# Gap Inc. DNS Practice Statement for the .GAP Zone

**Version 0.1**

# Table of contents

# 1 INTRODUCTION

This document, "DNSSEC Practice Statement for the .GAP Zone" (DPS) describes Gap Inc.'s policies and practices with regard to the DNSSEC operations of the .GAP zone.

## 1.1 Overview

The purpose of DPS is to provide operational information related to DNSSEC for the .GAP zone managed by Gap Inc.. The document follows the DPS framework proposed by the IETF Domain Name System Operations (DNSOP) Working Group.

## 1.2 Document Name and Identification

DNSSEC Practice Statement for the .GAP Zone (.GAP DPS)
Version: 0.1
Available on: XXXXXX
Effective on: YYYYYY

## 1.3 Community and Applicability

The stakeholders with their expected roles and responsibilities regarding .GAP DNSSEC Service are described below.

### 1.3.1 Zone Manager

Gap Inc. is the .GAP zone manager

### 1.3.2 Zone Administrator

Neustar is the .GAP zone administrator.

### 1.3.3 Server Operators

Neustar is the only server operator.

### 1.3.4 Registry

Gap Inc. is Registry Operator of .GAP domain name registrations. As part of the DNS services, Gap Inc. provides DNSSEC services to its registrars who in turn provide these services to their registrants. The registry signs the zone using a combination of ZSK and KSK keys. DS record(s) of the KSK keys are registered and available in the root zone which then enables DNSSEC enabled resolver to maintain a chain of trust between the root and the .GAP registry.

### 1.3.5 Registrar

The Registry provides services for registrars of .GAP domain name registration system. Registrars have contractual business relationships with the Registry to register and maintain domains for their registrants. Registrars provision domain information including DS records in the .GAP zone.

### 1.3.6 Registrant

The Registrant is the owner of the .GAP domain registered in the Registry through a .GAP Registrar. A Registrar or a DNS provider selected by the Registrant is responsible for providing DS records for the registered domain. Through the submission of these records to the Registry, a chain of trust from the Registry to the Registrant's authority subzone can be established.

### 1.3.7 .GAP Zone Key Signing Key Operator

Neustar is the .GAP Zone Key Signing Key Operator. Neustar is responsible for generating the .GAP Zone's Key Signing Key (KSK) and signing the .GAP Keyset use the KSK. They are also responsible for securely generating and storing the private keys and distributing the public portion of the KSK.

### 1.3.8 Root Zone Zone Signing Key Operator

Neustar is the the.GAP Zone Zone Signing Key Operator. Neustar is responsible for performing the function of generating the .GAP Zone's Zone Signing Key (ZSK) and signing the .GAP Zone File using the ZSK.

### 1.3.9 Relying party

Relying parties include DNS resolvers e.g., the browsers or hosts which resolve names in the zone, DNS providers, ISPs, and any user that uses or replies upon .GAP DNSSEC services for the secure resolution of a name using the DNSSEC protocol.

## 1.4 Specification Administration

### 1.4.1 Specification administration organization

The administrator of .GAP DPS is Gap Inc..

### 1.4.2 Contact information

Gap Inc.
2 Folsom Street
San Francisco, CA 94105
USA
415-427-0100

#### 1.4.3 Specification change procedures

Contents of the DPS are reviewed annually, or more frequently as needed. Amendments are made in the existingdocument or published as a new document. All amendments will be made available in the repository described below. Gap Inc. reserves the right to publish amendments with no notice.

# 2 PUBLICATION AND REPOSITORIES

## 2.1 DPS Repository

The DPS is published in a repository located on Gap Inc.'s website. The URL is to be determined.

## 2.2 Publication of Key Signing Keys

KSKs are published in the root zone. The chain of trust can be achieved using the root keys as trust anchors.

## 2.3 Access Controls on Repositories

The DPS is publicly available for all to access and read in the DPS repository. All change requests must be submitted to Gap Inc. for review. Controls have been implemented to prevent unauthorized changes to the DPS.

# 3 OPERATIONAL REQUIREMENTS

## 3.1 Meaning of Domain Names

Domain names are available for the public to register. In some cases, the registry reserves the right to delete or deny a registration if it violates certain policies.

## 3.2 Activation of DNSSEC for Child Zone

Chain of trust from the .GAP zone to the Child Zone is established when the signed DS records of the Child Zone have been published in the .GAP zone. After the chain of trust is established, the Child Zone is DNSSEC activated.

## 3.3 Identification and Authentication of Child Zone Manager

The registry has no direct relationship with the Child Zone Manager and therefore does not identify and authenticate the Child Zone Manager.

## 3.4 Registration of Delegation Signer (DS) Records

Registrars connect to the registry to provision and manage domain registration data, including DS records, on behalf of their registrants..

## 3.5 Method to Prove Possession of Private Key

The Registry does not validate the possession of the private key at the child authoritative zone.

## 3.6 Removal of DS Record

A Registrar can at any time request the removal of the DS record for a domain that Registrar manages. Upon receipt of a valid request from the Registrar, the Registry will remove the DS from the zone

# 4 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

## 4.1 Physical Controls

The .GAP Registry is housed in data center facilities which meet or exceed all of the environmental specifications expected of a mission critical platform.

### 4.1.1 Site Location and Construction

The .GAP Registry and DNSSEC services are operated from multiple, fully redundant data centers in Sterling, Virginia and Charlotte, North Carolina USA. The facility locations provide diverse network connectivity and appropriate network capacity necessary to effectively operate all aspects of the Registry and protect against natural and man-made disasters. In both data centers, cryptographic keys are stored in a FIPS 140-2 Level 3 Hardware Security Module (HSM).

### 4.1.2 Physical access

Neustar operates out of highly secure data centers to provide the highest levels of security and service availability. Physical access to the facilities is closely controlled. Physical security mechanisms include security guards, closed circuit TV surveillance video cameras, and intrusion detection systems. The NOC monitors access to all locations on a 24/7 basis.

Access to HSM requires at least two Key Administrator and Security Auditor. Key backups are stored on PIN entry device (PED) keys and locked in a 2 hour fire combination safe.

#### 4.1.3 Power and air conditioning

Each data center operates from multiple power sources, including backup generators and battery power. Each facility has multiple air conditioning units to control temperature and humidity.

#### 4.1.4 Water exposure

Gap Inc. and Neustar have taken precautions to minimize the impact of damage to the systems from water exposure.

#### 4.1.5 Fire prevention and protection

Gap Inc. and Neustar have taken precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. All systems are protected by automated fire suppression systems.

#### 4.1.6 Media storage

Media storage and handling procedures are defined by Neustar's Data Protection Policy.

#### 4.1.7 Waste disposal

Neustar Information Security policy and procedure includes guidelines for the appropriate disposal of outdated materials based on their sensitivity. The procedure involves the deposit outdated paper information in specially marked disposal bins on Neustar premises (subject to shredding). Further, electronic data is reliably expunged or cleared or media physically destroyed. Hard disks and backup tapes, which are no longer required, are subject to demagnetizing.

#### 4.1.8 Off-site backup

Backup software is installed and utilized for the backup of all critical systems and backup media is rotated to an off -site location on a regular basis. Further, all critical system backups are incorporated into the established process for semi-annual backup recovery testing in accordance with Neustar Backup policy.

### 4.2 Procedural Controls

#### 4.2.1 Trusted role

Neustar has a limited number of trusted roles in the DNSSEC management and operations. The roles are as follows:

Key Administrator

- Generation of Keys and DS records
- Management of key rollover events

Security Auditor

- Oversees security audits
- Ensures rules/procedures are followed

DNSSEC Officer

- Participates in community conferences and workshops
- Expert in the DNSSEC technology
- Coordinator between Neustar and external parties

#### 4.2.2 Number of persons required per task

Key signing ceremony and HSM activation require a minimum of two Key Administrators and a Security Auditor.

#### 4.2.3 Identification and authentication for each role

Only authorized personnel are allowed to gain physical access to data center where the .GAP DNSSEC systems are located. Access to the system is only granted to members of the roles identified above.

#### 4.2.4 Tasks requiring separation of duties

Tasks requiring separation of duties include key generation, implementation, and removal.

### 4.3 Personnel Controls

#### 4.3.1 Qualifications, experience, and clearance requirements

Only employees may be assigned to the DNSSEC roles described in section 4.2.1. Experience and qualifications are evaluated on a case by case basis but generally extensive knowledge in DNS operations and security related technologies are required.

#### 4.3.2 Background check procedures

Background checks included a review of an Applicant's qualifications, work history, references, educational background, and any other data relevant to the duties of the position.

#### 4.3.3 Training requirements

Personnel are provided continuous training in DNSSEC operations and management. The training includes but is not limited to .GAP specific rules and procedures and related technologies. Personnel actively participate in DNSSEC workshops and conferences.

#### 4.3.4 Retraining frequency and requirements

Retraining is provided as necessary and is done on a case by case basis.

#### 4.3.5 Job rotation frequency and sequence

Not applicable in this document.

#### 4.3.6 Sanctions for unauthorized actions

Not applicable in this document.

#### 4.3.7 Contracting personnel requirements

Not applicable in this document.

#### 4.3.8 Documentation supplied to personnel

All personnel participating in DNSSEC related activities are provided with documents containing operational procedures, rules and policies governing the service.

### 4.4 Audit Logging Procedures

#### 4.4.1 Types of events recorded

The .GAP Registry logs all necessary information concerning an event (who, what, and when) including:

- Access to data centers where DNSSEC services are located
- Access to servers and HSM
- Modifications to files and file systems
- Key operations:
    - Key generation/deletion and other events relating to lifecycle of a key
    - Generation of DS record and submission to root zone

#### 4.4.2 Frequency of processing log

Audit logs are monitored at regularly timed intervals in order to ensure the operational integrity of the .GAP DNSSEC Service. Abnormal events are flagged for further investigation by the DNSSEC Security Auditor.

#### 4.4.3 Retention period for audit log information

Registry logs are kept online for at least 3 months. Older logs are stored are archived for up to 5 years.

#### 4.4.4 Protection of audit log

Access to audit logs is only available to authorized personnel to protect the files from unauthorized viewing, modification, deletion, or other tampering. Audit logs do not contain any information that could be used to compromise the integrity of the private keys.

#### 4.4.5 Audit log backup procedures

Audit logs are backed up at pre-defined intervals to an offline storage system. Access to these archives can only be requested and viewed by authorized DNSSEC personnel.

#### 4.4.6 Audit collection system

The Registry utilizes software and applications that automate the logging of essential events into audit logs. Along with the systems level logging, application logs are recorded and stored.

#### 4.4.7 Notification to event-causing subject

Not applicable in this document.

#### 4.4.8 Vulnerability assessments

Automated and manual assessments of vulnerabilities are done in part by monitoring of audit logs. Registry personnel also participate and share security related information with other members of the community.

### 4.5 Compromise and Disaster Recovery

#### 4.5.1 Incident and compromise handling procedures

If an incident and compromise is detected, the scope of the issue is determined. In the event a key has been compromised, an emergency key roll-over is immediately initiated. The Registry has emergency roll-over policies for both KSK and ZSK.

#### 4.5.2 Corrupted computing resources, software, and/or data

The Registry has backup systems and failover sites in case of resource, software, and/or data corruption. Depending on the nature of the issue, appropriate actions will be taken according to the Registry recovery plan.

#### 4.5.3 Entity private key compromise procedures

In the event of compromise of the Registry's KSK, the following steps will be taken:

- Generate and activate a new KSK or activate the preview KSK that is already in the registry zone. As part of the activation, the DNSKEY set will be resigned.
- Replace the DS record of compromised key with new DS record in root zone.
- Revoke and then remove the compromised KSK in the Registry's zone as soon as it is sufficiently safe to remove.

In the event of a compromise of the Registry's ZSK, the following steps will be taken:

- Generate and activate a new ZSK or activate the preview ZSK that is already in the registry zone. As part of the activation, all signatures will be resigned.
- Remove the compromised ZSK from the registry's zone as soon as its signatures expired.

#### 4.5.4 Business continuity and IT disaster recovery capabilities

The Registry maintains a fully operational backup/failover site. In case of disaster, the failover/backup site will take over DNSSEC operations.

### 4.6 Entity Termination

In the event that the Registry is terminated, an orderly transition will be conducted with full cooperation of the Registry.

## 5 TECHNICAL SECURITY CONTROLS

### 5.1 Key Pair Generation and Installation

#### 5.1.1 Key pair generation

KSK and ZSK key pairs are generated during the signing ceremony that occurs once per year or more frequently if required. Generally, due to the scheduled key roll-over cycles, enough key pairs are generated during the ceremony to allow months of .GAP DNSSEC Services operations. Key generation is performed by authorized personnel in a FIPS 140-2 Level 3 Hardware Security Module.

#### 5.1.2 Public key delivery

Public keys used by the Registry KSK and ZSK are available as part of the Registry's DNSKEY Resource Record Set (RRset). It is not distributed by any other means.

### 5.1.3 Public key parameters generation and quality checking

Validating of the public key is performed periodically.

### 5.1.4 Key usage purposes

The keys are used for signature generation in the Registry's zone and not used for any other purposes.

## 5.2 Private Key Protection and Cryptographic Module Engineering Controls

### 5.2.1 Cryptographic module standards and controls

ZSK and KSK are generated and stored within a FIPS 140-2 Level 3 Hardware Security Module .

### 5.2.2 Private key multi-person control

During key generation, at least two authorized members of DNSSEC Key Administrator must be present.

### 5.2.3 Private key escrow

Private keys of the .GAP zone are not escrowed.

### 5.2.4 Private key backup

Private keys are backed up on FIPS140-2 compliant PCMCIA cards and stored both offsite and in a 2 hour fire combination safe.

### 5.2.5 Private key storage on cryptographic module

Not applicable in this document.

### 5.2.6 Private key archival

Private keys are not archived for storage purposes except at backup site in case of failover.

### 5.2.7 Private key transfer into or from a cryptographic module

ZSK and KSK generated in HSM are transferred to backup site in encrypted form.

### 5.2.8 Method of activating private key

Private keys are activated by Key Administrators supplying PINs to the hardware security module with presence of Security Auditor.

#### 5.2.9 Method of deactivating private key

Private keys are deactivated at shutdown of system.

#### 5.2.10 Method of destroying private key

KSK and ZSK private keys are removed from system in manner that they cannot be used again.

### 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

A KSK remains active in the Registry's zone for approximately one year plus the time it period for the transition including publish and deactivation. Due to the large number of signatures signed by the ZSK, the ZSK remains active for approximately three months plus the transition period including publish and deactivation. The Registry may change these periods as necessary.

### 5.4 Activation Data

#### 5.4.1 Activation data generation and installation

Activating of HSM requires Key Administrator supplying PIN to their PIN entry device with presence of Security Auditor.

#### 5.4.2 Activation data protection

Key Administrators are responsible for protecting and safeguarding their PIN and PED. Access can be revoked or modified if needed.

### 5.5 Computer Security Controls

All components of the DNSSEC service have different sets of authorized personnel that are granted access and the ability to execute certain operations. These access and operations are logged and written to audit logs. Any deviation of the rules or malicious attempts are monitored and recorded for further investigation.

### 5.6 Network Security Controls

All operations of the DNSSEC Service are hosted and performed inside Neustar's datacenters. These are internal networks protected by several layers of physical and networking protections. The networks are secured in accordance with the Network and Physical Security policies.

## 5.7 Timestamping

All timestamps used by the DNSSEC Service are in UTC and are synchronized using NTP (Network Time Protocol) servers.

## 5.8 Life Cycle Technical Controls

### 5.8.1 System development controls

All components of DNSSEC Service follow strict development guidelines prior to deployment. These strict guidelines ensure reliable, high-quality, and reproducible results.

### 5.8.2 Security management controls

The Registry has mechanisms to monitor any software changes on its servers and produce daily reports to be verified by authorized personnel.

### 5.8.3 Life cycle security controls

The Registry continues to enhance its controls based on feedback and community driven best practices. Any changes to software or security policies and procedures will be evaluated, tested, and approved before deployment.

# 6 ZONE SIGNING

## 6.1 Key Length and Algorithms

Both of the Registry's KSK and ZSK are RSASHA256. The KSK is 2048 bits while the ZSK is 1024 bits.

## 6.2 Authenticated Denial of Existence

The Registry uses NSEC records as specified in RFC 4034 to authenticate denial of existence.

## 6.3 Signature Format

The signature format for records in the .GAP zone is RSA/SHA-2 specified in RFC 5702.

### 6.4 Zone Signing Key Roll-over

The .GAP ZSK is rolled-over every 3 months.

### 6.5 Key Signing Key Roll-over

The .GAP KSK is rolled-over every 12 months.

### 6.6 Signature Validity Period and Re-signing Frequency

Signatures are valid for 30 days for both signatures signed by the ZSK and the KSK. Re-signing of the signatures occur around 7 days prior to the expiration.

### 6.7 Verification of Zone Signing Key Set

The ZSK is generated during the signing ceremony follows a well-defined set of procedures. The generated public keys along with its metadata are further verified by another set of automated validation tools.

### 6.8 Verification of Resource Records

On periodic basis, the Registry performs online verification of all resource records in the zone. It records all resource records and validates all signatures within the zone.

### 6.9 Resource Records TTL

The TTL of DNSKEY, DS and their corresponding Resource Record Signature (RRSIG) is set to 518400 (6 days). The TTL of the NSEC and their corresponding RRSIG is 86400 (1 day). The TTL could change in the future as needed.

## 7 COMPLIANCE AUDIT

A regular audit for .GAP DNSSEC Service is performed by Auditor.

## 8 LEGAL MATTERS

### 8.1 Fees

No fees are charged for acceptance, signing and publishing of Delegation Signer resource records, or any other function related to DNSSEC.

## 8.2 Financial responsibility

Gap Inc. accepts no financial responsibility for improper use of signatures issued under this DPS.

## 8.3 Confidentiality of business information

### 8.3.1 Scope of confidential information

The following records shall be kept confidential and private (Confidential/Private Information):

- Private keys and information needed to recover such private keys
- Signatures of key sets to be published in the future
- Transactional records (both full records and the audit trail of transactions)
- Audit trail records created or retained by Neustar
- Audit reports created by Neustar (to the extent such reports are maintained), or their respective auditors (whether internal or public), until such reports are made public
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of Neustar hardware and software and the administration of DNS Keys

### 8.3.2 Information not within the scope of confidential information

Information pertaining to the database of domains operated by Neustar such as Public Keys other status information are public.

### 8.3.3 Responsibility to protect confidential information

Not applicable.

## 8.4 Privacy of personal information

### 8.4.1 Information treated as private

Not applicable.

### 8.4.2 Types of information not considered private

Not applicable.

### 8.4.3 Responsibility to protect private information

Not applicable.

#### 8.4.4 Disclosure Pursuant to Judicial or Administrative Process

Gap Inc. shall be entitled to disclose Confidential/Private Information if, in good faith, Gap Inc. believes that disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

### 8.5 Limitations of liability

Gap Inc. shall not be liable for any financial loss, or loss arising from incidental damage or impairment, resulting from its performance of its obligations hereunder. No other liability, implicit or explicit, is accepted.

### 8.6 Term and termination

#### 8.6.1 Term

The DPS becomes effective upon publication in the Gap Inc. repository. Amendments to this DPS become effective upon publication in the Gap Inc. repository.

#### 8.6.2 Termination

This DPS as amended from time to time 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.

#### 8.6.4 Governing law

This DPS shall be governed by the laws of the United States of America.