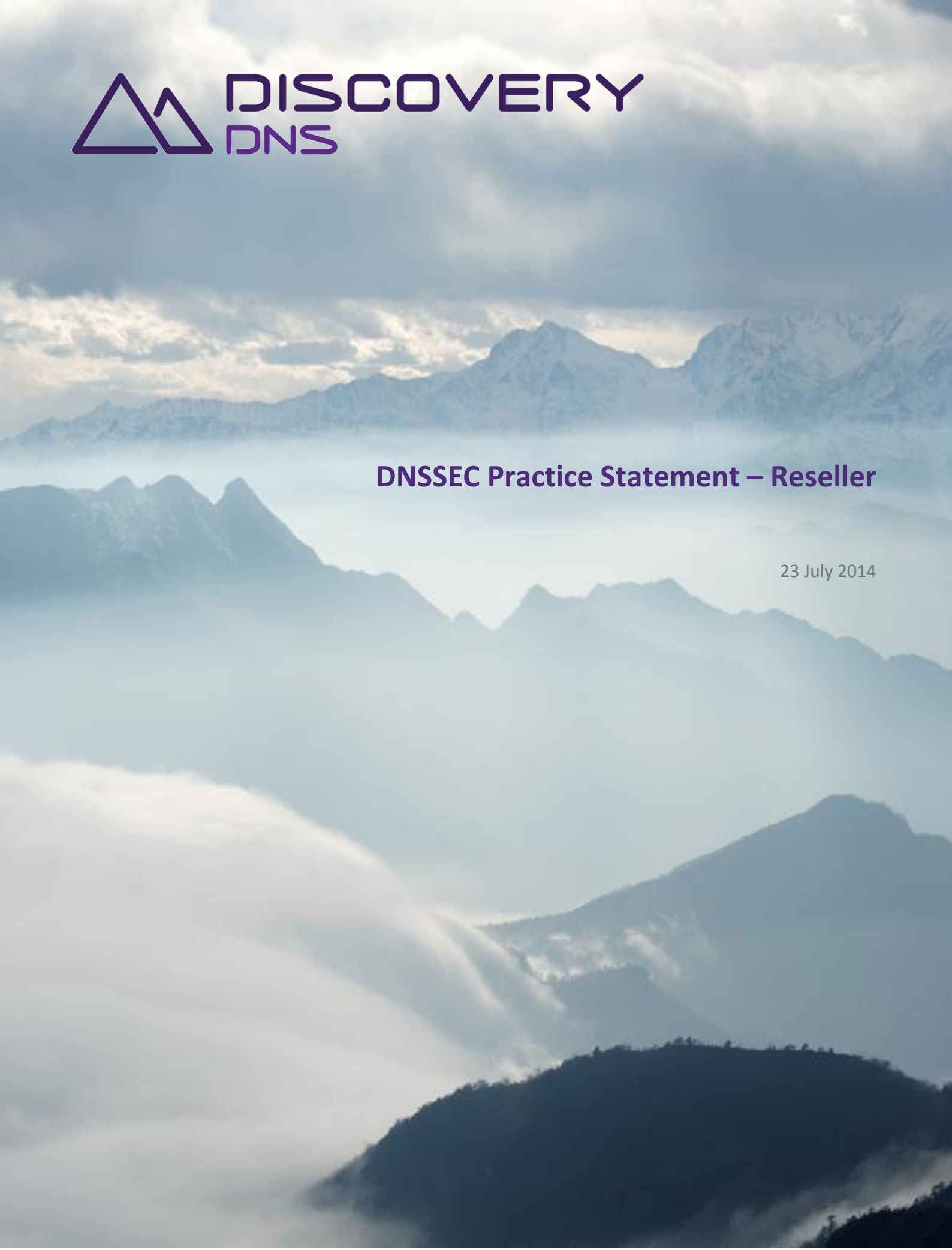

DISCOVERY DNS

DNSSEC Practice Statement – Reseller

23 July 2014

This document is provided pursuant to the disclaimer provided on the last page.

Contact

Name	Customer Support
Address	L8, 10 Queens Rd, Melbourne, Vic 3004, Australia
Number	+61 3 9090 1700
Email	support@discoverydns.com

Classification

Confidential

About DiscoveryDNS

Based on client demand and leveraging over 11 years of experience ARI Registry Services launched DiscoveryDNS. DiscoveryDNS provides a global DNS service to ARI Registry Services' clients around the world.

About ARI Registry Services

ARI Registry Services, part of the Bombora Technologies group of companies, is driving innovation and the expansion of the Internet through the delivery of world-class domain name Registry Services. With over 11 years of experience, ARI Registry Services is a leading provider of Domain Name Infrastructure Services and DNS Services for generic Top-Level Domain applicants and country code Registry Operators.

We help governments, major brands and entrepreneurs across the globe realise the full potential of the Internet by providing expertise, security and reliability in operating a core Internet infrastructure.

Contents

1 Introduction 1

1.1 Overview 1

1.2 Document name and identification 1

1.3 Community and applicability 1

1.4 Specification administration 2

2 Publication and repositories 3

2.1 Repositories 3

2.2 Publication of public keys 3

2.3 Access controls on repositories 3

3 Operational Requirements 4

3.1 Meaning of domain names 4

3.2 Identification and authentication of Child Zone Manager 4

3.3 Registration of Delegation Signing (DS) Resource Records 4

3.4 Method to prove possession of Private Key 4

3.5 Removal of DS Resource Record 4

4 Facility, management and operational controls 5

4.1 Physical controls 5

4.2 Procedural controls 7

4.3 Personnel controls 7

4.4 Audit logging procedures 8

4.5 Compromise and disaster recovery 10

4.6 Entity termination 11

5 Technical security controls 12

5.1 Key pair generation and installation 12

5.2 Private key protection and cryptographic module engineering controls 13

5.3 Other aspects of key pair management 14

5.4 Activation data 14

5.5 Computer security controls 14

5.6 Network security controls 14

5.7 Time stamping 15

5.8 Lifecycle technical controls 15

6 Zone Signing 16
6.1 Key lengths, key types and algorithms 16
6.2 Authenticated denial of existence 16
6.3 Signature format 16
6.4 Key roll-over 16
6.5 Signature Lifetime and Re-Signing Frequency 16
6.6 Verification of resource records 16
6.7 Resource records time-to-live 17
7 Compliance Audit 18
7.1 Frequency of entity compliance audit 18
7.2 Identity/qualifications of auditor 18
7.3 Auditor's relationship to audited party 18
7.4 Topics covered by audit 18
7.5 Actions taken as a result of deficiency 18
7.6 Communication of results 18
8 Legal Matters 19
8.1 Fees 19
8.2 Financial responsibility 19
8.3 Confidentiality of business information 19
8.4 Privacy of personal information 20
8.5 Limitations of liability 20
8.6 Term and termination 20
9 Glossary 22

1 Introduction

This document is ARI Registry Services' DNSSEC Practices Statement for the DiscoveryDNS's Reseller DNS system. It states the considerations that ARI Registry Services follows in providing DNSSEC services for the system.

This document details the practices used by ARI Registry Services on behalf of their clients in ARI Registry Services' capacity as a wholesale DNS hosting service provider.

1.1 Overview

Domain Name System Security Extensions (DNSSEC) has been proposed to add data integrity and authentication to the existing Domain Name System (DNS). The DNSSEC system asserts trustworthiness of data using a chain of public-private keys. For end users wanting to use DNSSEC enabled name servers, DNSSEC aware resolvers will be necessary to take advantage of the system.

RFC 4033, RFC 4034 and RFC 4035 should be read to gain a better understanding of DNSSEC.

1.2 Document name and identification

Document Name	DNSSEC Practice Statement
Version	1.0
Date Created	1 July 2014
Date Modified	12 July 2014

1.3 Community and applicability

The following stakeholders of this DNSSEC implementation have been identified:

Backend Operator	Technical services provider providing DNS functions to the Reseller.
Reseller	The entity that is utilising the DiscoveryDNS system.
Registrant	Owner of an individual zone.
Recursive Name Server Providers	For example, ISPs who provide their customers with name servers to use.
End users	Those accessing services supplied on the domain name.

Relationship between different entities is regulated through the following agreements:

Relationship	Agreement
Reseller and Backend Operator	DiscoveryDNS Reseller Agreement

1.4 Specification administration

1.4.1 Specification administration organisation

Organization	ARI Registry Services
Website	www.ariservices.com

1.4.2 Contact information

Name	Customer Support
Address	L8, 10 Queens Rd, Melbourne, Vic 3004, Australia
Number	+61 3 9090 1700
Email	support@discoverydns.com

1.4.3 Specification change procedures

Queries with regards to the content of this document may be made directly in writing via email, post or telephone to the contact listed. Some requests may only be made in writing via email or post and requestors may be notified to do so should they place the initial request via telephone.

ARI Registry Services reserves the right to amend the DNSSEC Practice Statement without notification. An updated or new DNSSEC Practice Statement will be published as specified in Section 2.

2 Publication and repositories

2.1 Repositories

ARI Registry Services publishes this DNSSEC Practice Statement at the following link: http://discoverydns.github.io/dnsapi-client/

2.2 Publication of public keys

DS records of SEP keys are made available to the Reseller via the API or web interface for publication in the parent zone. ARI Registry Services maintains a mailing list which will notify of policy changes specific to DNSSEC and will contain alerts in the event of an emergency key rollover.

Email	dnssec-announce@lists.ariservices.com

2.3 Access controls on repositories

Information that ARI Registry Services deems publically viewable is published on our website at www.ariservices.com. Other information may be requested by writing to the contact specified in Section 1.4.1. Provision of requested information is at the sole discretion of ARI Registry Services.

This document may refer to documents that are confidential in nature, or considered for internal use of ARI Registry Services. These documents may be made available on request after consideration on a case by case basis. ARI Registry Services reserves the right to deny access to confidential documents or documents classified for internal use only.

ARI Registry Services will take all the necessary measures to protect information and material that is of a secure nature with respect to DNSSEC. These measures will be commensurate with the nature of such information and material being secured.

3 Operational Requirements

3.1 Meaning of domain names

There are no restrictions on the meaning of domain names hosted in the ARI Registry Services DiscoveryDNS Reseller system.

3.2 Identification and authentication of Child Zone Manager

ARI Registry Services does not conduct any identification or authentication of the child zone manager. This is the responsibility of the Reseller.

3.3 Registration of Delegation Signing (DS) Resource Records

The chain-of-trust to the child zone is established by publishing a signed DS record into the relevant parent zone. Method to submit DS records into the relevant zone are registry dependent. Please consult with your Registrar for more information.

3.4 Method to prove possession of Private Key

Authentication of the DS record to be inserted into the hosted zones is the sole responsibility of the Reseller or Registrant. ARI Registry Services will publish whatever information is supplied to us by an appropriately authenticated Reseller.

3.5 Removal of DS Resource Record

The Reseller uses the API interface to remove the DS record.

4 Facility, management and operational controls

4.1 Physical controls

4.1.1 Site location and construction

The architecture consists of a primary site, a secondary site, and geographically dispersed DNS sites. The components at the secondary site are identical to those at the primary site.

ARI Registry Services chose data centres for operations after carrying out stringent checks and visits on a large number of available providers. Each data centre provides the following minimum set of requirements:

- Redundant Power Feed
- Un-interruptible Power Supply (minimum 30 minutes)
- Backup Power source (generator)
- Fire Detection System (High Sensitivity Smoke Detectors)
- Fire Suppression System
- Water Detection System
- Multiple (Diverse) Internet Links
- Stringent Physical Security (On-site security personnel, bio-metric access control)
- 24/7 Access Availability
- Robust Cooling System (HVAC)
- Real Time/Pro-active Power & Environmental Monitoring

4.1.2 Physical access

Access to all systems at each data centre is severely restricted. Equipment is located in private locked racks and keys to these are only given out to authorised administrators as part of stringent data centre security procedures.

Remote environment surveillance is employed, including cameras and entry alarms.

In addition, direct physical access to equipment is monitored and controlled as an un-trusted interface, login sessions are not permitted to idle for long periods, and network port security is employed to minimise the opportunity for a direct network connection to be used as a security threat vector.

4.1.3 Power and air-conditioning

N+1 power is utilised at all selected data centres to maximise uptime availability. Uninterruptible Power Supply (UPS) systems are used to prevent power spikes, surges, and brownouts, and redundant backup diesel generators provide additional runtime. Alerts are set on all power provision systems to allow ARI Registry Services to begin failover preparation in the event of a potential power provision issue to ensure a smooth and controlled failover if required.

Similarly N+1 monitored air conditioning at data centres is configured to provide maximum temperature control for the installed equipment in order to provide a stable operating environment.

4.1.4 Water exposures

ARI Registry Services has implemented reasonable measures for flood detection and protection at its sites, as well as having a key selection criterion for sites that they be in areas which are not likely to suffer flooding.

4.1.5 Fire prevention and protection

Fire protection in each data centre is world-class, with very early smoke detection apparatus installed and set as one element of a multi-stage, human controlled multi-zone dry-pipe, double-interlock, pre-action fire suppression system in a configuration that complies with local regulations and industry best practice.

4.1.6 Media storage

Sensitive media is stored offsite securely and is protected by access restrictions. Such media is reasonably protected from fire, water and other disastrous environmental elements.

4.1.7 Waste disposal

Sensitive documents are shredded before disposal. Where sensitive data is stored electronically, appropriate means are used to render the data unsalvageable prior to disposal.

4.1.8 Off-site backup

DNSSEC components and necessary data is stored off-site regularly as part of backup and disaster recovery. Such data is protected by reasonably secure means and has access restrictions that are similar to those implemented for online systems and data.

4.2 Procedural controls

4.2.1 Trusted roles

The following table presents all procedures that ARI Registry Services has implemented for providing DNSSEC services for the DiscoveryDNS Reseller DNS system. These procedures require corresponding roles as below:

Procedure	Roles
Key Rollover	
Key creation	Automated by the Reseller System
Disposal of old keys	Automated by the Reseller System
KSK rollover	Not Supported

4.2.2 Number of persons required per task

No human intervention is required.

4.2.3 Identification and authentication for each role

ARI Registry Services requires all personnel dealing with secure DNSSEC material and systems to have completed a National Police Check with the Australian Federal Police. ARI Registry Services reserves the right to interpret the findings of the National Police Check equitably with respect to the secure nature of this DNSSEC implementation as covered by the ARI Registry Services Human Resources Policy.

4.2.4 Tasks requiring separation of duties

Tasks that are part of a Key Rollover require separation of duties. Please refer to Section 4.2.1 for further information.

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Each person who fulfils a DNSSEC role must:

- Be employed full time by ARI Registry Services
- Not be within their initial employment probation period
- Have completed a National Police Check with the Australian Federal Police

4.3.2 Background check procedures

A National Police Check conducted by the Australian Federal Police must be completed prior to taking part in DNSSEC tasks.

4.3.3 Training requirements

Each person who is responsible for DNSSEC tasks must have attended an ARI Registry Services DNSSEC training session and be fully qualified to perform that function.

ARI Registry Services provides frequent retraining to its staff to assist them with keeping their skills current and enabling them to perform their job proficiently.

4.3.4 Job rotation frequency and sequence

ARI Registry Services rotates the responsibility for DNSSEC related tasks between staff that satisfy the skill set required to execute those tasks.

4.3.5 Sanctions for unauthorised actions

ARI Registry Services will conduct investigations where it detects or is made aware of unauthorised actions on the DNSSEC environment. The company will take necessary disciplinary action should such action be warranted.

4.3.6 Contracting personnel requirements

Contractors and consultants are not authorised to participate in secure DNSSEC tasks.

4.3.7 Documentation supplied to personnel

ARI Registry Services provides requisite training and support material to its staff to enable them to proficiently perform their duties. Supplied documentation is provided to staff under security controlled guidelines to ensure operational security.

4.4 Audit logging procedures

All systems deployed by ARI Registry Services utilise audit log functionality which is coordinated centrally. Logging is used to monitor the health of systems, trace any issues and conduct diagnosis.

4.4.1 Types of events recorded

A high level categorisation of events that are recorded is as follows:

Zone File Activity	Addition and removal of names. Changes in RRs associated with names in the zone.
Hardware Failures	Failure of server and network infrastructure or their components.
Access To Hardware	Changes in access controls granting physical, console and network access to infrastructure.
Security Profile	Changes in settings and configuration that determine the security of infrastructure or the services it provides.
System Updates	Updates to operating environment and packages on servers and firmware on network appliances.
Network Activity	Divergences from observed patterns of network activities.
Redundancy Failure	Failure in backups, DR or transitions between primary and secondary site.
Incident Management	Incidents being raised, allocated, acted upon and resolved.
Failure In Event Monitoring	Failure of event monitoring system. This would be detected using a secondary event monitoring system.

4.4.2 Frequency of processing log

Audit logs and event monitoring feed into the ARI Registry Services monitoring system that raises alerts based on states that are not normal in regular operations.

4.4.3 Retention period for audit log information

Audit log information is securely archived for a period of seven (7) years.

4.4.4 Protection of audit log

Audit logs are only available to ARI Registry Services employees with appropriate privileges. Audit logs do not contain private keys or other sensitive information that may lead to a compromise by using existing and known methods.

4.4.5 Audit log backup procedures

Audit logs are backed up as part of the backup procedures in place for production systems. Those logs containing sensitive data are stored in a secure manner. Disposal of audit logs is carried out in accordance with Section 4.1.7.

4.4.6 Audit collection system

In addition to information recorded manually by staff while conducting operations, Audit information is collected in Audit logs automatically. Methods specific to applications and operating environments are used to record audit logs.

Manual logs are scanned and the original documents archived in a fireproof safe.

4.4.7 Notification to event-causing subject

No notification is issued to the event causing subject as part of automatic event logging. However, selected events are monitored and alerts delivered to ARI Registry Services staff that may choose to notify event causing subjects.

During execution of manual procedures the participants are informed that logging is taking place.

4.4.8 Vulnerability assessments

ARI Registry Services engages an external entity to perform a vulnerability audit annually. This is in addition to monitoring and analysis that is in place for production systems. A broader annual compliance audit is also performed as discussed in Section 7.

4.5 Compromise and disaster recovery

4.5.1 Incident and compromise handling procedures

Any event that may cause or has caused an outage, damage to the system or disruption to service is classified as an incident. Any event that is an incident and has resulted in exposure of private DNSSEC components is classified as a compromise. Incidents are addressed using ARI Registry Services' incident management procedures.

Should ARI Registry Services detect or be notified of a compromise, ARI Registry Services will conduct an investigation in order to determine the nature and seriousness of the compromise. Following the investigation ARI Registry Services will take the necessary measures to re-instate a secure state. This may involve rolling over the ZSK(s), KSK(s) or both.

Incident management is conducted in accordance with the ARI Registry Services Incident Management process.

4.5.2 Corrupted computing resources, software, and/or data

Detection or notification of corrupted computing resources will be responded to with appropriate incident management procedures and escalation procedures as necessary.

4.5.3 Entity private key compromise procedures

An emergency ZSK and KSK rollover will be carried out in the event that ARI Registry Services detects or is notified of a private key compromise of either key. On suspicions of a compromise, ARI Registry Services will instigate an investigation to determine the validity of such suspicions. ARI Registry Services will notify the public through an update on the DNSSEC website and mailing list discussed in section 2.2, Publication.

4.5.4 Business continuity and IT disaster recovery capabilities

Business continuity planning and disaster recovery for DNSSEC is carried out in accordance with ARI Registry Services' Business Continuity and Disaster Recovery Policies, and contracts in place with the Registry Operator.

4.6 Entity termination

ARI Registry Services will ensure that should its responsibilities to manage DNS for the zone under consideration be terminated, it will provide all necessary information to facilitate the transition.

Should it be decided to return the zone to an unsigned position, ARI Registry Services will endeavour to carry it out in an orderly manner.

5 Technical security controls

This section provides an overview of the security policies and procedures ARI Registry Services has in place for the operation of DNSSEC within the Reseller system presented as a summary for purposes of this DNSSEC Practice Statement.

5.1 Key pair generation and installation

5.1.1 Key pair generation

The generation of KSK and ZSK is carried out automatically by the Reseller system at the time of requesting DNSSEC signing through the API. The Key Pairs are generated on a separate system not connected to the internet.

Key Pair Generation is an audited event and audit logs are recorded and kept in accordance with relevant policies.

5.1.2 Public key delivery

The DS is delivered to the parent zone by the Reseller.

The DNSKEY is published in the DNS zone.

5.1.3 Public key parameters generation and quality checking

Key Pairs are automatically generated by the system utilising pre-configured parameters. These parameters are configured by an ARI Registry Services staff member in accordance with Section 4.2.1. Quality of the parameters is examined as part of ARI Registry Services' standard change control procedures.

5.1.4 Key usage purposes

Keys will be used in accordance with the DNSSEC implementation defined in this DNSSEC Practice Statement and other relevant documents such as agreements stated in Section 1.3. The keys are not exported from the signing system in an unencrypted form and are only exported for backup and disaster recovery purposes.

5.2 Private key protection and cryptographic module engineering controls

All cryptographic operations are carried out within the signing system. The private components of keys stored on the signing system are exported in encrypted forms only for backup and disaster recovery purposes.

5.2.1 Cryptographic module standards and controls

Systems used for cryptographic functions must be able to generate acceptable level of randomness.

5.2.2 Private key backup

Private components of keys used for the zone are backed up in an encrypted format in accordance with ARI Registry Services backup and disaster recovery policies.

5.2.3 Private key storage on cryptographic module

Private keys are stored on the signer system and restricted to be only accessible to signing functions.

5.2.4 Private key transfer into or from a cryptographic module

There are no circumstances under which a private key would be transferred into the signing systems. In accordance with Section 4.6 and in consultation with the relevant stakeholders, a private key can be transferred out of these systems. The private key will be transferred to the relevant stakeholder in encrypted form unless specifically requested otherwise by that stakeholder.

5.2.5 Method of activating private key

Keys are activated during a key rollover automatically by the Reseller System.

5.2.6 Method of deactivating private key

A private key is deactivated by removing all signatures that deem the key valid and subsequently removing the DNSKEY record from the zone. This is also performed as an automated action by the Reseller System.

5.2.7 Method of destroying private key

ARI Registry Services destroys keys by securely removing them from the signing system. However, encrypted backups of the keys are not destroyed but rather archived as described in Section 5.2.3.

5.3 Other aspects of key pair management

5.3.1 Public key archival

Public components of keys are archived as part of backups and disaster recovery procedures.

5.3.2 Key usage periods

Item	Value
KSK	Indefinite
ZSK	90 days
Signature validity periods	30 days

Keys that have been superseded are not used to sign resource records.

5.4 Activation data

Activation data is securely generated and is protected by a confidentiality agreement between ARI Registry Services and stakeholders that hold activation data. Activation data is decommissioned by destroying, invalidating or by using another suitable method applicable to the type of data.

5.5 Computer security controls

ARI Registry Services limits access to production servers and only authorised staff members from the IT department are allowed privileged access. Access may be extended to other personnel for valid business reasons.

Authentication methods are complimented with network security measures. Passwords are rotated regularly and best practices such as tiered authentication and two factor authentication are implemented where appropriate.

5.6 Network security controls

Networks for secure DNSSEC infrastructure are segregated using firewalls. Audit logs are kept for all sensitive DNSSEC operations and archived for investigative purposes should security breaches be suspected or detected. Systems are divided into their applicability (e.g. frontend and backend) and user

and application access to them is restricted using appropriate means. Production infrastructure is logically separated from non-production infrastructure to limit access at a network level in accordance with ARI Registry Services security policies.

5.7 Time stamping

Timestamps are used for:

- Audit logs generated manually and automatically
- DNSSEC signatures.

ARI Registry Services synchronises its timeservers with stratum 2 or 3 timeservers. All manually recorded times are stated in time that is local to the location of record. All automatically recorded times are in UTC.

5.8 Lifecycle technical controls

5.8.1 System development controls

All ARI Registry Services software deployed on production systems is maintained in version controlled repositories. ARI Registry Services implements rigorous change control systems for production infrastructure.

5.8.2 Security management controls

ARI Registry Services monitors its system for access, configuration changes, package installs and network connections in addition to other critical metrics that can be used to detect suspicious activities. Detailed audit logs enable ARI Registry Services to trace any transaction on its systems and analyse events.

5.8.3 Lifecycle security controls

ARI Registry Services implements fully redundant signing infrastructure and contracts with hardware manufacturers to provide four (4) hour business day turnaround on support.

All production infrastructure and software is thoroughly tested before being deployed. Source code of all software deployed to production systems is authenticated and verified.

6 Zone Signing

6.1 Key lengths, key types and algorithms

ARI Registry Services uses a split key signing method. The RSA algorithm with a key length of 2048 bits is used for the KSK and 1280 bits is used for the ZSK.

6.2 Authenticated denial of existence

NSEC is used to provide authenticated denial of existence.

6.3 Signature format

Signatures are generated using SHA256 hashes.

6.4 Key roll-over

The ZSK rollover is every 90 days using a pre-publish method.

KSK considered cryptographically secure enough that the complexities and risks of the multiparty rollover are not necessary, thus the KSK is never rotated.

6.5 Signature Lifetime and Re-Signing Frequency

Signatures are valid for 30 days. Signatures are automatically regenerated every 50% to 75% of this time.

6.6 Verification of resource records

Validity checks are made against the zone as part of ARI Registry Services' standard monitoring process. This includes verifying DNSSEC material.

All resource records are validated by the system before delivery to be signed and distributed into the zone file.

6.7 Resource records time-to-live

TTL for each DNSSEC Resource Record in seconds:

DNSKEY	3600
DS	3600
NSEC	600
RRSIG	Same as covered Resource Record

7 Compliance Audit

An audit for DNSSEC operations is performed annually in in conjunction with our ISO 27001:2006 audit.

7.1 Frequency of entity compliance audit

Compliance audits are conducted annually at the sole expense of ARI Registry Services.

7.2 Identity/qualifications of auditor

ARI Registry Services' compliance audits are performed by independent auditors.

7.3 Auditor's relationship to audited party

Compliance audits of ARI Registry Services' operations are performed by independent auditors. Third party auditors do not participate in the multi-person control for any tasks, as stated in Section 4.2.1.

7.4 Topics covered by audit

The scope of ARI Registry Services' annual Compliance Audit includes all DNSSEC tasks as stated in Section 4.2.1.

7.5 Actions taken as a result of deficiency

Action items that are raised as a result of compliance audits are presented to ARI Registry Services' management for consideration. ARI Registry Services' management will investigate and implement corrective actions should they determine them to be necessary.

7.6 Communication of results

A report of the audit results to will be published at www.ariservices.com no later than thirty (30) days after the audit.

8 Legal Matters

8.1 Fees

Not applicable.

8.2 Financial responsibility

Not applicable.

8.3 Confidentiality of business information

8.3.1 Scope of confidential information

The following information is kept confidential and requires privileged access as controlled by ARI Registry Services policy:

- Secure DNSSEC information
- Audit logs
- Reports created by auditors
- Procedures
- Policies that relate to security

8.3.2 Types of information not considered confidential

Information that is classified as public as part of the DNSSEC extensions to DNS are considered to be public by ARI Registry Services and will not be subject to access restriction.

8.3.3 Responsibility to protect confidential information

ARI Registry Services is committed to the confidentiality of information and takes all measures reasonably possible to prevent the compromise of such information.

8.4 Privacy of personal information

8.4.1 Information treated as private

Not applicable.

8.4.2 Information not deemed private

Not applicable.

8.4.3 Responsibility to protect private information

Not applicable.

8.4.4 Disclosure pursuant to judicial or administrative process

ARI Registry Services shall be entitled to disclose confidential/private Information if ARI Registry Services believes that disclosure is necessary in response to judicial, administrative, or other legal process.

8.5 Limitations of liability

ARI Registry Services to the extent permitted by law excludes liability for any losses, direct or indirect, punitive, special, incidental or consequential damage, in connection with or arising out of this DNSSEC Practice Statement or the actions of it or any third party (including for loss of profits, use, data, or other economic advantage), however it arises, and even if ARI Registry Services has been previously advised of the possibility of such.

8.6 Term and termination

8.6.1 Term

This DNSSEC Practice Statement becomes effective upon publication with the most current version being published at the following link: http://discoverydns.github.io/dnsapi-client/

8.6.2 Termination

This DNSSEC Practice Statement will be amended as required 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.

With the exception of injunctive or provisional relief, disputes involving ARI Registry Services require an initial negotiation period of no less than sixty (60) days prior to the commencement of legal action.

Subject to the foregoing, any legal action in relation to this DNSSEC Practice Statement against any party or its property may be brought in any court of competent jurisdiction in the State of Victoria, Australia and the parties irrevocably, generally and unconditionally submit to the nonexclusive jurisdiction of any court specified in this provision in relation to both itself and its property.

8.6.4 Governing law

This DNSSEC Practice Statement shall be governed by and construed under the law in the State of Victoria, Australia.

9 Glossary

Acronym	Expansion
DNS	Domain Name System
DNSKey	Resource record containing a public key
DNSSEC	Domain Name System Security extensions
DP	DNSSEC Policy
DPS	DNSSEC Practice Statement
DS	Delegation Signer
SEP	Secure Entry Point
ISP	Internet Service Provider
KSK	Key Signing Key
NSEC	Next Secure
NSEC3	Next Secure with hashes for next secure domain
RFC	Request For Comments
RR	Resource Record
RRSIG	Resource Record Signature
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
ZSK	Zone Signing Key

Definitions

We, us and our means any or all of the Bombora Technologies Pty Ltd group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Disclaimer

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

Confidentiality Notice

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

Trademarks Notice

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.

Pricing Notice

Any information or pricing provided in this document is subject to change without notice. Whilst we have compiled this document in good faith, based on what we believe is accurate and up-to-date information, it is possible that the pricing or other information contained in this document may require amendment due to changing market or other circumstances (including product discontinuation, manufacturer price changes, errors, or insufficient or inaccurate information having been provided by the recipient of this document or others, and other external circumstances). Additional charges may also apply for work that is out of scope.

The pricing in this document is based on our standard terms and conditions and is valid for a period of thirty (30) days from the date of this document.

ARI REGISTRY SERVICES