CIRA DNSSEC PRACTICE STATEMENT

1. Introduction

This DNSSEC Practice Statement ("DPS") is a statement of security practices and provisions made by the Canadian Internet Registration Authority (CIRA). These practices and provisions are applied in conjunction with DNS Security Extensions (DNSSEC) of in all gTLD zone(s) under CIRA's services.

This DPS conforms to the template included in RFC 6841[1]. The approach described here is modelled closely on the corresponding procedures published in a corresponding DNSSEC Policy and Practice Statement published by .SE (The Internet Infrastructure Foundation) for the Swedish top-level domain[2], whose pioneering work in DNSSEC deployment is acknowledged.

DPS is subject to CIRA's Policies, Rules and Procedures, which are available on CIRA's website at: https://cira.ca/legal-policy-compliance/policies.

1.1. Document Name and Identification

The Domain Name System (DNS) is described in RFC 1034[3] and RFC 1035[4].

Name:	CIRA-DPS-gTLD-EN
Version:	1.0
Purpose:	DNSSEC Practice Statement
Date of Last Modification:	2016-08-20
Document Available From:	https://cira.ca/build-better-internet/dnssec-securing-domain-name-system

[1] https://tools.ietf.org/rfc/rfc6841.txt
[2] https://www.iis.se/docs/se-dnssec-dps-eng.pdf

1.2. Community and Applicability

The following functional subsets of the community to which this document has applicability have been identified.

1.2.1. TLD Registry

The Canadian Internet Registration Authority (CIRA) operates the Top Level Domain (TLD) registry as Back-End Service Provider (BESP). CIRA is responsible for the management of the registries, and consequently for the registration of domain names under the TLD.

CIRA is responsible for generating cryptographic key material, for protecting the confidentiality of the private component of all key pairs and for publishing the public component of relevant key pairs for use as DNSSEC trust anchors.

CIRA is also responsible for signing the TLD DNS zone using DNSSEC.

1.2.2. TLD Registrars

A registrar is a party responsible for requesting changes in the TLD registry on behalf of registrants. Each registrar is responsible for the secure identification of the registrant of a domain name under its sponsorship. Registrars are responsible for adding, removing or updating Delegation Signer (DS) records for each domain at the request of the domain's registrant.

1.2.3. TLD Registrants

Registrants are responsible for generating and protecting their own keys, and registering and maintaining corresponding DS records through a registrar.

Registrants are responsible for emergency key rollover if the keys used to sign their domain names are suspected of being compromised or have been lost.

1.2.4. Relying Party

The relying party is the entity that makes use of DNSSEC signatures, such as DNSSEC validators and other applications. The relying party is responsible for maintaining appropriate trust anchors. Relying parties who choose to make use of TLD-specific trust anchors must stay informed of any relevant DNSSEC-related changes or events in the TLD domain. Relying parties who make use of a root zone trust anchor should not need to make trust anchor changes in response to events in the TLD registry, since trust anchors are published by CIRA in the root zone as DS records.

1.2.5. Secure Identification

Each entity in the DNSSEC process will require an appropriate level of validation to ensure true identity, ownership, and responsibility. This will apply to CIRA staff, 3rd party service providers, and registrants.

1.2.6. Trusted Role

A person engaged in the support of DNSSEC infrastructure, deployment and management must be a full time employee of CIRA. Contractors may provide assistance for technology and process but should have restricted physical and logical access to any DNSSEC operational component. A contractor cannot act in a trusted role.

1.2.7. Applicability

Each registrant and relying party is responsible for determining an appropriate level of security for their domain and DNSSEC infrastructure. This DPS applies exclusively to the TLD zone. With the support of this DPS, registrants and relying parties can determine an appropriate degree of trust in the TLD zone and assess their own risk accordingly.

1.3. Specification Administration

This DPS is updated as appropriate to reflect modifications in systems or procedures.

1.4. Specification Administration Organisation

Canadian Internet Registration Authority (CIRA)
979 Bank Street, Suite 400
Ottawa, Ontario, K1S 5K5
Canada

1.5. Contact Information

Chief Information Officer
Canadian Internet Registration Authority (CIRA)
979 Bank Street, Suite 400
Ottawa, Ontario, K1S 5K5
Canada

1.6. Specification Change Procedures

Changes to this DPS will result in new revisions of the entire document. The current version of this document is available at < https://cira.ca/build-better-internet/dnssec-securing-domain-name-system >. Only the most recent version of this DPS is applicable. CIRA may amend the DPS without notification for changes that are not considered significant. Changes are designated as significant at CIRA's discretion. CIRA will provide reasonable notice of significant changes.

All changes to this DPS will be approved by the CIRA and be effective immediately upon publication.

2. Publication and Repositories

Notifications relevant to DNSSEC at CIRA will be distributed by e-mail to dnssec-announce@cira.ca.

2.1. Repositories

CIRA publishes DNSSEC-related information at < https://cira.ca/build-better-internet/dnssec-securing-domain-name-system>.

2.2. Publication of Key Signing Keys

CIRA publishes Key Signing Key (KSK) for the TLD zone as DS records in the root zone.

2.3. Access Controls on Repositories

Information published in the CIRA DNSSEC repository is intended to be available to the general public.

3. Operational Requirements

3.1. Meaning of Domain Name

A domain name is a unique identifier in the DNS, as described in RFC 1034[3] and RFC 1035[4]. For the purposes of this document a domain name is a name registered under the TLD top-level domain, and corresponds to a delegation from the TLD zone to name servers operated by or on behalf of the domain name's registrant.

3.2. Activation of DNSSEC for Child Zone

DNSSEC for a child zone is activated by publishing a signed DS record for that zone. The addition of a DS record to the TLD registry for the corresponding domain name, establishes a chain of trust from the TLD zone to the child zone.

3.3. Identification and Authentication of Child Zone Manager

Identification and authentication of each child zone manager is the responsibility of the sponsoring registrar for the domain name.

[3] http://www.ietf.org/rfc/rfc1034.txt
[4] http://www.ietf.org/rfc/rfc1035.txt

3.4. Registration of Delegation Signer Resource Records

The TLD registry accepts DS records through an EPP interface according to RFC 4310[5] and manually via our TLD Manager application. Any valid DS record will be accepted by the registry, and no checks are performed as to the accuracy of the trust anchor with respect to the child zone's KSK. Domain registrants will be responsible for providing current and accurate information to registrars.

3.5. Method to Prove Possession of Private Key

The sponsoring registrar for a domain name is responsible for validating the registrant as the manager of a private key.

3.6. Removal of Delegation Signer Record

DS records are removed from the TLD registry using an EPP interface according to RFC 4310[6] or manually via the web interface. The removal of all DS records for a domain name will remove the chain of trust between the TLD zone and the child zone.

3.7. Authority to Request Deregistration

The registrant for a domain name has the authority to request removal of a DS record.

3.8. Procedure for Removal Request

The registrant of a domain name requests the domain's sponsoring registrar to remove the DS record. The registrar transmits this request to the TLD registry using EPP or manually via the web interface. Once the transaction has been successfully received and processed by the TLD registry, the DS record will be removed from the TLD zone when the following revision of the TLD zone is distributed.

[5] http://www.ietf.org/rfc/rfc4310.txt
[6] http://www.ietf.org/rfc/rfc4310.txt

3.9. Emergency Removal Request

There is no provision for a registrant to be able to make an emergency removal request of the TLD registry. All DS record removals must be executed through the domain's sponsoring registrar.

4. Site, Management and Operational Controls

4.1. Physical Controls

CIRA has implemented the CIRA Security Policy, which supports the security requirements of this DPS. Compliance with these policies is included in Section 7 Compliance Audit.

4.1.1. Site Location and Construction

CIRA has established two fully-operational and geographically-dispersed operation centres. Each site serves as a back-up to the other. Both sites are protected by multiple tiers of physical security that deters, prevents and detects unauthorized access attempts.

4.1.2. Physical Access

Physical access to operation centres is restricted to authorised personnel. All entry to both operation centres is logged and the environment is continuously monitored. Access to secure containers is further restricted to personnel with trusted roles.

The physical security system includes additional tiers of key management security which serves to protect both online and inline storage of signers and keying material. Online signers are protected through the use of locked cabinets. Access to signers and keying material are restricted in accordance to CIRA's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

4.1.3. Power and Air Conditioning

Operation centres are equipped with multiple power sources, including battery and generator support to ensure an uninterrupted supply.

Operation centres are cooled with redundant air conditioning systems to ensure a consistent, stable operating environment.

4.1.4. Water Exposure

Both operation centres implement flood protection and detection mechanisms.

4.1.5. Fire Prevention and Protection

Operation centres are equipped with fire detection and extinguishing systems.

4.1.6. Media Storage

All media containing production software and data, audit, archive, or backup information is stored within the operation centers.

Sensitive media and other material that may contain sensitive information are destroyed in a secure manner, either by CIRA or by a contracted party.

4.1.7. Off-Site Backup

CIRA performs regular backups of critical data, audit logging data and other sensitive information.

4.2. Procedural Controls

4.2.1. Trusted Roles

Trusted roles include all employees that have access to or control cryptographic operations that may materially affect:

a. Generation and protection of the private component of the CIRA Zone Signing Key (ZSK) and Key Signing Key (KSK)
b. Secure export and import of any public components; and
c. Generation and signing Zone file data

Trusted roles include; but are not limited to:

a. Naming resolution operations personnel;
b. Security personnel;
c. System administration personnel;
d. Executives that are designated to manage infrastructure

4.3. Personnel Controls

4.3.1. Qualifications, Experience and Clearance Requirements

Candidates for any trusted role must demonstrate appropriate background and qualifications.

4.3.2. Background Check Procedures

Background checks for candidates for any trusted role are carried out by the Human Resources department at CIRA, and follow normal procedures for background checks on new hires.

4.3.3. Training Requirements

CIRA provides its personnel with training upon hire as well as on-going training need to for them to perform their job responsibilities competently and satisfactorily. CIRA reviews and enhances its training programs as necessary.

CIRA provides training programs specific to job roles and responsibilities and will include the following as relevant:

a. DNS/DNSSEC concepts
b. Cryptographic principles
c. Use and operation of deployed hardware and software
d. Security and operational policies and procedures
e. Incident and compromise reporting and handling
f. Disaster recovery and business continuity procedures and testing

4.3.4. Contracting Personnel Requirements

CIRA may choose to use contractors to assist CIRA in the development and management of DNSSEC technology. Contractors are to have restricted access to cryptographic material at all times. Contractors are subject to the same responsibility agreements and background checks as CIRA trusted roles.

4.3.5. Documentation Supplied to Personnel

CIRA will supply all personnel with trusted roles with necessary documentation to allow the tasks designated to those personnel to be executed effectively.

4.4. Audit Logging Procedures

CIRA implements automatic log collection from CIRA computer systems, for the purposes of monitoring and statistical analysis purposes in the event that a security violation is suspected.

Paper documentation relating to the execution of procedures is also collected for the purposes of auditing performance of those procedures.

4.4.1. Types of Events Recorded

CIRA manually or automatically logs the following significant events.
All KSK and ZSK key life cycle management events, including:

a. Key generation, backup, storage, recovery, archival and destruction
b. Exporting of public key components
c. Cryptographic device life cycle management events

All network systems use a centralized time system to ensure events across all devices are synchronized for time and date information.

4.4.2. Audit Collection System

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by CIRA personnel and stored using current methods for physical and fire protection.

4.4.3. Notification to Event-Causing Subject

All authorized personnel are informed that logging is taking place, and that logs are being retained.

4.4.4. Vulnerability Assessments

Vulnerability assessments are conducted against all data center sites on a regular basis. Any issues identified result in a risk management issue and are resolved using project management techniques to resolve and track.

4.4.5. System and Network Monitoring

All network access is monitored in real-time to detect anomalies. These events shall be investigated to analyse potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and Compromise Handling Procedures

All actual and suspected events relating to security that have caused or could have caused an outage, damage to computer systems, disruptions and defects due to incorrect information or security breaches are defined as incidents.

All incidents are handled according to CIRA's standard procedures.

4.5.2. Corrupted Computing Resources, Software and/or Data

Any defect which results in the generation of inaccurate data will be addressed by the deployment of multiple, independent signers. All such defects will trigger incident management procedures.

4.5.3. Entity Private Key Compromise Procedures

A suspected or actual ZSK compromise will be addressed by immediately removing the compromised ZSK from service, replacing it with a newly-generated or pre-generated replacement key.

A suspected or actual KSK compromise will be addressed by immediately executing a controlled key rollover.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

CIRA's organisation-wide business continuity and IT disaster recovery plans include measures to ensure continuity of operation for registry and zone distribution systems. Multiple live log collection, zone audit and signer components are deployed to ensure continuity of operation for DNSSEC systems.

4.5.5. Entity Termination

If CIRA needs to discontinue DNSSEC for the TLD zone for any reason and return to an unsigned zone, the removal of DNSSEC will take place in an orderly manner with public notification.

If operation of the TLD registry is transferred to another party, CIRA will participate in the transition so as to make it as smooth as possible.

5. Technical Security Controls

5.1. Key Pair Generation and Installation

Key generation takes place in signers using a Software Hardware Security Module (softHSM) that is managed by trained and specifically authorized personnel in trusted roles on dedicated hardened systems.

The KSK, and ZSK are generated in a pre-planned key generation ceremony. The activities of this key generation ceremony are recorded, dated, and signed by the individuals involved. These records are kept for audit and tracking purposes. Private components of zone KSK and ZSK are not escrowed.

CIRA KSK and ZSK key pairs do not expire, but are retired when superseded.

5.2. Other Aspects of Key Pair Management

Public keys are backed up and archived as part of CIRA's routine backup procedures. The operational period of each KSK and ZSK ends upon its supersession. The superseded zone KSK and ZSK will be never be reused to sign a resource record.

5.3. Computer Security Controls

All production computer systems are housed in secure facilities. Physical access to computer systems is limited to authorized personnel. The signing systems are contained in a secure zone. All attempts to access computer systems, successful and unsuccessful, are logged.

5.4. Network Security Controls

CIRA's production network is logically separated from other components with zones. This separation prevents network access except through defined application processes. CIRA uses firewalls to protect the production network from both internal and external intrusion and to limit the nature and source of network activities that may access production systems that are related to key signing activities.

All firewall components generate logs which are collected, analysed and retained. Other techniques such as IPS/IDS will alert when attempts to modify system packages have been made.

5.5. Timestamping

All DNSSEC components are time-synchronised to diverse, reputable time servers using authenticated NTP. Timestamps are always generated in UTC.

5.6. Life Cycle Technical Controls

5.6.1. System Development Controls

Applications are developed and implemented by CIRA in accordance with CIRA systems development and change management processes.

All software deployed on production systems shall be traced to change management tickets.

5.6.2. Security Management Controls

CIRA has technologies and/or policies in place to control and monitor the configurations of its systems.

5.6.3. Life Cycle Security Controls

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system will be applied after formal testing and approval. The origin of all software and firmware will be securely authenticated by available means. Critical hardware components of the signer system will be transported in tamper-evidence bags to their destination in the secure site. All hardware will be decommissioned well before the specified life time expectancy.

6. Zone Signing

6.1. Key Lengths and Algorithms

KSK Algorithm	RSA
KSK Length	2048 bits
ZSK Algorithm	RSA
ZSK Length	1024 bits

6.2. Authenticated Denial of Existence

Authenticated denial of existence may be provided through the use of NSEC3 records as specified in RFC 4033–35 and RFC 5155 (TLD dependant)

6.3. Signature Format

Zone KSK and ZSK signatures are generated using RSA over SHA256 (RSASHA256, as specified in RFC 5702[7]).

6.4. Zone Signing Key Rollover

Key Activity	Length	Description
Active	30 days	The number of days a key is used to sign a zone before rolling over to a new key
Emergency rollover post-publish	2 days	If a ZSK is believed to be compromised, an emergency rollover of the ZSK will result in the old key still being published in the zone for 2 days; ensuring resolvers do not malfunction but the zone is not signed with it.

[7] http://www.ietf.org/rfc/rfc5702.txt

6.5. Key Signing Key Rollover

KSK rollover is carried out every year.

Key Activity	Length	Description
Active	365 days	The number of days a key is used to sign a zone before rolling over to a new key
Pre-publish	30 days	Before we begin to sign a zone with a key, we pre-publish the key in the zone for this period
Post-publish	30 days	After the old key is rolled over, it is still published (however nothing is signed with it) in the zone for this period
Emergency rollover post-publish	7 days	If a ZSK is believed to be compromised, an emergency rollover of the ZSK will result in the old key still being published in the zone for 2 days; ensuring resolvers do not malfunction but the zone is not signed with it.

6.6. Signature Lifetime and Re-Signing Frequency

Resource Record sets (RRSets) are signed with ZSKs with a validity period between six and eight days. Re-signing takes place every time a new TLD zone is generated.
The apex DNSKEY RRSet is additionally signed with the KSK with the same validity period and re-signing frequency.

6.7. Verification of Zone Signing Key Set

Each signed zone is subject to an array of tests, all of which must pass before the signed zone is distributed to name servers. These tests include verification of the chain of trust from the root zone to signatures over the apex DNSKEY RRSet.

6.8. Verification of Resource Records

All resource records are verified prior to distribution. The integrity of the unsigned zone contents is also validated prior to distribution.

6.9. Resource Records Time-to-Live

SOA	86400 seconds (24 hours)
DNSKEY	21600 seconds (6 hours)
NS, A, AAAA	86400 seconds (24 hours)
RRSIG	inherited from signed RRSet
Delegation Signer (DS)	86400 seconds (24 hours)
NSEC3	3600 seconds (1 hour)

7. Compliance Audit

Audits are conducted using retained logs and other relevant information to ensure that proper procedures have been followed at all times, and that the procedures have been executed accurately.

7.1. Frequency of Entity Compliance Audit

CIRA conducts audits at least annually. Circumstances which might lead to additional audits being carried out include recurring anomalies, significant staff changes or changes in equipment.

7.2. Identity and Qualifications of Auditor

CIRA compliance audits are performed by security consulting firms that demonstrate proficiency in security and public key infrastructure technology, information security tools, security auditing and assessments.

The auditor will demonstrate proficiency in IT security, DNS and DNSSEC.

7.3. Auditor's Relationship to Trusted Party

CIRA will appoint an external auditor who is responsible for the audit's implementation.

7.4. Topics Covered by Audit

Each audit will include a review of events which occurred during a specified audit period. The auditor will ensure that CIRA is informed and prepared prior to the audit, including details of the particular topic of the audit.

7.5. Actions Taken as a Result of Deficiency

The auditor will immediately inform CIRA of any observed anomaly and/or areas of risk which will be managed as part of CIRA's risk management methodology.

7.6. Communication of Results

Results of each audit will be provided to CIRA in a written report no later than 30 days following the completion of the audit.

8. Legal Matters

8.1. Fees

No fees are charged for any function related to DNSSEC.

8.2. Financial Responsibility

CIRA accepts no financial responsibility for improper use of Trust anchors or signatures, or any other improper use under this DPS.

8.3. Term and Termination

This DPS applies until further notice.

8.3.1. Term

This DPS is valid until it is replaced by a new version.

8.3.2. Termination

This DPS is valid until it is replaced by a new version.

8.3.3. Dispute Resolution Provisions

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

8.3.4. Governing Law

This DPS shall be governed by the laws of the province of Ontario and the laws of Canada applicable therein.