auDA PUBLISHED POLICY

Policy Title: INTERIM DNSSEC POLICY AND PRACTICE STATEMENT (DPS) FOR THE .AU DOMAIN
Policy No: 2014-02
Publication Date:
Status: Replaced by Policy No 2014-08

1. BACKGROUND

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

1.2 auDA's Interim DPS is at Schedule A of this document. It is intended to provide information on how auDA will implement and manage the .au Key Signing Keys (KSK) and Zone Signing Keys (ZSK) for the Australian (.au) top level domain.

1.3 The Interim DPS is based on IETF RFC 6841, A Framework for DNSSEC Policies and DNSSEC Practice Statements.

SCHEDULE A

INTERIM DNSSEC POLICY AND PRACTICE STATEMENT (DPS)
FOR THE .AU DOMAIN

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.

This 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

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.

Document name and identification

Document Title	DNSSEC Policy and Practice Statement
Version	0
Date Created	04/02/14
Date Modified	

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 current .au zone contains delegation points for the existing Second Level Domains (2LDs):

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

.sa.au	AusRegistry Pty Ltd	Restricted to Community Groups
.tas.au	AusRegistry Pty Ltd	Restricted to Community Groups
.vic.au	AusRegistry Pty Ltd	Restricted to Community Groups
.wa.au	AusRegistry Pty Ltd	Restricted to Community Groups

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 2LD Registry Operators
- performing an 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. Only a Registrar has direct access to a 2LD Registry Operator's database and 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 and auDA takes no responsibility for any failures that occur due to static Trust Anchor configurations. auDA does not comply with or utilise RFC 5011

Specification administration
This DPS is a living document and will be periodically reviewed and updated as appropriate.

Specification administration organisation
.au Domain Administration Ltd (auDA)
114 Cardigan St
Carlton, VIC, 3053
Telephone: +61 (0) 3 83414111
Fax: +61 (0) 3 83414112
Email: info@auda.org.au
Web: http://www.auda.org.au
ABN: 38 079 009 340

Specification change procedures
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 below.

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.

PUBLICATION AND REPOSITORIES

auDA publishes this DPS and other related DNSSEC information on its website at http://www.auda.org.au/dnssec.

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
http://www.lists.auda.org.au/mailman/listinfo/dnssec-announce

Publication of public keys
auDA publishes the KSK public key in one format, Delegation Signer (DS) records. The DS record for the .au zone is provided to IANA for publication into the root zone, no other repositories will be used.

auDA will announce the start and end of KSK rollovers via the dnssec-announce@lists.auda.org.au mailing list and also on Network Operator Group mailing lists including AusNOG, NZNOG and NANOG.

OPERATIONAL REQUIREMENTS

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

Identification and authentication of child zone manager
2LD Registry Operators are required to provide a designated Point of Contact (POC) to auDA for all DNS related modifications or deletions. All change requests are confirmed prior to inclusion in the .au zone.

Registration, Modification and Deletion of delegation signer (DS) resource records
Registration, modification and deletion of DS records must follow the guidelines documented in the auDA 2LD Registry Operator DNS Change Request document.

Emergency removal request
2LD Registry Operators may request an emergency removal of the DS resource record. This request must be in the same format as described above but must clearly be marked as an emergency change. All Emergency Requests will be treated with the highest priority and actioned as soon as possible.

The total removal of all DS records would be treated as an Emergency Removal Request and should be submitted as such.

Method to prove possession of private key
During pre-delegation checks, auDA will ensure that:

- the DS records provided are available as DNSKEY records at the apex of the child zone
- DNSKEYs are signed and verified against at least one of the supplied DS records
- the DNSKEY has its SEP bit set
- signature validity period is not due to expire.

FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

Site location and construction
auDA operates multiple sites which include a server room in the auDA office and racks within data centres that are geographically dispersed.

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 or accompaniment of auDA authorised personnel.

Power and air conditioning
The auDA office server room has separate air conditioning and UPS capabilities. All data centres 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.

Water exposures
auDA has taken reasonable precautions to minimise the impact of water exposure at all sites.

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

Media storage
Media considered sensitive is encrypted and stored in a safe which is only accessible to auDA management personnel.

Waste disposal
Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Where cryptographic devices are used they are physically destroyed or zeroised in accordance with the manufacturers' guidance prior to disposal.

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

Procedural controls

Trusted roles
Trusted persons include auDA management and IT personnel that have access to the .au zone to perform their day to day responsibilities. Access to signer systems requires a minimum of two personnel, each holding separate passcodes that when combined allow for operational actions to be completed.

A trusted person may hold multiple roles within a signing procedure but no single trusted person can effect change to the Hardware Security Module (HSM). All changes will be authorized, documented and signed off by a minimum of two trusted personnel.

Personnel controls

Qualifications, experience, and clearance requirements
Trusted persons who fulfil trusted roles must have demonstrated appropriate background, qualifications and experience relative to their prospective job responsibilities and have been employed with auDA for a minimum of one year.

Background check procedures
All trusted persons are subject to a national police check with the Australian Federal Police, have been employed with auDA for more than one year and are in a senior role. Applicants must disclose previous employments in the last five years and provide references for validation. Trusted persons will be re-checked every five years.

Training requirements
Training for a trusted role will be conducted by auDA and will be specific to the role and responsibility of each trusted person. All trusted persons will be required to have an understanding of how the DNS works, auDA's role in the DNS and the role of DNSSEC in the DNS.

Job rotation frequency and sequence
auDA will provide refresher training and updates for persons in trusted roles to the extent and frequency required to ensure that such persons maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

Trusted persons are rotated and replaced when and as required.

Sanctions for unauthorised actions
Disciplinary actions will be undertaken for unauthorised 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 unauthorised actions.

Contracting personnel requirements
Contractors are not permitted physical or logical access to the HSM. They may be used in an advisory role but will not perform any actions in relation to key generation or activation.

Documentation supplied to personnel
Trusted personal will be provided HSM procedural documentation and a check list for use during interaction with the HSM that will be signed and dated upon completion.

Audit logging procedures

Types of events recorded
Machine generated logs are securely stored in a central monitoring system. These logs will be reviewed with greater scrutiny during and after key signing and key rollovers.

Zone edits and comments for the .au zone file are versioned using a repository which 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 backup procedure.

Protection of audit log
All logs are encrypted and backed up and stored in a secure location. Logs are only available to auDA management and do not contain any private key or other sensitive information that may lead to compromise. Paper logs are scanned and stored electronically, and the paper logs themselves are then stored in a fireproof safe.

Audit log backup procedures
Audit logs are encrypted and backed up to external storage as part of the auDA back up procedure. Access to safes containing paper log material is only accessible to authorised auDA management.

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

Vulnerability assessments
Anomalies or discrepancies in log data are investigated to analyse any potential vulnerabilities.

Compromise and disaster recovery
In the event an incident leads to, or has the potential to lead to, a security compromise auDA will conduct an investigation to determine and identify the potential threats. If the incident leads to, or could lead to, a private key compromise of an active key the Emergency Key Rollover procedure will be performed.

Corrupted computing resources, software, and/or data
All signing related hardware will be covered by vendor maintenance contracts. In the event of a hardware fault the equipment will be replaced as per the contractual agreement with the vendor. In addition auDA maintains redundancy on all equipment at all sites. Failures will be investigated immediately and systems restored to full operation as soon as possible.

In the event of software corruption or failure auDA trusted staff will investigate the cause and restore systems from the most recent unaffected backup.

Business continuity and IT disaster recovery capabilities
auDA has business continuity and IT disaster recovery plans in place to address the restoration of information systems services and key business functions. These plans address:

- roles and responsibilities in the event of a disaster
- fallback procedures for restoring business-critical processes within time appropriate time frames
- resumption procedures for restoring normal operations
- the criteria for activating the plan
- communication with the public.

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

If auDA was to discontinue DNSSEC, a plan would be implemented and all notifications regarding the return to an unsigned zone will be provided via the auDA website and via the dnssec-announce@lists.auda.org.au mailing list.

TECHNICAL SECURITY CONTROLS

Key pair generation and installation

Key pair generation
Key pair generation takes place in an HSM that is managed by trained and specifically authorised personnel in trusted roles.

Public key delivery
The public component of each generated KSK is exported from the HSM as a DS record and published as per the Publication and Repositories section.

The DS is delivered to the parent zone as per the IANA procedures listed at http://www.iana.org/procedures/root-dnssec-records.html.

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

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.

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.

Cryptographic module standards and controls
The system uses an HSM, which conforms to the requirements in FIPS 140-2 level 3.

Private key (m-of-n) multi-person control
Access to the signer system is documented in the Trusted Roles section.

Private key escrow
Private key components used for zones are not escrowed.

Private key backup
auDA performs routine backups of the .au ZSK and KSK private keys after each new key pair is generated. All backups are encrypted and only accessible by auDA trusted persons. Both the backup and restoration of the private keys requires dual authorisation.

Private key storage on cryptographic module
Private components of keys used for the zone are stored on an HSM in an encrypted format.

Private key archival
Private keys are not archived on the HSM after rollover, however private keys can be restored from backups as listed above.

Private key transfer into or from a cryptographic module
Keys are transferred to and from an HSM in an encrypted format using hardware specific operator cards that are encrypted and passcode protected.

Method of activating private key
Private keys are activated by configuring an activation and publication date when generating the relevant key pair.

Method of deactivating private key
Private keys are deactivated by specifying a delete date during generation of the relevant key pair.

Method of destroying private key
Where required, auDA will utilise the zeroisation function of its HSM and other appropriate means to ensure the complete destruction of the .au KSK and ZSK. 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.

Other aspects of key pair management
auDA will only publish the public keys that are current to the operation of the .au zone. Public keys will not be archived past their deletion date.

Activation data
Trusted persons will hold credentials to be able to activate the HSM. Activation data is stored on a hardware specific card, which is encrypted and protected by a PIN. Trusted persons are required to safeguard their PIN in accordance with the auDA password policy.

Computer security controls
All production computer systems are housed in secure facilities. Physical and remote access to signing systems is limited to trusted persons. All access, physical and remote, to computer and signing systems, successful and unsuccessful, are logged.

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.

Timestamping
auDA uses trusted time sources within the signing system network to synchronise system clocks. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

Life cycle technical controls
auDA tests all new sources of software in a lab environment prior to deploying to production servers. Systems are evaluated prior to deploying it, in order 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-evidence bags to their destination in the secure facility. All hardware will be decommissioned well before the specified lifetime expectancy.

ZONE SIGNING

Key lengths, key types and algorithms
auDA uses RSA algorithms with a key length of 2048 bits for the KSK and 1280 bits for the ZSK.

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.

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

Key rollover
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.

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

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.

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.

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)

LEGAL MATTERS

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 2.1.

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

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.

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