1. INTRODUCTION

A Domain Name System Security Extension (DNSSEC) Policy and Practice statement (DPS) defines the policy, practices and summarises procedures an entity uses to sign and manage a Domain Name System (DNS) Zone.

The document is intended to provide information on how .au Domain Administration LTD (auDA) will implement and manage the .au Key Signing Keys (KSK) and Zone Signing Keys (ZSK) for the Australian (.au) top level domain.

The information contained in this document is to assist stakeholders in determining the level of confidence and trust they wish to confer in auDA and the .au top-level domain.

This DPS is based on the IETF RFC 6841, A Framework for DNSSEC Policies and DNSSEC Practice Statements

1.1. Overview

The DNS is described in RFC 1034 and RFC 1035.

DNSSEC is described in RFC 4033, RFC 4034 and RFC 4035 and is a set of specifications that add security to the DNS.

DNSSEC provides a mechanism to validate DNS data to prove that it has not been modified during transit over the Internet. This is achieved by incorporating public key cryptography into the DNS hierarchy, forming a chain of trust originating at the root zone.

1.2. Document name and identification

Document Title	DNSSEC Policy and Practice Statement
Version	2
Date Created	1 June 2013
Date Last Modified	5 July 2018

Deleted: 1

Deleted: 1 May 2

1.3. Community and applicability

This DPS applies exclusively to the .au zone. It describes the procedures and security controls applicable when managing and employing keys and signatures for the signing of the .au zone

auDA is responsible for the country code Top Level Domain (ccTLD) .au. Direct registrations at the second level are not permitted. The table below identifies the current Second Level Domain (2LD) delegations within the .au zone and the 2LD Registry Operator responsible for the delegated zone.

Zone	2LD Registry Operator	Status of Zone
.asn.au	Afilias Australia Pty Ltd	Open
.act.au	Afilias Australia Pty Ltd	Open
.com.au	Afilias Australia Pty Ltd	Open
.conf.au	Afilias Australia Pty Ltd	Open
.csiro.au	CSIRO (Commonwealth Scientific and Industrial Research Organisation)	Restricted within CSIRO
.edu.au	Afilias Australia Pty Ltd	Restricted to the Education Sector
.gov.au	Afilias Australia Pty Ltd	Restricted to the Government Sector
.id.au	Afilias Australia Pty Ltd	Open
.net.au	Afilias Australia Pty Ltd	Open
.nsw.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.nt.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.org.au	Afilias Australia Pty Ltd	Open
.oz.au	Kevin Robert Elz	Open
.qld.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.sa.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.tas.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.vic.au	Afilias Australia Pty Ltd	Restricted to Community Groups
.wa.au	Afilias Australia Pty Ltd	Restricted to Community Groups

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

Deleted: Pty Ltd

auDA is responsible for

- Generating KSK and ZSK key pairs for signing the .au zone.
- Protecting the confidentiality of the KSK and ZSK private components used to sign the .au zone.
- Signing all authoritative DNS resource records in the .au zone.
- Providing and maintaining the DS resource record in the root zone.
- Facilitating necessary additions, updates and removals of entries within the .au zone file with respect to the zones listed above.
- Providing a process for each 2LD Registry Operator to submit their respective zones' DS resource record.
- Validating a 2LD Registry Operator's DS record prior to publishing it into the .au zone.
- Providing a policy for Emergency Key Rollovers for the 2LD Registry Operators.
- Performing Emergency Key Rollover at the request of a 2LD Registry Operator.

2LD Registry Operator

In .au each 2LD Registry Operator is responsible for:

- Generating KSK and ZSK key pairs for signing their delegated zone.
- Protecting the confidentiality of the KSK and ZSK private components used to sign their delegated zone.
- Signing all authoritative DNS resource records within their delegated zone.
- Providing the applicable DS resource record to the .au zone manager.
- Facilitating necessary additions, updates and removals for entries within their delegated zone.
- Providing a mechanism for each Registrar to submit a Registrant's DS resource record into the applicable zone.
- Providing a policy for Emergency Key Rollovers.
- Performing Emergency Key Rollovers at the request of a Registrar.

Registrars

Registrars act as an agent for a Registrant. A Registrar is granted direct access to a 2LD Registry Operator's database via a Registrar agreement. All change requests made by a Registrant must be made via a Registrar.

The Registrar is responsible for:

- The administration and management of domain names on behalf of the Registrant.
- Identifying Registrants prior to accepting change requests.
- Enabling Registrants to submit DS resource records into the applicable registry.
- Providing a policy for Emergency key rollovers.
- Performing Emergency Key Rollovers at the request of a Registrant.

Registrants

The Registrant is a physical or legal entity that controls a domain name. Upon approval of a .au Domain Name Application Registrants enter into a binding and enforceable agreement with the Registrar and auDA.

Registrants are responsible for:

- Generating KSK and ZSK key pairs for signing their delegated zone.
- Protecting the confidentiality of the KSK and ZSK private components used to sign their delegated zone.
- Signing all authoritative DNS resource records within their delegated zone.
- The registration and maintenance of DS resource records through their Registrar.

Registrants may choose to delegate the responsibility of key management and signing to a registrar or third-party zone operator.

Relying Party

A relying party is the entity that makes use of DNSSEC signatures, such as DNSSEC validators and other applications. auDA will only publish DS Resource Records in the root zone and does not recommend a relying party configure static Trust Anchors. Any relying party who creates a Trust Anchor from the DS Resource Record does so at their own risk. auDA is not responsible for any failures that occur due to static Trust Anchor configurations. auDA does not comply with or utilise RFC 5011

1.4. Specification administration

This DPS is a living document, it will be periodically reviewed and updated as appropriate.

1.4.1. Specification administration organization

.au Domain Administration Ltd (auDA)

1.4.2. Contact Information

Name	Chief Technology Officer
Address	Level 17, 1 Collins St, VIC, 3053
Telephone	+61 (0) 3 83414111
Fax	+61 (0) 3 83414112
Email	info@auda.org.au
Web	https://www.auda.org.au/
ABN	38 079 009 340

1.4.3. Specification change procedures

Enquiries regarding this DPS may be made in writing, via email, fax or post.

Changes to the DPS that are approved by auDA will result in a new version of the document being released. New versions of the DPS will be available at the repositories listed in Section 2.

Only the most recent version of the DPS will be applicable. All changes identified in a review will be implemented within 3 months of the latest version's publication date.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

auDA publishes the current version of the DPS at https://www.auda.org.au/policies. All other related DNSSEC information is available on the auDA website at https://www.auda.org.au/dnssec.

No other repositories will be used.

2.2. Publication of public keys

auDA publishes the KSK public key as a DNSKEY record within the .au zone and as a Delegation Signer (DS) record in the parent (root) zone. The DS record is a hash of the corresponding DNSKEY record; this hash is consistent with the format of a DS resource record as described in RFC 4034.

2.3. Access Controls on Repositories

This document may refer to other documents that are for internal use only and are considered confidential in nature. auDA will review the need to provide these documents to a third-party request on a case-by-case basis. auDA reserves the right to refuse a request to documents.

All documents classified as publicly viewable will be available in the repositories listed in Section 2.1.

2.4. Notification Services

Notifications relevant to DNSSEC within the .au zone will be distributed via a mailing list operated by auDA, dnssec-announce@lists.auda.org.au.
This list is open to all users of the Internet and subscription information can be found at
https://www.lists.auda.org.au/mailman/listinfo/dnssec-announce

3. OPERATIONAL REQUIREMENTS

auDA will only accept DS resource records for inclusion in the .au zone from 2LD Registry Operators as listed in Section 1.3.

3.1 Meaning of a Domain name

Valid domain names in the .au name space are regulated by policy. auDA polices are developed using open and transparent advisory panels, committees and consultative groups that represent a broad sector of Internet users in .au.

Further information about auDA policy, policy reviews and policy panels can be found at https://www.auda.org.au/policies.

3.2 Identification and authentication of child zone manager

2LD Registry Operators are identified via contract or agreement whereby auDA has delegated responsibility to a 2LD Registry Operator for a specific child zone. A list of 2LD Registry Operators and their delegated zones can be found in Section 1.3.

Change requests made by 2LD Registry Operators are done using the appropriate method for that specific child zone. This may include in and out-of-band communication, confirmation of change requests from multiple personnel within a 2LD Registry Operator and the use of digital signatures.

3.3 Registration of delegation signer (DS) resource records

auDA provides each 2LD Registry Operator with a document that contains information regarding the process for submitting a change request (including adding and removing DS records) to auDA for inclusion in the .au zone.

The DS record provided by a 2LD Registry Operator is vetted by an auDA DNSAdmin and incorporated into an auDA change request, which then requires administrative authorisation prior to being included in the .au zone.

The DS resource record must be valid and submitted in the DS RR Presentation Format as described in RFC 4034. As part of the vetting process the DS record is checked against the child zones DNSKEY keyset and signatures.

3.4 Method to prove possession of private key

auDA verifies all change requests submitted by a 2LD Registry Operator prior to inclusion in the .au zone file by validating

- The DS records provided are available as DNSKEY records at the apex of the child zone.
- The DNSKEY matching the supplied DS has been used to sign and can validate a ZSKs DNSKEY.
- The DNSKEY matching the supplied DS has its SEP bit set.
- The Signature validity period is not due to expire.

If a DS resource record does not validate, auDA will verbally confirm the authenticity and intention of publishing the DS resource record with the 2LD Registry Operator.

3.5 Removal of DS resource records

3.5.1 Who can request removal

The removal of DS records from the .au zone, either active or expired, can only be requested by a 2LD Operator of that zone.

3.5.2 Procedure for removal request

auDA provides each 2LD Registry Operator with a document that contains information regarding the process for submitting a change request (including adding and removing DS records) to auDA for inclusion in the .au zone.

The request for removal of a DS record from a 2LD Registry Operator Zone is vetted by an auDA DNSAdmin and incorporated into an auDA change request, which then requires administrative authorisation prior to being removed in the .au zone.

Upon receiving the request and authentication of the requester, the DNSAdmin will conduct checks to confirm the removal of the relevant key from the 2LD Registry Operators zones DNSKEY RRset as part of the vetting process. The DS record will not be removed if the corresponding DNSKEY is still present in the 2LD Registry Operators zone.

3.5.3 Emergency removal request

If a 2LD Registry Operator is unable to produce a valid DNSSEC zone they may request an emergency removal of the DS resource record. A request can be made as per Section 3.5.2 but must be clearly identified as an emergency. All emergency requests will be treated with the highest priority and actioned within 48 hours.

The total removal of all DS records would be treated as an emergency removal request and should be submitted as such.

4 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1 Physical Controls

Physical controls are in place to prevent unauthorised access to signing systems. These include but are not limited to:

- Two-factor authentication
- Video and sensor monitoring
- Onsite security personnel
- Multi layered access restrictions
- Tamper evident bags for storage of physical materials and documents

4.1.1 Site location and construction

DNSSEC signing operations are conducted in physically secure environments. Each site has multiple layers of physical security implemented, is built using materials designed to prevent unauthorised access and is monitored using video and motion sensors. Equipment is housed in secured racks, which are also monitored for activity.

4.1.2 Physical access

Physical access is restricted and limited to authorised personnel. Third parties, including co-location staff, are not permitted access to racks containing auDA equipment without the authorisation of authorised auDA personnel.

4.1.3 Power and air conditioning

Facilities of operational signing systems must have:

- Redundant Power Feed
- Uninterruptible Power Supply (UPS)
- Backup Power source (generators)
- Robust Cooling System (HVAC)
- Each of these systems must be a minimum of N+1 for redundancy purposes.

4.1.4 Water exposures

auDA evaluates each facility to ensure it is not in a flood-prone area. Facilities are also fitted with Fire Suppressions Systems that do not use water and thereby further reduce the risk of water exposure.

4.1.5 Fire prevention and protection

All facilities are equipped with fire detection devices and all datacentres are fitted with gas fire suppression systems. Detection measures are designed to comply with local safety regulations.

4.1.6 Media storage

Media used for the backup of key material is encrypted and stored in auDA access controlled facilities. This media is protected by access restrictions.

4.1.7 Waste disposal

Sensitive documents and data storage media are shredded before disposal. Media used to collect or transmit sensitive information are rendered unsalvageable before disposal. Where cryptographic devices are used, they are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

4.1.8 Off-site backup

auDA performs regular backups of critical data, audit logging data and other sensitive information for disaster recovery. All data is encrypted and stored off-site in a secure storage facility with appropriate physical and logical access controls.

4.2 Procedural controls

4.2.1 Trusted roles

The following trusted roles exist for providing DNSSEC services for the .au zone in an M of N approach. Where a minimum of M trusted personnel is required to complete a trusted role and where M is never equal to 1.

- DNSAdmin
- Security Officer
- Operator

All changes are authorized, documented and signed off by a minimum of 2 trusted personnel.

4.2.2 Number of persons required per task

auDA ensures multiple trusted persons are required to perform the duties of a trusted role. Each task requires an M of N approach, where M is a minimum of a total group of N candidates. Each trusted person is provided documentation that defines his or her roles and responsibilities.

A trusted person may be required to perform any of the following tasks:

HSM configuration	Security Officers & Operators
HSM backups	Security Officers & Operators
HSM initialisation or restoration	Security Officers & Operators
Key generation	DNSAdmin, Security Officers & Operators
Key removal	DNSAdmin, Security Officers & Operators
Destruction of key material or physical media	DNSAdmin, Security Officers & Operators

4.2.3 Identification and authentication for each role

auDA verifies a trusted person's identity through personal (physical) presence. All trusted personnel must have completed a Police Check with the relevant state Police. auDA reserves the right to assign a trusted role based on the findings of the Police Check.

4.2.4 Task requiring separation of duties

As each aspect of the signing system requires M of N authentication, and where the M is never equal to 1, it is unnecessary for any task to require separation of duties.

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

To fulfil a trusted role auDA will chose candidates who are known by auDA to have:

- Demonstrated appropriate background knowledge and understanding of DNS and DNSSEC principles.
- Have sufficient experience, and where applicable, qualifications in the DNS industry.
- Have completed a Police Check with the relevant state Police.

Where an auDA staff member is to fulfil a trusted role, they must have been employed full time with auDA for more than 6 months.

Where non-auDA personnel fulfil a trusted role, the trusted person will have been involved with auDA for a minimum of three years. This may include participation in panels, committees, board appointments and contract work.

4.3.2 Background check procedures

All trusted persons are subject to a Police Check with the relevant state Police. Applicants must disclose previous employments in the last 5 years and provide references for validation when requested. Trusted persons will be re-checked every 5 years.

4.3.3 Training requirements

auDA will provide DNSSEC training to each trusted person that is specific to his or her assigned trusted role. All trusted personnel must complete annual retraining for their assigned trusted role to ensure that such persons maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. All trusted persons are required to have an understanding of how the DNS works, auDA's role in the DNS and the role of DNSSEC in the DNS.

4.3.4 Job rotation frequency and sequence

Trusted persons are rotated and replaced as and when required.

4.3.5 Sanctions for unauthorized actions

Disciplinary actions will be undertaken for unauthorized actions with respect to this DPS and/or other violations of auDA policies and procedures. Disciplinary actions may include:

- Measures up to and including termination.
- Damage liability.
- Prosecution.

Disciplinary action will be assessed with the frequency and severity of the unauthorized actions.

4.3.6 Contracting personnel requirements

auDA uses a combination of auDA employees and non-auDA personnel to fulfil trusted roles. Non-auDA personnel are required to meet the criteria listed in Section 4.3.

Non-auDA personnel are always accompanied and observed by a minimum of two auDA employees who hold one or more trusted roles.

4.3.7 Documentation supplied to personnel

Trusted personal will be provided HSM procedural documentation and a checklist for use during interaction with the HSM. Checklists are signed, dated and then digitally stored for audit purposes

4.4 Audit logging procedures

4.4.1 Types of events recorded

auDA maintains logging to a centralised logging server for analysis. auDA will log a minimum of:

- Key generation/destruction/export/import.
- HSM access/backup/restoration.
- Successful/Unsuccessful zone signing events.
- Hardware failures.
- Successful and unsuccessful system access.
- File modification.

Zone edits require a change request form be completed and authorised. Additionally, zone edits and comments for the .au zone file are versioned using a repository that includes a description of the change, the requester of a change, who authorised the change and who performed the change. This information is backed up as per the auDA Information Security Standard.

Deleted: backup procedure

Procedures requiring paper logs are signed at the completion of each step by each of the trusted persons involved. The paper logs are scanned and stored digitally; paper copies are then stored in a fireproof safe.

4.4.2 Frequency of processing log

Logs are reviewed during and after key signing and key rollovers. auDA also reviews its logs in response to alerts/notifications triggered during operational activities.

4.4.3 Retention period for audit log information

Logs are retained for a minimum of 12 months.

4.4.4 Protection of audit log

System generated audit logs are configured to generate/append to local and external log files. External logging occurs over encrypted mediums. Systems containing audit logs are housed in secure facilities with restricted physical and logical access.

Only authorised Trusted Persons are permitted to view or handle audit logs and each request is logged and authorised. Trusted persons with access to audit logs are not permitted to modify or delete the audit records.

Paper logs require signatures for each step of completion. If comments are required, these are marked at the end of line to prevent further addition of information. Paper logs are then scanned and stored electronically.

Logs do not contain sensitive information, such as private keys, which may be used to compromise the DNS.

4.4.5 Audit log backup procedures

Internal and external systems that contain audit log material are backed up as part of the auDA Information Security Standard.

Deleted: backup policy

4.4.6 Audit collection system

All system-generated audit data that is recorded at the application, network, and operating system level are output to log files that are stored locally and externally on a centralised log server. Audit data that is recorded on paper is done so by auDA personnel and is archived in a fireproof safe. Each piece is then scanned and stored electronically.

4.4.7 Vulnerability assessments

auDA performs vulnerability scans regularly on all production systems. Monitoring is in place to alert IT staff of events that have the potential to affect the stability and security of the DNS.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and compromise handling procedures

In the event of a security incident, or a potential compromise, auDA will contain the breach, then conduct an investigation to determine the cause and vector of the breach.. If the breach relates to a private key, the emergency key rollover procedure will be performed. Incidents are addressed as per the Incident Response section of the auDA Information Security Standard.

Deleted: Policy

4.5.2 Corrupted computing resources, software, and/or data

Corruption of computing resources, software and/or data will require auDA staff to investigate and identify the cause. The level of impact will be determined and appropriate action will be developed based on the severity in accordance with the auDA incident management procedure.

All signing-related hardware is covered by vendor maintenance contracts and where the cause is determined to be hardware failure it will be replaced as per the contractual agreement with the vendor. auDA maintains (and tests) redundancy on all signing-related hardware to assist in minimising down time during hardware replacement.

When a computing system, is identified as corrupted or has failed, auDA will restore the system from the most recent unaffected backup. Backups will be verified prior to being deployed. If data corruption occurs auDA will restore files or entire systems to the most recent unaffected backup.

Notifications, and any incident reports deemed publicly-viewable, of an incident that causes impact to the .au domain space will be made available via the channels listed in Section 2.

4.5.3 Entity private key compromise procedures

In the event auDA detects or is notified that the KSK private component has been compromised, auDA will activate the Emergency Key Roll Over procedure. This document details the steps required to successfully perform a KSK rollover, including but not limited to:

- Generating a new KSK

- Signing the ZSK with the new KSK
- Adding the new KSK DS to the root zone
- Removal of the compromised KSK

Notifications will be made in accordance with Section 2.

4.5.4 Business continuity and IT disaster recovery capabilities

Business continuity and disaster recovery planning is documented in the auDA Information Security Standard and the auDA Business Continuity & Disaster Recovery Policy.

Deleted: Policy

Private key material is stored on dedicated equipment that is sensitive to temperature, voltage, movement and interference. Private key material is destroyed and rendered unrecoverable if any of these thresholds are met. In addition, private keys are backed up and maintained in accordance with DPS section 5.2.4 and can be restored to standby hardware within 48 hours.

4.6 Entity termination

If auDA is removed as the administrator of the .au zone, the auDA trusted personnel will co-operate with the new party/parties to facilitate a smooth transition. The new Administrator would be responsible for maintaining the state of the .au zone.

If auDA was to discontinue using DNSSEC, a plan would be implemented and all notifications regarding the return to an unsigned zone will be provided as per Section 2.

5 TECHNICAL SECURITY CONTROLS

5.1 Key pair generation and installation

5.1.1 Key pair generation

The private component of the KSK and ZSK key pairs are generated using a Hardware Security Module (HSM). The DNSAdmin is responsible for generating key pairs in accordance with the Key Signing Key, Zone Signing Key and RRSIG Generation and Validity Period documents.

Key generation requires all key generation activities to be logged and all changes are subject to administrative review and authorisation before being included in the .au zone file.

5.1.2 Public key delivery

The public component of each generated KSK is published as per Section 2.2.

The DS is delivered to the parent zone as per the IANA procedures listed at https://www.iana.org/help/nameserver-requirements.

The public component of each generated ZSK is published in the .au zone as a DNSKEY record.

5.1.3 Public key parameters generation and quality checking

Key generation is performed in accordance with the relevant auDA key generation procedures. Procedures clearly identify the parameters required for the specific key being generated. The DNSAdmin is responsible for validating the parameters before submitting the changes as part of the auDA change request procedure. The change request procedure requires multiple parties to review and authorise the changes before they can be applied

5.1.4 Key usage purposes

Keys are generated for the use of signing the .au zone and not for any other purpose outside of the signing system. Where keys are required to be exported, for backup and disaster recovery purposes, they are only exported in encrypted format with dual-authorisation security.

5.2 Private key protection and cryptographic module engineering controls

All cryptographic operations are performed in an HSM and no private keys are made available, unprotected, outside of the HSM.

5.2.1 Cryptographic module standards and controls

The signing system uses a HSM, which conforms to the requirements in FIPS 140-2 level 3.

5.2.2 Private key (M-of-N) multi-person control

Access to the signer system is restricted to trusted personnel in trusted roles as identified in Section 4.2.1. M of N multi person control is implemented as identified in Section 4.2.2.

5.2.3 Private key escrow

For the purpose of this document, escrow is defined as the export of private key material so as it may be held by an escrow agent or third party. Backups of the private key material for the purpose of disaster recovery by auDA are not considered an escrow procedure.

auDA does not escrow the private key material to an escrow agent or third party.

5.2.4 Private key backup

auDA performs backups of the .au ZSK and KSK private keys after each new key pair is generated. Backups are performed using hardware specific smart cards that are encrypted and passcode protected. Both the backup and restoration of the private keys requires dual authorisation.

5.2.5 Private key storage on cryptographic module

Private components of keys used for the zone are stored on a HSM in an encrypted format.

5.2.6 Private key archival

Private keys are archived on the HSM for a minimum of 2 months but no greater than 18 months after rollover. Private keys can also be restored from backups as listed above.

5.2.7 Private key transfer into or from a cryptographic module

Keys are transferred to and from a HSM in an encrypted format using hardware specific smart cards that are encrypted and passcode protected. Transfer occurs only during backup or restoration of private key material and is performed by trusted personnel, as defined in section 4.2.1

5.2.8 Method of activating private key

Private keys are activated by configuring an activation and publication date when generating the relevant key pair. These dates are verified during the quality checking detailed in Section 5.1.3

5.2.9 Method of deactivating private key

The deactivation of a private key is set using the deletion date parameter during its creation. This date is verified during the quality checking detailed in Section 5.1.3. Once deactivated, the keys are removed from the .au zone and no longer used to generate signatures for records within the zone.

5.2.10 Method of destroying private key

The DNSAdmin is responsible for destroying private key material in accordance with the auDA removal, deletion and destruction of key material procedure. The zeroization function of the HSM is used to destroy the private key material.

auDA will take all reasonable precautions to ensure that there are no residual remains of the keys that could lead to the reconstruction of the keys.

5.3 Other aspects of key pair management

5.3.1 Public key archival

KSK public keys are backed up and archived for a minimum of 2 months but no greater than 18 months.

5.3.2 Key usage periods

auDA will only publish the public keys that are current to the operation of the .au zone. Key operational periods and usage is defined in Section 6. Rollover start and end dates will be announced as per section 2 of this document. A deactivated key will never be reused to sign a resource record.

5.4 Activation data

5.4.1 Activation data generation and installation

Activation data is generated during the initial activation of the HSM. Backups of activation data are maintained in a separate secure facility and are protected by AES256 encryption. Hardware specific cards are allocated to trusted personnel as per the HSM Smart Card Policy and Replacement document. Allocations are documented and logged.

5.4.2 Activation data protection

Trusted persons must protect credentials used to access and activate the HSM with a PIN. Trusted persons are supplied documentation specific to their trusted role and which includes requirements for safe guarding their PIN and protecting the integrity of their credentials.

5.4.3 Other aspects of data protections

Management of hardware specific smart cards, including policy and processes for:

- lost, stolen or damaged cards

- issuing replacements cards
- destruction of expired cards
- protection and storage of cards

is detailed in the HSM Smart Card Policy and Replacement document and will be supplied to trusted persons.

5.5 Computer security controls

All production computer systems are housed in secure facilities. auDA ensures the systems maintaining key software and data files are secure from unauthorized access. auDA limits access to production systems to those individuals identified in Section 4.2.

All access, physical and remote, to computer and signing systems, successful and unsuccessful, are monitored and logged.

5.6 Network security controls

The HSM is directly connected to a secured server and is not directly network accessible via LAN or Internet. This secure server is protected by a firewall. Audit logs are kept and archived for investigative purposes.

5.7 Time stamping

auDA uses trusted time sources within the signing system network to synchronise system clocks.

5.8 Life cycle technical controls

auDA tests all new sources of software in a lab environment prior to deploying to production servers. Lab and production systems are logically separated. Systems are evaluated prior to being deployed, to maintain the quality and security of the DNS in .au.

auDA has technologies and policies in place to control and monitor the configuration of its systems, this includes monitoring of access on all systems, configuration changes and package install or updates.

The HSM 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 HSM will be procured directly from the manufacturer and transported in tamper-evident bags to their destination in the secure facility. All hardware will be decommissioned before the specified lifetime expectancy.

6 ZONE SIGNING

6.1 Key lengths, key types and algorithms

Key pairs are required to be of sufficient length to prevent others from determining the key pair's private key using crypto-analysis during the period of expected utilization of such key pairs. Key algorithms and length are defined in internal key generation documents and reviewed annually in line with current industry best practice.

6.2 Authenticated denial of existence

The contents of the .au zone file are small and well known. For this reason auDA will use NSEC records as specified in RFC 4034

6.3 Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA-256 (RSA/SHA-256, RFC 5702).

6.4 Key roll-over

Due to the size and algorithm used for the KSK auDA has determined the KSK will be rolled over annually using the double signing method.

Double Signature Method:
For the Double-Signature method, both the new key and signatures created using it are introduced at the same time. After a period during which this information propagates to validating resolver caches, the old key and signature are removed.

The ZSK, being smaller in size, will be rolled quarterly using the pre-publish method.

Pre-Publish Method
For the pre-publish method the new key is introduced to the zone but it is not used to generate signatures. The new key is then allowed to propagate to validating resolvers caches. After a period of time the new key is used to generate signatures and replaces the signatures generated by the old key. The old key remains in the zone for a period of time to allow for cached signatures to be validated and to allow validating resolvers to clear their cache of the old key signatures. After a predetermined time (based on the zone TTL) the old key is removed from the zone.

6.5 Signature life-time and re-signing frequency

RRsets are signed with the ZSK and have a validity period of 90 days. Automatic resigning takes place daily and all signatures are regenerated at that time.

6.6 Verification of resource records

auDA verifies that all resource records are conformant with the current standards before publishing the zone. This is achieved using available tools and custom scripts.

6.7 Resource records time-to-live

RRtype	TTL
DNSKey	86,400 seconds (24 hours) (Same as the SOA).
Delegation Signer (DS)	Inherit TTL from the corresponding delegation (NS-Set).
RRSIG	Inherit TTL from the corresponding signed RRset.
NSEC	43,200 seconds (12 hours) (Same as the negative TTL).

7 Compliance Audit

auDA conducts both internal and external audits of the DNSSEC signing system. Audits are conducted using retained logs and other relevant information to ensure that proper procedures have been followed, and that the procedures have been executed accurately.

7.1 Frequency of entity compliance audit

Audits are conducted both regularly and on an adhoc basis as required by auDA. Circumstances which will require an audit to be scheduled include, but are not limited to:

- More than 36 months have elapsed since the last audit.
- Recurring discrepancies or incidents are brought to auDA's attention.
- Significant staff changes are made.
- Significant hardware changes or process changes are made.
- Any other incident or event occur that may have resulted in the weakening of the DNS and/or DNSSEC environment.

7.2 Identify/qualifications of auditor

The auditor must be able to demonstrate proficiency with IT security tools, security auditing, DNS and DNSSEC.

7.3 Auditors relationship to audited party

For external audits, an independent auditor shall be appointed to conduct and lead the audit. If necessary, the auditor may engage technical experts with the relevant background experience from auDA, or organizations affiliated with auDA. Auditors do not participate in the signing operations or management for .au.

7.4 Topics covered by audit

The scope of the Compliance Audit includes all DNSSEC-related procedures such as key environmental controls, key management operations, infrastructure/administrative controls, KSK and ZSK signature life cycle management and practices.

7.5 Actions taken as a result of deficiency

Significant exceptions or deficiencies identified during the Compliance Audit will be provided in a report to the auDA Executive Management Team. A review of the report will require a set of actions that the auDA IT Team implements as part of a corrective action plan.

If auDA determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the KSK, a corrective action plan will be developed within 30 days and implemented within a commercially-feasible timeframe.

For less serious exceptions or deficiencies, auDA Management will evaluate the significance of such issues and determine the appropriate course of action.

7.6 Communications of results

auDA does not publicize compliance audits reports.

8 LEGAL MATTERS

8.1 Disabling DNSSEC

auDA reserves the right to disable DNSSEC if the protocol introduces, or attributes to, increased instability or risk to the .au zone. Notifications of intention to remove DNSSEC from the .au zone will be provided via the mailing list as described in Section 2.

8.2 Fees

auDA does not charge fees for any function related to DNSSEC in the .au zone file.

8.3 Financial responsibility

auDA is not responsible for the improper use of Trust Anchors or signatures issued under this DPS.

8.4 Confidentiality of business information

8.4.1 Scope of confidential information

The following records shall be kept confidential and private:

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

8.4.2 Information not within the scope of confidential information

Public key information is published as DNSKEY records in the .au zone and as DS records in the root zone. 2LD Registry Operators DS records are published as public information in the .au zone and as DNSKEY records in their respective 2LD zone.

8.4.3 Responsibility to protect confidential information

Not applicable.

8.5 Privacy of personal information

auDA does not store personnel identifiable information in the DNS.

8.5.1 Information treated as private

Not applicable.

8.5.2 Types of information not considered private

Not applicable.

8.5.3 Responsibility to protect private information

Not applicable.

8.5.4 Limitations of liability

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

8.6 Term and Termination

This DPS is reviewed annually and remains valid until it is replaced by a new version or if auDA ceases to be the .au registry operator.

8.7 Governing Law

auDA is governed by and in accordance with the laws of Victoria.