGuru.

2. Publication and Repositories

2.1. Repositories

DNSGuru manages the DPS repositories and its availability mechanisms, publishes the DPS at its website.

2.2. Publication of signing keys

The public portion of the signing keys are published in the form of DS-Records directly in the relevant upstream zones.

3. Operational Requirements

Policies regarding restrictions on domain names within a given zone are specified by the registry operator, and vary from TLD to TLD. For Customer owned domains names, customer should make sure these requirements are met.

For domains for which the Customer has opted-in to the DNSGuru DNSSEC signing service, DNSGuru will communicate the relevant DS resource records. Customer is responsible for the communication of those resource records to the relevant registrar or registry, including removal of the resources when needed.

4. Facility, Management, and Operational Security Controls

Physical Facility controls: as all nameserver and DNS management nodes are hosted by various public cloud providers, the facility controls are carved out for this policy.

When selecting the infrastructure providers, the security controls they have implemented are part of the assessment.

DNSGuru follows the KINDNS.org Guidelines for Critical Operators and SLD Operators, and the KINDNS.org system hardening practices.

4.1. KINDNS Practices for TLDs and Critical Zones

The generated keys are used for one zone only, and consist of either a ZSK/KSK key pair, or a single Combined Signing Key (CSK). Documented procedures exist for the generation, rotation and lifecycle management of the keys.

Access to zone transfer is limited using NSEC3 and ACLs to restrict zone transfers to replica servers only.

Zone file integrity is controlled to avoid unexpected modifications.

Authoritative and recursive DNS service do not coexist on the same DNS server.

At least two distinct nameservers are used for any given zone.

There is diversity in the authoritative operations to promote resilience.

Monitoring of the services, servers, and network equipment that make up your DNS infrastructure is implemented.

4.2. KINDNS Practices Platform Hardening

ACLs are implemented to restrict network traffic to your DNS servers.

BCP38/MANRS egress filtering is implemented so that no network traffic can leave our platform with a source IP address that is not assigned to the platform.

The configuration of each DNS server is be locked down. This includes the following:

- All services and software packages that are not required for offering DNS service on the system are uninstalled or disabled.
- Hosts running DNS services run only DNS software. In other words, DNS servers do not run other services, such as web or email servers.
- All relevant logging channels and levels for the DNS subsystem are be enabled. Logs are sent to a central location for archiving, inspection, and auditing, and they are retained for a reasonable time in accordance with retention policies.

User permissions and application access to system resources are limited. File permissions and ownership restrictions are set so that users and services not directly associated with management of the

DNS subsystem do not have read or write access to DNS service configuration, data files, and database subsystems.

System and service configuration files are versioned. For authoritative operators, zone files/data are also versioned.

Access to management services (e.g., SSH, web-based configuration tools) are restricted. All services not needed for DNS or management are disabled or uninstalled if possible, otherwise network access to the unnecessary services is blocked.

Access to the system console is secured using cryptographic keys, protected with a passphrase (e.g. SSH keys) or using suitable two-factor authentication (OTP generator or token-based).

Credentials for customer access (registrants and other domain contacts) follow sound credential management practices, including offering two-factor authentication as an option.

5. Zone Signing

The ECDSA algorithm with a key length of 256 bits is used for generating keys.

DNSGuru uses NSEC3 without Opt-OUT and follows the Guidance for NSEC3 Parameter Settings (RFC9276).

If a split ZSK/KSK is used, the expected lifetime of the ZSK is maximum 100 days and a KSK rollover will be performed as needed.

If a single CSK is used, a CSK rollover will be performed as needed.

The RRSIG validity period is 3 weeks. This period starts at most a week in the past and continues at least a week into the future. At all times,

only one RRSIG per signed RRSet per ZSK is served when responding to clients.