Google DNSSEC Practice Statement

Table of Contents

1. INTRODUCTION
   - 1.1. Overview
   - 1.2. Document name and identification
   - 1.3. Community and Applicability
     - 1.3.1 The Google Registry
     - 1.3.2 Registrar
     - 1.3.3 Registrant
   - 1.4. Specification Administration
     - 1.4.1. Specification administration organization
     - 1.4.2. Contact information
     - 1.4.3. Specification change procedures

2. PUBLICATION AND REPOSITORIES
   - 2.1. Repositories
     - 2.2. Publication of key signing keys
     - 2.3. Access controls on repositories

3. OPERATIONAL REQUIREMENTS
   - 3.1. Meaning of domain names
   - 3.2. Activation of DNSSEC for child zone
   - 3.3. Identification and authentication of child zone manager
   - 3.4. Registration of delegation signer (DS) resource records
   - 3.5. Method to prove possession of private key
   - 3.6. Removal of DS record Approach 1

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS
   - 4.1. Physical Controls
     - 4.1.1. Site location and construction
     - 4.1.2. Physical access
     - 4.1.3. Power and air conditioning
     - 4.1.4. Water exposure
     - 4.1.5. Fire prevention and protection
     - 4.1.6. Media storage
     - 4.1.7. Waste disposal
     - 4.1.8. Off-site backup

Abstract

This document is the DNSSEC Practice Statement for any Charleston Road Registry Authoritative DNS TLD zone, hereafter referred to as "the Zone". It states the practices that are employed in providing and therefore zonefile signing, zone signing, and zone distribution services for the Zone.

1. INTRODUCTION

This document is the DNSSEC Practice Statement (DPS) for the Zone. This document states policies and practices that are employed by Google with regard to DNSSEC operations for the Zone.

1.1. Overview

DNSSEC is a set of IETF specifications that add data origin authentication and integrity guarantees to the Domain Name System. DNSSEC uses public key cryptography to apply digital signatures to DNS records, preventing various forms of falsification and tampering.

The following RFCs define DNSSEC and related concerns:

RFC 4033

DNS Security Introduction and Requirements

http://www.ietf.org/rfc/rfc4033.txt

RFC 4034

Resource Records for the DNS Security Extensions

http://www.ietf.org/rfc/rfc4034.txt

RFC 4035

Protocol Modifications for the DNS Security Extensions

http://www.ietf.org/rfc/rfc4035.txt

RFC 5910

Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP) http://tools.ietf.org/html/rfc5910

RFC 4509

Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs) http://tools.ietf.org/search/rfc4509

RFC 6781 (updates 4641)

DNSSEC Operational Practices

http://tools.ietf.org/search/rfc6781

RFC 5155

DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

http://tools.ietf.org/search/rfc515

Table of Contents Continued
4.2. Procedural Controls
4.2.1. Trusted roles
4.2.2. Number of persons required per task
4.2.3. Identification and authentication for each role
4.2.4. Tasks requiring separation of duties
4.3. Personnel Controls
4.3.1. Qualifications, experience, and clearance requirements
4.3.2. Background check procedures
4.3.3. Training requirements
4.3.4. Retraining frequency and requirements
4.3.5. Job rotation frequency and sequence
4.3.6. Sanctions for unauthorized actions
4.3.7. Contracting personnel requirements
4.3.8. Documentation supplied to personnel
4.4. Audit Logging Procedures
4.4.1. Types of events recorded
4.4.2. Frequency of processing log
4.4.3. Retention period for audit log information
4.4.4. Protection of audit log
4.4.5. Audit log backup procedures
4.4.6. Audit collection system
4.4.7. Notification to event-causing subject
4.4.8. Vulnerability assessments
4.5. Compromise and Disaster Recovery
4.5.1. Incident and compromise handling procedures
4.5.2. Corrupted computing resources, software, and/or data
4.5.3. Entity private key compromise procedures
4.5.4. Business Continuity and IT Disaster Recovery Capabilities

5. TECHNICAL SECURITY CONTROLS
5.1. Key Pair Generation and Installation
5.1.1. Key pair generation
5.1.2. Key installation
5.1.3. Public key delivery
5.1.4. Public key parameters generation and quality checking
5.1.5. Key usage purposes

1.2. Document name and identification

Google DNSSEC Practice Statement for the Zone (GOOGLE DPS)
Version: 1.1

1.3. Community and Applicability

1.3.1 The Google Registry

The Google Registry is the domain name registry for the Zone. The Google registry provides standard registry services for registrars as well as DNS service. To implement DNSSEC, Google generates Zone Signing Keys (ZSK) and Key Signing Keys (KSK), and uses them to sign resource records in the Zone. The Google Registry also submits a DS record corresponding to its KSK to IANA in order to form a chain of trust with the root zone.

1.3.2 Registrar

Registrars are ICANN Accredited Registrars that have signed up to register domain names in the Zone. With regards to DNSSEC, Registrars are responsible for transmitting DS records submitted by the Registrant to the Registry.

1.3.3 Registrant

The Registrant is an entity that has registered a domain name in the Google registry via a Registrar. Optionally, the Registrant may submit DS records for the zones they control.

1.4. Specification Administration

This DPS will be periodically reviewed and updated based on legal, security, technical, and business requirements of Google, and of governing bodies that authorize the use of the Zone.

1.4.1. Specification administration organization

Google, Inc.

1600 Amphitheatre Parkway

Mountain View, CA 94043

USA

1.4.2. Contact Information

DNSSEC Administrator

Charleston Road Registry

1600 Amphitheatre Parkway

Mountain View, CA 94041

USA

(650) 253-0000 (voice)

(650) 253-0001 (fax)

dnssec-admin@charlestonroadregistry.com

tld-replies@google.com

1.4.3. Specification change procedures

Amendments to this DPS are made by Google Domain Security as a new DPS with a new version number and release date. The latest version of this DPS can be found at www.charlestonroadregistry.com/faq/dps updates supercede all previous versions of the DPS.

Google reserves the right to update the DPS without notification for amendments that are not material. Major amendments will be updated and posted before a new version of the DPS is published.

Table of Contents Continued

5.2. Private key protection and Cryptographic Module Engineering Controls
5.2.1. Cryptographic module standards and controls
5.2.2. Private key (m-of-n) multi-person control
5.2.3. Private key escrow
5.2.4. Private key backup
5.2.5. Private key archival
5.2.6. Private key transfer into or from a cryptographic module
5.2.7. Private key storage in cryptographic module
5.2.8. Method of activating private key
5.2.9. Method of deactivating private key
5.2.10. Method of destroying private key
5.3. Other Aspects of Key Pair Management
5.3.1. Public key archival
5.3.2. Key usage periods
5.4. Activation data
5.5. Computer Security Controls
5.6. Network Security Controls
5.7. Timestamping
5.8. Life Cycle Technical Controls
5.8.1. System development controls
5.8.2. Security management controls

6. ZONE SIGNING
6.1. Key lengths and algorithms
6.2. Authenticated denial of existence
6.3. Signature format
6.4. Key Roll-Over
6.5. Signature life-time and re-signing frequency
6.6. Verification of zone signing key set
6.7. Verification of resource records
6.8. Resource records time-to-live

7. COMPLIANCE AUDIT
7.1. Frequency of entity compliance audit
7.2. Identity/qualifications of auditor
7.3. Auditor's relationship to audited party
7.4. Topics covered by audit
7.5. Actions taken as a result of deficiency
7.6. Communication of results

8. LEGAL MATTERS
8.1. Information privacy and associated agreements
8.2. Limitations of liability
8.3. Term and termination
8.4. Dispute resolution provisions
8.5. Governing law

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

A repository of past and present versions of this DPS can be found at:

www.charlestonroadregistry.com/faq/dps

2.2. Publication of key signing keys

The Zone will publish a DS record in the root zone. The public portion of the KSK will not be explicitly published as a trust anchor.

2.3. Access controls on repositories

The repository of this DPS is open to the public to read. Google maintains strict physical and logical access control around who can modify the DPS.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

DNSSEC as applied to the Zone does not have any interaction with the meaning of the domains in the Zone. DNSSEC as applied to the Zone only provides for authenticated DNS queries.

3.2. Activation of DNSSEC for child zone

DNSSEC for a child zone under the Zone is activated when a child zone publishes a DS record. This DS record is a cryptographic shorthand representation of the child zone's KSK, which Google then signs with the ZSK for the Zone. This establishes a chain of trust from the Zone to the child zone.

3.3. Identification and authentication of child zone manager

Google does not provide for any verification of the child zone manager. It only applies DS records directly specified by the Registrar acting on behalf of the Registrant.

3.4. Registration of delegation signer (DS) resource records

Registrants submit DS records through their respective Registrars, which in turn forward them to the Google Registry for inclusion in the Zone.

3.5. Method to prove possession of private key

The Google Registry does not specify requirements of its Registrars to prove possession of private keys corresponding to DS records for child zones.

3.6. Removal of DS record

On behalf of the Registrant, the Registrar submits requests to the Google Registry to remove the DS record.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

All Google employees and contractors must present identification with a badge with photo on both sides. This badge is also used to allow Google employees into Google buildings. Sensitive locations containing server or other equipment are locked down to appropriate groups within Google.

Google employees are instructed to ensure that those following them into a building are displaying their badge. Those not displaying their badge are not allowed to enter, and must proceed to a lobby to get a temporary badge.

All visitors to Google must register at a Google frontdesk with their host in order to get access to Google premises. Visitors must be accompanied by a Google employee at all times. Visitors are not allowed into sensitive areas.

Video surveillance is used extensively at Google on nearly all building entrances. Tapes are archived and rotated on a reasonable basis determined necessary by the security team.

A 24/7 physical security team is present to ensure the security and safety of everybody on Google property. Google employees have a direct number they can call to report a security incident.

4.1.1. Site location and construction

Google data centers locations are published at the following URL:

http://www.google.com/about/datacenters/locations/index.html

Google office locations that have employees who could potentially access DPS related systems are specified here:

http://www.google.com/about/company/address.html

4.1.2. Physical access

Google DNS systems are located in secured sites with restricted physical access and 24/7 on-site security to prevent intrusion. Physical access is given based on biometric identifiers combined with authorized badges, and all access to DNSSEC systems is logged.

4.1.3. Power and air conditioning

Google's DNSSEC systems are equipped with primary and backup power systems, as well as air conditioning to maintain proper temperature and humidity.

4.1.4. Water exposure

Google DNSSEC systems are located inside secure facilities with minimal possible risk of water exposure to systems.

4.1.5. Fire prevention and protection

Google DNSSEC systems are located in secure facilities with the appropriate equipment and procedures in place to prevent, detect, or address any risk associated with fire and smoke. Fire prevention and protection measures comply with all local fire safety regulations.

4.1.6. Media storage

Data used in the operation of Google DNSSEC systems are stored on media in secure data centers. Data is backed up continuously, with redundant on-site and off-site data backup. All data backup is transported and stored in a manner designed to protect media from damage and unauthorized access.

4.1.7. Waste disposal

All documents and materials are shredded before disposal with a major data shredding service.

4.1.8. Off-site backup

Google performs routine backups of all system data and logging data. Off-site backups are made regularly using a recognized major third-party storage facility.

4.2. Procedural Controls

4.2.1. Trusted roles

* Keystore Engineer

Keystore is a system that manages master and master keys here at Google. Master keys are used to generate fine-grained encryption keys for specific electronic assets. Master keys will not be used for DNSSEC. Master keys are used by services for a specific purpose. For DNSSEC, we will be using a master key to encrypt KSKs and ZSKs before they are stored onto disk. This master key will be referred to as the DNSSEC master key for the remainder of this document.

A Keystore Engineer is an engineer who works on the Keystore system.

* Authoritative DNS Engineer

The Authoritative DNS Engineer is an engineer who works on Google's Authoritative DNS System. The engineer may propose requests to change the DNSSEC master key. The Authoritative DNS Engineer may start jobs that can retrieve the DNSSEC master key, generate ZSKs and KSKs for the zones under control of the Authoritative DNS System, and encrypt those generated keys with the DNSSEC master key.

* SecOps

SecOps has access to an uber-master key used to encrypt all service encryption keys used here at Google. This key is only available to specific individuals on an as-needed basis.

4.2.2. Number of persons required per task

One Keystore Engineer and one Authoritative DNS Engineer are required to create or rotate the DNSSEC master key.

Creating a ZSK and deploying it into the Zone is fully automated.

Creating a KSK and deploying it into the Zone requires a Authoritative DNS Engineer to submit the relevant DS record changes with the root zone, but is fully automated otherwise.

4.2.3. Identification and authentication for each role

Google runs standard identity and background checks before hiring all Google employees.

While on any Google premises, Google employees must be identified using a name badge with a photo designed to minimize the risk of forgery.

Google Engineers of all types must first authenticate to the production network by inputting their google.com password and a one-time-password generated by a device kept on their person (two-factor authentication). Once authenticated to the production network, their credentials can be used to determine group membership. All production activities and systems are protected by groups. With regards to the DNSSEC implementation, Authoritative DNS Engineers and Keystore Engineers are in separate groups which guard access to systems relevant to their roles.

4.2.4. Tasks requiring separation of duties

Separation of duties is achieved by not allowing a single individual to change or update keys in Keystore. An individual can propose or submit a candidate change, but a different individual has to approve the change request.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

- Google requires that personnel seeking Trusted roles:
- Demonstrate appropriate skill levels to accomplish tasks
- Provide references to confirm claimed professional history
- Provide proof of eligibility for employment

4.3.2. Background check procedures

Google has established background investigations for all Google employees in accordance with local laws and will continue to do background investigations for any new Google employees. Criminal court, SSN trace, education and employment verification, global sanctions and enforcement checks are all performed. Background checks are handled by an established external investigative agency.

4.3.3. Training requirements

Google employees go through standard training and onboarding with respect to the role they perform. Training includes specific guidelines of Google's security procedures and requirements. Google continually revises training material and programs to improve them through time.

Google software engineering teams are responsible for creating documentation and procedures for onboarding new team members. With regards to teams managing systems using DNSSEC, new team members will be expected to learn about DNSSEC in its entirety and how DNSSEC is applied in the system they are maintaining.

4.3.4. Retraining frequency and requirements

Google periodically retrains employees on a variety of general topics as required by HR policy.

4.3.5. Job rotation frequency and sequence

No mandatory job rotation occurs in positions related to the operation of the Zone or the maintenance of DNSSEC systems.

No job rotation occurs with regards to job positions which affect the Zone's DNSSEC implementation and operation.

4.3.6. Sanctions for unauthorized actions

Google takes disciplinary actions as needed for unauthorized actions with respect to this DPS and other security policies, as appropriate for the nature of the unauthorized actions.

4.3.7. Contracting personnel requirements

Contracting personnel are sometimes used to fill Trusted roles. Any assignment of a temporary employee, vendor, or contractor to a Trusted role occurs on a case-by-case basis, with the same training and security criteria as full-time employees.

4.3.8. Documentation supplied to personnel

Google provides employees and contracting personnel with required documentation and training to perform roles.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

- Google logs all significant access to DNSSEC data. The types of events recorded include but are not limited to:
- Generation of keys
- Backup and storage of keys
- Activation of keys
- Receipt of public key data
- Signing of keys
- Rollover of keys
- Creating, reading, update, and delete of key-related data
- System access
- Errors or failures detected
- Access to data facilities
- Known incidents and resolutions
- Access to log information
- Changes in process or implementation of security policies
- Launching of jobs in production
- All activities related to passwords or employee authentication
- Communication to hosts outside of the production network
- Transmission of material identified as confidential, private, or intellectual property

In addition to event itself being recorded, the logger, time, date, end-user, client hostname and IP, server hostname and IP, and other relevant fields are stored in the log entry.

4.4.2. Frequency of processing log

Google constantly monitors for suspicious or unusual activity, and any detected activity is investigated by administration teams, with escalation as needed to address any problems found.

Logs are examined in response to any identified issue or possible compromise. Logs are examined as needed for auditing.

4.4.3. Retention period for audit log information

All audit data is held online for at least six months after creation. Additionally, audit logs are retained on tape indefinitely as needed.

4.4.4. Protection of audit log

Audit log information is treated as secure information and is protected from alteration or unauthorized access appropriately.

4.4.5. Audit log backup procedures
Audit logs that have a permanent retention policy are backed up to tape in an incremental fashion daily. Tapes are stored both on-site and off-site.

4.4.6. Audit collection system
All services performing sensitive operations with integrate with Google's production logs system. Services define a log message type, and submit logs during runtime for every relevant event.

4.4.7. Notification to event-causing subject
When an event is logged in the audit logs collection system, notice is given to the subject that caused the event only when appropriate actions are required from the subject.

4.4.8. Vulnerability assessments
With DNSSEC audit logs, Google runs tools to create reports that highlight "interesting" records that do not fit normal usage patterns. In addition, queries and reports over DNSSEC audited events can be created manually to highlight suspicious activity, e.g. KSK access by a new system or user.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures
In the case of a compromise or disaster, data is stored on-site for immediate restoration, or off-site with a time delay.

4.5.2. Corrupted computing resources, software, and/or data
If corrupted computing resources, software, or data are discovered, Google investigates the source of corruption and attempts to address and correct the source of the corruption immediately, escalating issues and assigning personnel to the issue as needed.

Last known good data is backed up and made available for restoration as needed during or after any incident of corrupted resources, software, and/or data. Additional hardware can be deployed immediately to address any detected problems.

4.5.3. Entity private key compromise procedures
Procedures below are identical for both KSK and ZSK keys.

When a compromise (or suspected compromise) of any sort is detected, a security incident is reported to a 24/7 team which evaluates the incident, and then upon verification, transitions responsibility to a response team to develop an action plan, and handle the compromise. For a private key compromise, participants will include the SecOps, Engineers working on DNSSEC systems, security incident team, and supporting staff.

A part of the action plan related to the security incident will be a key rotation strategy for the compromised key. At a bare minimum, an emergency key rollover will occur with the pre-publish method specified in RFC 6781. More extreme measures, such as outright removal of the key, will be considered depending on the severity of the compromise and possible impact of DNSSEC signature verification errors for the Zone.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities
DNSSEC systems will use the same data centers, server technology, and operations management capabilities that support other Google applications and services that already provide extremely high continuity for applications such as Google Search and Google Mail. Our production technology does not rely on any one specific data center for its continued operation, and can provide continued service even in the case of more than one complete data center outage. Google's technology provides for redundant equipment, applications, services and data across multiple data centers. The Google Registry Service will operate on multiple, live, geographically dispersed instances to support vital registry functions.

Google will maintain a recovery time objective of two-hours for all DNSSEC systems.

For disruptions that are expected to affect DNSSEC systems beyond the normal two-hour recovery time limit, such as natural disasters, power grid failures, and such, Google will enter an Activation and Notification phase to prepare responsible personnel to perform recovery measures to restore Google Registry system functions.

The following roles may activate the registry contingency plans during this phase:

- Google Registry Incident Manager
- Site Reliability Director responsible for a critical registry function

- Site Reliability engineering teams responsible for a critical registry function
- Google Disaster Recovery Sponsor
- Google Disaster Recovery Coordinator

Google will provide a Disaster Response Communication Plan to personnel with detailed steps for an incident reporter to follow in case of an extraordinary event. This plan will describe how the incident reporter should respond to an event initially, and whom the reporter should notify. The plan will include up to date contact lists for related Google personnel, as well as other teams responsible for the underlying technical and operational services used by DNSSEC and related systems.

Any and all relevant parties will be contacted with respect to the severity of issue. Local law enforcement, fire departments, and other officials may be contacted as necessary.

4.6. Entity termination

In the event that operation of the Zone is assigned to other entities, Google will coordinate with other entities to implement the change securely.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Keystore is a key storage and management solution at Google. Keystore supports key creation, rotation, and destruction. Keystore uses a FIPS 140-2 level 3 HSM in order to generate an uber-master key. This uber-master key is then used to encrypt additional [er service master keys generated by Keystore before they are given to engineers. In general, engineers never see a raw key except development-only keys. Engineers then check in the encrypted master key material into source control along with its name, type, and access-control-list. Once checked in, the encrypted master key material is pushed to Keystore into production by an automated system. At this point, the created master keys are available to services which request them by name and type according to the access-control-list of the key.

We will be generating a AES CTR key with a size of 128-bits. This key will be the DNSSEC master key, and it will be stored in Keystore.

The Authoritative DNS System will generate the KSK and ZSK for the Zone using a open-source library such as openssl.

5.1.2 Key installation

To create or rotate the DNSSEC master key, an Authoritative DNS Engineer will generate the key in encrypted form, and create a change request. An authorized Google engineer will approve the change request. The Authoritative DNS Engineer will then submit the change request, and the DNSSEC key will be made available from the Keystore service globally.

The Authoritative DNS system will generate a ZSK and KSK key per zone. These keys will be stored encrypted by the DNSSEC master key along with other information with the zone. The Authoritative DNS store and the keys are globally replicated.

5.1.3. Public key delivery

A DS record for the Zone will be submitted to IANA using IANA's secure change request procedure for DS records. This will validate the KSK published as a DNSKEY in the Zone.

5.1.4. Public key parameters generation and quality checking

The Google Registry periodically reviews parameters used to generate the ZSK and KSK to see that they follow industry best-practices.

5.1.5. Key usage purposes

Any KSK or ZSK will be used only for signing the relevant RRsets or self-signing within the Zone.

5.2. Private key protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic module standards and controls

As previously stated in 5.1.1 above, the HSM used for generating the Keystore uber-master key is FIPS 140-2 level 3 compliant. Keystore generated keys are not generated using cryptographic modules. ZSKs and KSKs are not generated

using cryptographic modules.

5.2.2. Private key (m-of-n) multi-person control)
Since the Authoritative DNS System will potentially control hundreds of zones, private keys are entirely managed by this system. Engineers do not directly update or access private keys.

5.2.3. Private key escrow
Private components of the Zone KSK and ZSK are not escrowed.

5.2.4. Private key backup
Google will routinely backup all information stored in the Google Registry and related DNS data, including all keys for disaster recovery reasons. All tape backup data is stored encrypted using AES-128 bit encryption. Multiple levels of redundancy will be used including disk, tape, and off-site facilities. Iron Mountain is used for off-site backup storage. All access to data is governed through Google's overall access control system, which limits read, write, and ownership by specific groups based on job role. At no time will any private or symmetric keys be written to persistent storage in an unencrypted form.

5.2.5. Private key archival
ZSK and KSK keys are removed from the Authoritative DNS System once no longer needed. They will continue to exist on previous tape backups.

5.2.6. Private key transfer into or from a cryptographic module
Not applicable for this document.

5.2.7 Private key storage in cryptographic module
Not applicable for this document.

5.2.8. Method of activating private key
The Authoritative DNS System will generate ZSKs and KSKs for the zones it controls when the zone is created and periodically thereafter. ZSKs are generated automatically while KSKs will be generated manually on an as-needed basis.

5.2.9. Method of deactivating private key
The Authoritative DNS system will deactivate ZSKs periodically by removal of private key from storage and the public key from the published keyset. KSKs are deactivated manually when no longer needed.

5.2.10. Method of destroying private key
When a key is no longer needed, the persistence records storing the encrypted keys will be zeroed out. This will prevent further use of the key unless it's restored from backup.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival
ZSK and KSK keys removed from the Authoritative DNS System once no longer needed. They will continue to exist on previous tape backups.

5.3.2. Key usage periods
Keys will be used until rotated out of the zone. Once a key has been removed from the zone, the key will destroyed.

5.4. Activation data
Google does not use Activation data beyond the authenticated credentials of the engineers participating in updating or creating keys. Google employees must change their password yearly, cannot use previous passwords, and required to use industry-best practices when selecting a new password. In addition, Google employees are required to use a one-time-password (two-factor-authentication) in order to log onto the production network.

5.5. Computer Security Controls
Google secures systems that maintain key software and data files from unauthorized access. Google reviews and tests security on all systems. Access to production servers is given only to those in Trusted roles.

Google requires the use of passwords with a minimum character length and complexity, supplemented by two-factor authentication. Passwords are rotated regularly and systems exist to prevent reuse of passwords.

5.6. Network Security Controls

Network security for the administration and transmission of data complies with a standard policy for network security controls. Network access includes firewalls, system hardening, and regular testing and auditing of network security.

5.7. Timestamping

Time derived from the procedure will be used for timestamping of all audit logs and DNSSEC signatures. Asserted times are reasonably accurate.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

All code developed for DNSSEC systems at Google will require the following software development practice at a minimum:

- Checked into the standard source control for all Google code.
- Code owners explicitly indicated.
- Approval by code owners before making any changes.
- Programming Language “readability” ensuring adherence to Google-wide style.
- Unit and integration tests as applicable.
- Push-button (single command) deployment to each environment.

In addition, all source control for DNSSEC systems at Google can only be checked out on an encrypted partition on Google-approved workstations located at a Google office. Google employees must sign up for source control access separately. Engineering workstations all use a standard system image which is configured to protect the integrity of the system and code being developed on it.

5.8.2. Security management controls

Google deploys systems and policies that control and monitor the configuration of all systems. Systems are deployed using standardized hardware, operating systems, and software, with automated quality testing. All changes to production services are audited. Machine images include protection from unsupported software and software versions from being deployed.

6. ZONE SIGNING

6.1. Key lengths, key types and algorithms

The Zone adopts the standard RSA-SHA256 signing algorithm for signing RRsets as specified in RFC 5702. The length of the KSK key is 2048 bits. The length of the ZSK key is 1024 bits.

6.2. Authenticated denial of existence

The Zone will provide authenticated denial of existence through NSEC records as specified in RFCs 4033, 4034, 4035.

6.3. Signature format

Signatures will be in the RSA/SHA-2 format as specified in RFC 5702.

6.4. Key Roll-Over

ZSKs are automatically rolled over every 30-days with the pre-publish method specified in RFC 6781.

Google has no current plans to roll over the KSK for the Zone. Google will re-evaluate this need on a yearly basis.

6.5. Signature life-time and re-signing frequency

In the Zone, the signature validity period for RRsets will be 30 days and RRsets will be resigned weekly.

6.6. Verification of zone signing key set

The Authoritative DNS System introduces ZSKs as needed. No additional verification of the zone signing key is performed since the introduction is fully automated.

6.7. Verification of resource records
The Authoritative DNS will verify that all DNS resource records are valid according to DNS and DNSSEC RFCs before publishing them to the Zone.

6.8. Resource records time-to-live
- DNSKey: TTL 24 hours
- Delegation Signer (DS): TTL 24 hours
- RRSIG: same as the covered RRsets (varies by RRset)

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit
Compliance audits are conducted annually, with further audits conducted if special events demonstrate a need.

7.2. Identity/qualifications of auditor
An engineer separate from the Authoritative DNS team who specializes in security and DNSSEC enabled DNS systems in production will be performing the audit. This engineer will coordinate with Google security operations and application security to derive an audit plan on a yearly basis.

7.3. Auditor's relationship to audited party
The engineer will have no current professional relationship with the audited team except that the engineer may potentially report to the same VP.

7.4. Topics covered by audit
The compliance audit includes all DNSSEC operations as described in this document, such as KSK and ZSK generation, key publishing and rotation procedures, algorithm used for signatures, software development practice, etc.

7.5. Actions taken as a result of deficiency
If any significant exceptions or deficiencies are identified during a compliance audit, Google management will determine appropriate actions to be taken, with input from the auditor. Google will develop and implement a corrective action plan within 30 days and implemented in a commercially viable reasonable period of time.

For any insignificant exceptions and deficiencies, in particular those which do not impact external parties and can be fixed in less than 24 hrs, the auditor will work with the engineer to directly address the issue as time permits.

7.6. Communication of results
A copy of audit results will be made online at www.charlestonroadregistry.com/faq/dps.

8. LEGAL MATTERS

8.1. Information privacy and associated agreements
Subject to applicable laws, all information required to be published as part of a WhoIs database is not considered and will not be treated as confidential or private information. All information pertaining to the database of top-level domains is public information. Public Keys, Key Revocation, and other status information, is also not considered and will not be treated as confidential or private.

To the extent, Google receives or processes personally identifiable or confidential business information in the course of providing the Zone services, such information will be treated in accordance with the terms of its Registry Agreement, its agreements in force with its Registrars (Registry-Registrar Agreements), and in CRR's privacy policy, which is available at http://charlestonroadregistry.com/privacy.html which may be amended from time to time.

8.2. Limitations of liability
Google 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, including for the performance of third parties in providing DNSSEC or related services.

8.3. Term and termination

The DPS becomes effective upon publication by Google at www.charlestonroadregistry.com/faq/dps. This DPS, as amended from time to time, and will remain in force until it is replaced by a new version. Amendments to this DPS become effective upon each subsequent publication at www.charlestonroadregistry.com/faq/dps.

8.4. Dispute resolution provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties. Unless otherwise provided in the applicable agreements between the parties, disputes involving Google require an initial negotiation period of sixty (60) days followed by litigation for which the parties consent to the personal jurisdiction and the exclusive venue of the courts in Santa Clara County, California.

8.5. Governing law

The Google Registry is operated under the laws of California. This DPS shall be construed pursuant to the laws of California, excluding California's choice of law rules, unless otherwise provided in the applicable agreements among the parties.