.au Domain Administration Limited

Registry Service Description

28 February 2023

EXPOSURE DRAFT 28 February 2023

auDA Registry Service Description – Exposure Draft

The .au Domain Administration Limited (auDA) is supported in its administration of the .au domain by a Registry Operator.

The Registry Operator is appointed for a fixed term.

In or around April 2023, auDA will release to the open market a request for tender (RFT) for a Registry Operator for the .au domain.

In advance of the RFT, auDA has prepared an Exposure Draft Registry Service Description (Exposure Draft RSD) to provide information about the technical and administrative requirements that we anticipate we will require of the successful respondent to the RFT. It is structured to provide an intuitive flow to the requirements of each service within the Registry System and succinctly define our requirements.

auDA invites interested parties to provide feedback on this Exposure Draft RSD. We will consider all feedback received and may incorporate it into the RFT documents.

Interested parties should:

- Note that we will not be responsible for any costs interested parties incur in providing feedback on the Exposure Draft RSD.
- Not presume that the requirements ultimately set out in auDA's RFT will be the same or substantially the same as those specified in the Exposure Draft RSD.

Submissions containing feedback on the Exposure Draft RSD must be submitted:

1. In plain text, Microsoft .docx, or .pdf format
2. In English
3. Via email to: tenders@auda.org.au no later than 23:59:59 UTC on Tuesday 21 March 2023 (10:59:59 AEDT on Wednesday 22 March 2023)

Submissions made to auDA may be published by us, including the name of the entity or individual who made the submission. If a respondent does not wish for its submission to be published by auDA, it should make a request to this effect and set out the basis for withholding publication in its submission to auDA. If auDA is satisfied with the reasoning provided by the respondent, we will not publish the respondent's feedback unless we are authorised or required by law to disclose the feedback.

Definitions

In this document:

.au ccTLD means the .au country code top level domain.

ACSC means the Australian Cyber Security Centre (https://www.cyber.gov.au/).

Administrator means auDA.

auDA means .au Domain Administration Limited (ACN 079 009 340).

auDA Fee means the amount that the Registry Operator must pay to auDA as set out in the Registry Licence Agreement.

DNSSEC means the Domain Name System Security Extensions (RFC 4033).

EPP means the Extensible Provisioning Protocol (RFC 5730).

gTLD means a generic Top Level Domain, as defined by the Internet Corporation for Assigned Names and Numbers (ICANN) (https://www.icann.org/en/icann-acronyms-and-terms).

RDAP means the Registration Data Access Protocol (RFC 9082).

Registrar means any entity accredited by auDA and the Registry Operator to provide registrar services in the au country code Top Level Domain.

Registrant means the holder of a Licence (or any agent of such holder or applicant), as recorded in the Registry Data at the relevant time.

Registry Operator means the entity providing the service to auDA under the Registry Licence Agreement.

Registry means the primary and secondary nameservers and WHOIS servers, a database containing the Registry Data and a mechanism for accessing that data, in relation to the Designated Namespaces.

Registry Data means all data maintained in electronic form in the Registry, including without limitation:

a) Registrant contact information,
b) technical and administrative contact information,
c) WHOIS Data,
d) all other data submitted by Registrars in electronic form, and
e) other data concerning particular registrations or nameservers maintained in electronic form in the Registry database.

Registry Database means a database comprised of data about one or more DNS domain names within the .au ccTLD that is used to generate either DNS resource records that are published authoritatively or responses to domain name availability lookup requests or WHOIS queries, for some or all of those names.

Registry Lock Service means a domain name security feature which requires a registrar to complete additional authorisation steps ("unlock") to modify the state of a domain name record. The "locked" status of a domain name is recorded by applying serverDeleteProhibited, serverUpdateProhibited, and serverTransferProhibited statuses to the domain name at the Registry. The registry lock will prevent standard registrar API functions from modifying the state of the domain name. Note that domain name expiry and domain name purge lifecycle events will continue as per the .au Licensing Rules

Registry services means the services specified in the Registry Licence Agreement, including the registration services, authoritative nameserver services, the WHOIS registration data directory services, registrar support services and reporting and logging services.

Registry System means the system operated by Registry Operator under the Registry Licence Agreement.

UTC means *Coordinated Universal Time* as defined in the International Telecommunication Union (ITU) standard Recommendation TF.460-6 (02/2002) (https://www.itu.int/rec/R-REC-TF.460-6-200202-I/en) .

Purpose

The purpose of this document is to define the technical and administrative requirements of the Registry Operator appointed by auDA, the administrator of the .au country code Top Level Domain (.au ccTLD) for the benefit of all Australians.

Scope

The scope of this document is to describe the technical and administrative requirements the Registry Operator must meet to provide registry services for the .au ccTLD. It does not define their operational implementation. Implementation, of the requirements herein, will be at the Registry Operator's discretion.

Audience

This document is intended for the Australian Internet community.

Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. https://www.rfc-editor.org/rfc/rfc2119

Contents

Introduction

This document defines the technical and administrative requirements required for the registry and ancillary services to be undertaken by the registry operator for the .au ccTLD.

There are currently 4.2 million names under management on the .au registry platform as of January 2023. Historic trends are available via monthly reports available at: https://www.auda.org.au/industry/au-registry/registry-reports

Below is a list of 2022 average transactions seen across the registry system and ancillary services:

- over 150 million average EPP transactions per month,
- 100 million average WHOIS lookups per month,
- over 100 million average WHOIS checks per month, and
- over 6 billion DNS queries per day.

There are currently 36 namespaces in the .au ccTLD, 35 of which are managed by the registry operator:

- au
    - act.au
    - asn.au
    - com.au
    - conf.au
    - edu.au
        - act.edu.au
        - catholic.edu.au
        - eq.edu.au
        - nsw.edu.au
        - nt.edu.au
        - qld.edu.au
        - sa.edu.au
        - schools.nsw.edu.au

        - tas.edu.au
        - vic.edu.au
        - wa.edu.au
    - gov.au
        - act.gov.au
        - nsw.gov.au
        - nt.gov.au*
        - qld.gov.au
        - sa.gov.au
        - tas.gov.au
        - vic.gov.au
        - wa.gov.au
    - id.au
    - net.au
    - nsw.au
    - nt.au
    - org.au
    - qld.au
    - sa.au
    - tas.au
    - vic. au
    - wa.au

*nt.gov.au is currently managed outside of the Registry. The Registry Operator must be ready to support this zone in the future if required.

The technical specifications listed in the document are to apply equally to each of the zones listed above, and any future zones that may be introduced during the licence period.

The Registry Operator must not subcontract the whole or any part of the services described within the technical specifications:

except with the prior written consent of auDA; and

where consent is granted, it is the Registry Operators responsibility to ensure that the subcontractor meets the requirements of the technical specifications.

The technical specifications require adherence to various current industry standards, specifications, and protocols. The Registry Operator must implement new or updated version or errata issued of these standards, specifications, and protocols.

The legal entity of the Registry Operator must be an Australian incorporated entity.

Registry System

The minimum requirements of the Registry System are as follows:

The Registry software and databases must be on separate instances from other ccTLDs or gTLDs.

The Registry System may operate on shared computing environments, or public cloud infrastructure, with appropriate isolation from software/databases associated with other ccTLDs or gTLDs.

The operating environment used whether it be public cloud, private cloud, co-location or private datacentre must always be at a location within Australia pre-approved by auDA.

Key personnel necessary for supporting the registry environment and providing support to registrars must be located in Australia.

Registry Data and Registry System backups must be located in Australia.

The Registry Operator must request auDA to authorise all staff that require access to the Registry Data.

As part of the Registry System the Registry operator must deliver the following:

A Registry Data Store that stores information about Registry Objects (e.g. Domains, Contacts, Hosts, Registrars and other supporting objects) involved in providing the Registry Services.

Business Rules: The Registry System must be able to support specific .au business rules and data elements as described in this document.

A Registry Access Application Programming Interface (API) compliant with the Extensible Provisioning Protocol (EPP) Standard that allows provisioning and management of the Registry Objects in the Registry System.

A Registry HTTPS Interface, a human useable interface that augments the Registry Access API allowing for the same functionality as the API to be performed as well as additional requirements defined in the relevant section of this specification. The HTTPS interface must include enforced multi factor authentication.

A public Domain Lookup Service, based on the WHOIS standard provided over both a TCP port-43 at *whois.auda.org.au* and a HTTPS interface (https://whois.auda.org.au/

) that allows members of the public to view information about the objects registered in the Registry System.

A public Domain Lookup Service, based on the Registration Data Access Protocol (RDAP) standard that allows members of the public to view information about objects registered in the REGISTRY SYSTEM.

An authenticated Domain Lookup Service, based on the Registration Data Access Protocol (RDAP) standard that allows access to a limited set of Registry Data for cyber security purposes.

A public port-43 Domain Availability Check Service based on the WHOIS standard provided over TCP port-43 at *domaincheck.auda.org.au* that allows members of the public to check the availability of domain names in the Registry System.

A Registrant Domain Name Password Recovery Service delivered over HTTPS (https://pw.auda.org.au/) that allows a domain name registrant to recover the password ('EPP AuthInfo') for authorising registrar transfers and view the expiry date for their domain name.

A Registry Lock Service – the ability for a registrar to place a Registry Lock on high value names at the request of the Registrant.

A Domain Drop List Service that provides HTTPS access to the list of upcoming purging domain names.

A Domain Statistics Service that provides the Administrator with an API to access statistical information about the state of the namespace.

A DNS Signing and Publication Service – the mechanism by which changes to Registry Data is published to the Authoritative DNS Service, including DNSSEC signing.

An ability to interface with an Administrator API, or set of API's, that enables the Administrator to perform in-path validation of domain name registrations against policy at the time of domain name creation, renewal and transfer (between registrars and between registrants).

A .au Priority Contention Resolution Service – to facilitate the resolving of contention between multiple eligible applications for a .au direct (e.g. forexample.au) name (as shown in the Priority Status tool at: https://www.auda.org.au/tools/priority-status-tool) as per the .au Direct Priority Implementation Policy (https://www.auda.org.au/policy/auda-rules-au-direct-priority-implementation)

All domain names used for public facing services relating to the Domain Name Registry Systems are provided by auDA and will be delegated to the Registry Operator for the duration of the licence to manage and operate the public service.

1. Registry Database

The Registry must include a system or collection of systems used to store, amongst other information, the Domain, Contact, Host, Registrar and associated objects information.

1.1. The schema definition of the Registry Data Store must be documented and made available to the Administrator.

1.2. The Registry Database must be capable of meeting the performance, Restore Time Objective (RTO) and Restore Point Objective (RPO) requirements as outlined in Section 0.

1.3. The Registry Database must have scaling and replication functionality.

1.4. The Registry Database must be capable of being backed up without being taken offline.

1.5. The database software chosen for the Registry Database must be demonstrated to have an active support community.

1.6. The Registry Database must have a demonstrated history in being utilised in the operation of systems of a similar scale and criticality as the Registry.

1.7. Future implementations of the Registry Database must be backward compatible for registrars.

2. Business Rules

Regardless of interface the Registry System must ensure the following requirements are met.

2.1. Policy Compliance

2.1.1. Unless otherwise approved by the Administrator, the system must comply with Administrator policy at all times. Current policies can be found at: https://www.auda.org.au/policies/

2.1.2. Should any requirement in this specification wholly or partially contradict Administrator policy, the requirement as described in the policy document shall take precedence. The Registry Operator should raise any such contradictions with the Administrator when they are

identified to ensure the correct interpretations and clarifications are made prior to changes being implemented.

2.2. General Requirements

2.2.1. The system must implement standard industry requirements of a domain name registry as inferred by the Registry Access API.

2.2.2. The language(s) support by all interfaces must include English.

2.2.3. All interfaces to the system must accept and expose data utilising the Unicode Consortium's UTF-8 encoding scheme. The Unicode standard can be found at https://unicode.org/standard/standard.html. Other formats may be accepted/returned only where a method exists to signal as such and only after the client has signalled their ability to accept such encoding format. Where no mechanism exists UTF-8 is to be assumed.

2.2.4. The system must behave in an identical manner for all Registrars.

2.2.5. The system must behave in an identical manner for all namespaces covered by this technical specification.

2.2.6. Registry Object Identifiers (ROIDs) for Domain, Contact, Host and Registrar objects must be allocated utilising an algorithm that is unable to be predicted by users of the system. It must not be incremental.

2.2.7. ROIDs for Domain, Contact, Host and Registrar objects must be prefixed with 'D', 'C', 'H' or 'R' respectively.

2.2.8. ROIDs for Domain, Contact, Host and Registrar object must be postfixed with a Registry System specific identifier (currently the string '-AU' is used). This ensures that the identifiers are globally unique among registry systems.

2.2.9. All timestamps must be recorded and displayed in UTC format. The systems may also display timestamps in a user's preferred time zone as an additional output.

2.2.10. All modification transactions within the system must be assigned a system unique transaction reference by the system.

2.2.11. A complete history of all Domain, Contact, Host, Registrar and associated objects (at a minimum) must be maintained such that reconstructing the state of an object at any point in time is possible –

including even after removal of the object from the system. This history is to include:

2.2.11.1. The command used to modify the object

2.2.11.2. Whether the action was taken by the user, or an automated action taken by the system.

2.2.11.3. The source and destination IP address and port of the connection to the interface that initiated the transaction.

2.2.11.4. The username and account information of the user who was authenticated and initiated the transaction.

2.2.11.5. The interface (API, website etc.) used to perform the transaction.

2.2.11.6. The timestamp of the transaction.

2.2.11.7. The system unique transaction reference.

2.2.11.8. Any client specified transaction reference if supplied.

2.2.12. All transaction input and output of all interfaces must be logged and maintained indefinitely. These logs should include:

2.2.12.1. All information as per the object history.

2.2.12.2. Session identifiers.

2.2.12.3. The actual input and output command in the native format of the interface (XML, JSON etc.) – note for HTTPS requests it is sufficient to capture the 'access-log' style entry.

2.2.12.4. The command and response, and the associated parameters.

2.2.12.5. Whether or not the command was successful and the relevant response code.

2.2.12.6. The processing time of the transaction as observed by the interface.

2.2.12.7. For the purposes of the Domain Lookup Service – WHOIS and Domain Availability Check Service it is sufficient to keep a truncated version of the output only indicating whether or not the object being queried was found or not.

2.2.12.8. For the purpose of the Domain Lookup – RDAP must include transaction logs in the native format, including if the request was

anonymous or authenticated, the request including user and source IP and the requests response codes,

2.2.12.9. All sensitive information such as client credentials and object 'authinfo' is to be masked in the transaction logs.

2.2.13. The above logging and history requirements do not apply to the Authoritative DNS Service.

2.2.14. Unless otherwise required to implement the requirements of an interface all password / object 'authinfo' information is to be stored utilising a secure, non-reversible hash mechanism.

2.3. Domain Lifecycle

2.3.1. The system must implement the Domain Life Cycle as defined in Administrator policy and summarised in the table provided at Appendix B.

2.3.2. All time periods before default actions are taken, and which default action (e.g. approve or reject) are defined in the Administrators Domain Renewal, Expiry and Deletion policy.

2.3.3. The system must be configurable such that changes to timeframe requirements in policy can be implemented. The Administrator and the Registry Operator will work together to determine a suitable implementation timeframe. .

2.4. Validation

2.4.1. The system must ensure that all domain name and email address fields only accept protocol valid inputs.

2.5. Universal Acceptance

2.5.1. The system should ensure the universal acceptance of new TLDs, with respect to the use of new TLDs in email addresses, authoritative nameservers, and host names.

2.6. Internationalised Domain Names

2.6.1. The systems must support IDNs. The initial set of IDNs will be: Japanese, Chinese, Korean, Arabic, and Vietnamese (see clause 2.8 of the .au licensing rules: https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-8).

2.6.2. IDNs must only be accepted for use in email addresses and authoritative nameserver hosts.

2.6.3. IDNs must be expressed in their ASCII Compatible Encoding (ACE) form as well as their IDN-form when displayed in the Domain Lookup Services, WHOIS, Domain Check, and RDAP

For example:

Registrant Contact Name: David Müller

Registrant Email: david@müller.com [david@xn--mller-kva.com]

Name Server: autorité.example.com.au [xn--autorit-hya.example.com.au]

Name Server IP: 192.168.48.219

2.6.4.

2.6.5. The registry must only accept characters in registrant and contact data fields (i.e. company names, personal names, address, etc.) within the Unicode scripts of Basic Latin, Latin-1, Latin Ext-A and Latin Ext-B (U+0000-U+024F).

2.6.6. Registered domain names must be restricted to the syntax of domain names under the current .au licensing rules (https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-7).

2.6.7. The Registry System should be adaptable such that should Administrator policy change on permissible code points, the new policy can be adopted.

2.7. DNS Glue Records

2.7.1. The system must implement a narrow glue policy (see https://datatracker.ietf.org/doc/html/draft-koch-dns-glue-clarifications-03) and only publish glue records to the DNS where the hosts are directly associated as name servers to domains above them in the DNS hierarchy.

2.7.2. The Registry System must accept IPv4 and IPv6 glue records and capable of publishing them in all public facing services.

2.8. **Domain Name 'EPP authInfo'**

2.8.1. The Administrator policy sets out the EPP authInfo requirements in the Domain Name Password Policy which can be located in the policy section of the Administrators website, https://www.auda.org.au/policies.

2.9. Hierarchal Namespaces

2.9.1. The system must support the registration of domain names in namespaces that may be subordinate of another namespace configured in the system (i.e. registrations under .gov.au and .vic.gov.au). See Appendix C and Appendix D for additional requirements with edu.au and gov.au .

2.9.2. The system must include a technical validation mechanism to ensure that domain names registered in the parent namespace cannot conflict with, or affect the security and integrity of the child namespace.

2.10. Non-delegation Resource Records

2.10.1. The system must support the ability to publish non-delegation resource records into the namespace zone file.

2.10.2. The system must support the ability to publish resource records at the apex of the namespace DNS zones.

2.10.3. The system must ensure that domain name registration in the namespace cannot conflict with, or affect the security and integrity of the non-delegation or apex resource records.

2.10.4. The system must also ensure that non-delegation resource records do not interfere with the security and proper operation of any child namespaces.

2.11. Account Functions

2.11.1. The system must have the capability of sending expiry notices to Registrants on behalf of an account, in the event of a failure of a registrar's operations.

2.11.2. The system must have the capability of configuring an account to auto-approve outgoing transfers automatically.

2.12. Reserved Names

2.12.1. The Administrator will maintain, and provide to the Registry Operator, a list of reserved names. These domains are unavailable for provisioning in the registry system.

2.12.2. The system must have the capability to prohibit the registration of or require approval of certain domain names

2.12.2.1. Where a domain name may require an approval the 'create' request should create the domain name in a 'pendingCreate' status. The Administrator should be able to review the registration and if it approves the registration, the domain name can transition to an actual created status.

2.12.3. The system must be capable of prohibiting the re-registration of a name on the reserved list, if an existing registered domain name that matches the reserved name expires or is deleted.

2.12.4. Reserved names should not appear or be published on the Drop List

2.12.5. This system must support direct match entries on the reserved list.

2.12.6. The system must support configuring a reserved list entry as either a blocked entry or pending 'create' entry.

2.12.7. This system must support configuration of the message that is displayed in the WHOIS and EPP check results about the reason for the reserved entry.

2.12.8. The reserved reason message should be configurable on a per-entry basis.

2.12.9. The reserved reason message should be capable of being different between the WHOIS and EPP Check result.

2.12.10. The reserved domain names should be separately configurable on a per namespace basis.

2.12.11. Registrars must be able to download a list of the currently reserved names.

2.12.12. The system must have the capability to reserve the registration of certain domain names for the exclusive registration by a single registrar.

2.13. Registrar Notifications

2.13.1. The system must use the poll message functionality to notify Registrars of the following:

2.13.1.1. Transfer outs requiring approval;

2.13.1.2. Transfer ins being approved or rejected;

2.13.1.3. Low balance notifications;

2.13.1.4. Domain expiry actions; and

2.13.1.5. All changes to objects sponsored by the Registrar where the action was taken automatically by the system or by a user of any other account.

Notification Reason	Message Content
domain transfer approved – acquiring Registrar	Registrar <REG_ROID> has approved the transfer of domain <DOM_ROID>
domain transfer request – relinquishing Registrar	Registrar <REG_ROID> has requested the transfer of domain <DOM_ROID>
domain transfer cancelled – sponsoring Registrar	Registrar <REG_ROID> has cancelled the transfer of domain <DOM_ROID>
Registry has automatically approved the transfer of <Contact ROID>	The Registry has automatically approved the transfer of Contact <CONROID>
contact transfer approved – acquiring Registrar	Registrar <REG_ROID> has approved the transfer of contact <CON_ROID>
contact transfer requested – relinquishing Registrar	Registrar <REG_ROID> has requested the transfer of contact <CON_ROID>
contact transfer cancelled – sponsoring Registrar	Registrar <REG_ROID> has cancelled the transfer of contact <CON_ROID>
contact transfer auto-approved – relinquishing and acquiring Registrars	Registry has automatically approved the transfer of contact <CON_ROID>
Registrar account – low balance	<Severity> <Currency> <Balance>
Registrar account – daily closing balance	Your balance at end of business <DATE> was <BALANCE>
Domain expiry – serverHold	The domain <DOM_NAME> has expired
Domain expiry – pending delete	The expired domain <DOM_NAME> is now pending deletion.
Domain expiry – purged	The domain <DOM_NAME> has been purged from the Registry.

2.13.2. The Registrar should have the ability to elect to receive the poll messages to an email address. The system must allow the specification of different email addresses for different category of messages, e.g. an email address for financial messages, one for object actions etc.

2.13.3. Additional notifications should be sent by the system to users of the system for events such as:

2.13.3.1. New logins from an IP address/computer not previously used;

2.13.3.2. Password expiration warnings; and

2.13.3.3. Other relevant security events

2.14. Key-Value Pair

2.14.1. The system must support a generic 'key-value' pair system that allows the system to be configured to require the collection of additional data as part of a domain name registration.

2.14.2. The keys corresponding value, mandatory requirements and validation for the values must be configurable to enable implementation of the new requirements or changes to policy in a timeframe specified by the Administrator.

2.14.3. The key value pair groups should be configurable on a per-namespace basis.

2.15. AU Extensions

2.15.1. The system must support the collection of the 'AU EPP Extensions' as described in Schedule D of the .au licensing rules (https://www.auda.org.au/policy/au-domain-administration-rules-licensing#SD) (see the WHOIS entry for pavlova.au for an example of the use of these extensions) :

2.15.1.1. *Registrant* - legal name of the registrant entity

2.15.1.2. *Registrant ID* - Australian Government issued ID number associated with the Registrant legal entity (typically an ABN or ACN number)

2.15.1.3. *Eligibility Type* - Registrant's basis for how they meet the Australian presence requirements (e.g. company, sole trader, citizen/resident, trust, trademark holder, incorporated association)

2.15.1.4. *Eligibility Name* - Name used by the Registrant to establish eligibility, if different from their own legal name (e.g. registered business name, name of a trust, or trademark)

2.15.1.5. *Eligibility ID* - Australian Government issued ID number associated with the name used by the Registrant to establish eligibility (e.g. ABN for registered business name or Trust, TM number for registered trademark)

2.15.2. The extensions should be able to be entered utilising any of the EPP extensions described in Section 3.2 or using key-value pairs.

2.16. Expiry Synchronisation

2.16.1. The system must support the expiry synchronisation mechanism as defined in the Administrators Domain Renewal, Expiry and Deletion policy, which can be found at the following link: https://www.auda.org.au/policies/

2.16.2. Registrars must only be able to update the expiry date of a domain to a time that is earlier than the current expiry date.

2.17. Additional Commands

2.17.1. The system must support the following additional commands for domain names:

2.17.1.1. Unrenew;

2.17.1.2. Undelete;

2.17.1.3. PolicyDelete - Licence Cancellation (domain name is purged from the registry after 14 days). See clause 2.16 of the .au licensing rules (https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-16);

2.17.1.4. PolicyUndelete; to reverse a licence cancellation and restore the domain name;

2.17.1.5. Registrant Transfer, where a new licence is issued for a fee - see clause 2.13.2 of the .au licensing rules (https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-13)

2.17.1.6. PolicySuspension – 30 Day Licence Suspension (domain is placed on clientHold for 30 days, and then goes into policy delete status for 14 days) used to suspend a domain name whilst an Administrator investigation is completed. See clause 2.16 of the .au licensing rules: https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-16

2.17.2. The requirements for these commands are defined in Administrator policy, which can be found at the following link: https://www.auda.org.au/policies/

2.18. Reseller ID

2.18.1. The system must support the Reseller ID functionality as described in Administrator policy, which can be found at the following link: https://www.auda.org.au/policy/reseller-id-application-form-2014-09

2.18.2. The Administrator must have functionality to manage approved Resellers.

2.18.3. A mechanism must be provided for Registrar's to include the Reseller ID when creating or updating domain names.

2.18.4. If set, the Reseller ID must be exposed in the WHOIS response.

2.18.5. The system should comply with RFC8543 - Extensible Provisioning Protocol (EPP) Organization Mapping and RFC8544 - Organization Extension for the Extensible Provisioning Protocol (EPP)

2.19. Configurability

The following parameters should be configurable across the system:

2.19.1. Command rate limits.

2.19.2. WHOIS 'white list' and 'black list' as well as limits, see Section 5.

2.19.3. RDAP access control and authentication,

2.19.4. EPP 'white list', see Section 3.

2.19.5. The minimum and maximum number of Administrative, Technical and Billing contacts a domain name must have.

2.20. The following parameters should be configurable on a per namespace basis.

2.20.1. Domain name registration pricing rules.

2.20.2. Maximum domain name validity (license) period.

2.20.3. The minimum and maximum periods allowed when a domain name is created.

2.20.4. The minimum and maximum periods by which a domain name registration can be extended.

2.20.5. The default number of years to be used when the period is omitted from a 'create' or a 'renew' command.

2.20.6. The period of time prior to expiry where renewals can be performed.

2.20.7. Which extensions are required, which are optional, which are to be used.

2.20.8. DNSSEC requirements (use of key or DS data).

2.20.8.1. DS records submitted using the SHA1 Algorithms must not be accepted. SHA1 is considered insecure even for DNSSEC

2.20.8.2. Existing SHA1 DS record may be grandfathered until such time it is removed by the domain name owner.

2.20.9. Domain name registration approval by the Administrator

2.20.9.1. If domain name create approval is required, the allowable time for the Administrator to approve/deny, and the ability for automatic action to be taken at the end of that time.

2.20.10. Domain name renewal approval by the Administrator

2.20.10.1. If domain name renewal approval is required, the allowable time for the Administrator to approve/deny, and the ability for automatic action to taken at the end of that time

2.20.11. Domain name fee refunds on domain name creates that are cancelled or rejected

2.20.12. Domain name fee refund on domain name renewals that are cancelled or rejected

2.20.13. The minimum number of name servers that must be assigned to the domain name before it is published in the DNS.

2.20.13.1. Domains that end up with less than this number due to no fault of their own (e.g. hosts removed as the result of the parent domain expiring) should not be removed from the DNS.

2.20.14. The number of days after a domain name is registered that it can be cancelled, i.e. deleted and removed from the system immediately.

2.20.15. The number of days after a domain name is registered that it is eligible for a refund if deleted.

2.20.16. The number of days after a domain name is deleted that it is eligible to be purged from the system (i.e. how long it will remain in 'pendingDelete' state for) and if there is any random period involved.

2.20.17. If a domain transfer must always include a domain renewal.

2.20.18. How long an outstanding transfer waits for action by the losing Registrar before the system takes an automatic action and what automatic action should be taken (e.g. approve or reject).

2.20.19. The ability for a Registrar to prohibit domain name transfers (e.g. the use of the 'clientTransferProhibited' status).

2.20.20. If domain name transfers can be rejected by the losing Registrar.

2.20.21. The duration of grace periods for creation, renewal, transferring and deleting domain names.

2.20.22. The availability, transformation (e.g. 'expired', 'expiredHold', 'expiredPendingPurge') and DNS state of a domain name upon and after expiry.

2.20.23. The schedule of times, which days of the week, days of the year etc. that domain names may expire, transition through expiry states and be purged from the system.

2.20.24. Pricing for domains names, by operation and period, with effective dates.

2.20.25. The use of key-value pairs and their properties

2.20.26. If an inactive contact (e.g. one not associated with any objects) should be purged from the system.

2.20.26.1. The number of days before the contact must be inactive before purging from the system

2.20.27. The ability to transfer a contact

2.20.27.1. If contact transfers are permitted, how long an outstanding transfer waits for action by the losing Registrar before the system takes an automatic action and what automatic action should be taken (e.g. approve or reject).

2.20.27.2. The ability for a Registrar to prohibit contact transfers

2.20.27.3. The ability for a Registrar to reject a contact transfer (e.g. the use of the 'clientTransferProhibited' status).

2.20.28. If an inactive host (e.g. not associated with any objects) is to be purged from the system.

2.20.28.1. The number of days before the host must be inactive before purging from the system.

2.20.29. The maximum number of IPv4 and Ipv6 addresses that can be assigned to a host.

3. Registry Access API

The Registry Access API will be used by Registrars to programmatically provision and manage objects in the Registry Database in accordance with the Business Rules.

3.1. The Registry System must provide a programmatic provisioning API utilising the IETF's Extensible Provisioning Protocol (EPP) as defined in the following IETF Documents:

Standard 69 (STD69): https://www.rfc-editor.org/info/std69

RFC5730 – Extensible Provisioning Protocol (EPP)

RFC5731 – Extensible Provisioning Protocol (EPP) Domain Name Mapping

RFC5732 – Extensible Provisioning Protocol (EPP) Host Mapping

RFC5733 – Extensible Provisioning Protocol (EPP) Contact Mapping

RFC5734 – Extensible Provisioning Protocol (EPP) Transport over TCP

RFC5910 – Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

RFC8543 – Extensible Provisioning Protocol (EPP) Organization Mapping

RFC8544 – Organization Extension for the Extensible Provisioning Protocol (EPP)

3.2. The Registry Access API must also implement the following EPP extensions in support of specialised functionality required by Administrator policy:

Association (used for 2nd level launch)

Domain Sync (used to change expiry dates)

AU extension (used for AU properties)

Policy (used for policy delete)

Details of these extensions can be found at the following link: https://sourceforge.net/projects/epp-rtk/files/afilias-rtk-addon/0.6.15/

3.3. The system must support the Host object functionality of the EPP protocol.

3.4. The Registry Operator may, from time to time, be required to further extend the EPP protocol to support additional functionality. Such EPP extensions must:

3.4.1. Comply with RFC3735 – Guidelines for Extending the Extensible Provisioning Protocol (EPP)

3.4.2. Be documented in such a way as to comply with the guidelines outlined in RFC7322 – RFC Style Guide and RFC 7997 - The use of Non-ASCII Characters in RFCs

3.4.3. Any extensions that are to be utilised in support of providing functionality defined in Administrator policy must be made available royalty free and unencumbered for the use by all current and future members of the community.

3.5. Should inadequacies with the API protocol emerge, and updated versions of the EPP protocol be produced by the IETF, the Registry Operator must commit to implementing the revised version of the protocol in both the server and Registry Operator provided toolkit. Implementation timelines will be determined by the Administrator in consultation with the Registry Operator and Registrars.

3.6. Transport Security

The Registry Access API must implement transport encryption as described in Section 54.

3.7. Authentication

Authentication to the API must utilise the following three factors:

3.7.1. The source IP address of the connection must be one that is known to be under the control of the user attempting to authenticate (i.e. an IP 'white list' must be maintained and no access to the interface should be possible at the network level without an entry on the 'white list');

3.7.2. The client digital certificate presented during the underlying secure session establishment must be valid, known to belong to the user attempting to authenticate, issued by an allowed Certificate Authority (which could be one operated by the Registry Operator), signed using known secure algorithms and contain the identity of the user securely encoded in the client certificate; and

3.7.3. The username and password presented in the EPP login command must be valid and cross reference with the source IP address and client certificate presented during secure session establishment.

3.8. Connection Limits

3.8.1. The Registry Access API may enforce a limit on the number of sessions each client may establish.

3.8.2. Such limit must be applied consistently to all Registrars.

3.9. Rate Limiting

Rate limiting is to ensure equal access to the system for all Registrars. The Registry Operator may impose rate limits to mitigate excessive usage that may threaten the security and/or stability of the Registry System. Rate limits are not intended as a work around for an under resourced Domain Name Registry System. The Registry Operator is expected to be able to meet the minimum performance requirements outlined in the Section 'Performance Levels' at the volumes outlined in that section

3.9.1. The Registry Access API must include a mechanism to define rate limiting on a per-command and overall basis.

3.9.2. The rate limiting must apply on a per-connection basis.

3.9.3. The rate limiting must include an ability to 'burst' above the normal prescribed limit to accommodate traffic that is 'peaky' in nature.

3.9.4. The rate limiting must be documented and communicated to clients in a server policy document.

3.9.5. Changes to the rate limits that result in less access must only be implemented after appropriate notification has been given to clients.

3.9.6. Proposed rate limits must be approved by the Administrator prior to being implemented.

3.9.7. Rate limits must be identical for all Registrars.

4. Registry HTTPS Interface

The Registry HTTPS Interface will be used by Registrars to manually provision and manage objects in the Registry Data Store in accordance with the Business Rules.

4.1. The Registry System must provide a HTTPS provisioning and management interface.

4.2. All functionality that is available through the Registry Access API must be available through the Registry HTTPS Interface.

4.3. The HTTPS management interface should support bulk operations - so that a user can easily update information across multiple objects.

4.4. Authentication

User authentication must utilise the following two factors:

4.4.1. The username and password presented during the login command which establishes the session with the system; and

4.4.2. The user must be provisioned with a One Time Password token the value of which must be verified during login and during all object modification commands.

The Registry Operator may wish to include additional layers of authentication including but not limited to digital certificates.

4.5. The Registry Operator is not required to support 'scripting' against the Registry HTTPS Interface and should implement mechanisms to ensure the security and stability of the Registry HTTPS Interface is not compromised by any such usage.

4.6. The Registry Operator must ensure that the Registry HTTPS Interface is not used as a mechanism to 'work around' the rate limiting configured on the Registry Access API.

4.7. The Registry HTTPS Interface should have 3 effective access levels. Registrar, Administrator and Registry Operator. The Registry Operator and Administrator accounts must have the ability to make changes to all Domain, Contact and Host objects in the Registry Database.

4.8. Accounts and Users

4.8.1. The system should support multiple users associated with the one account (representing one or more Registrar Accreditations, the Administrator or the Registry Operator)

4.8.2. The system must have a full permissions and roles capability, such that the actions that can be performed by a user can be controlled by administrators of that account.

4.8.3. The system must have a full permission and roles capability, such that the actions that can be performed by an account can be controlled by the Registry Operator.

4.8.4. The system must support giving accounts various level of access to namespaces in the system including:

4.8.4.1. None – no access;

4.8.4.2. Read-only – no modification actions;

4.8.4.3. Restricted – can modify existing objects but can't create new ones; and

4.8.4.4. Full – no restrictions.

4.8.5. The account access levels, permissions and roles should also apply to the Registry API and any other interfaces as appropriate.

4.8.5.1. The Registry Access API users should simply be a special case of an account user.

4.9. The Registry HTTPS Interface must provide the following common functionality (for all account types) as a minimum:

4.9.1. A service availability indicator that shows the current status of the Registry Access API, Domain Lookup – WHOIS, Domain Lookup – RDAP, Domain Availability Check, and Authoritative DNS as well (if applicable) which of the Registry locations is currently serving as the primary location for each service.

4.9.2. Contact functionality (e.g. 'check', 'view', 'create', 'update', 'delete', 'view history').

4.9.3. Contact Transfer (e.g. 'list pending', 'approve', 'reject' or 'cancel' as relevant)

4.9.4. Contact Search (filter on combination of fields with a 'query builder').

4.9.5. Domain functionality (e.g. 'check', 'view', 'create', 'update', 'renew', 'unrenew', 'delete', 'undelete', 'PolicyDelete', 'PolicyUndelete', 'Registrant transfer', 'view history', 'expiry sync').

4.9.6. Domain Transfer (e.g. 'list pending', 'approve', 'reject' or 'cancel' as relevant)

4.9.7. Bulk operations (e.g. 'delete', 'undelete')

4.9.8. Domain Search (filter on combination of fields with a 'query builder' including .au extensions).

4.9.9. Domain Search by Contact (domain names linked to a contact).

4.9.10. Domain Search by Host (domain names linked to a host).

4.9.11. Domain Search by Registrant (by common .au extension details).

4.9.12. Host functionality (e.g. 'check', 'view', 'create', 'update', 'delete').

4.9.13. User management (e.g. 'search', 'create', 'delete', 'reset authentication information', 'set and modify permissions', 'suspend access').

4.9.14. Account management (e.g. 'update details', 'manage message assignments').

4.9.15. View zone configuration and pricing information.

4.9.16. Download a list of reserved and restricted domain names.

4.9.17. Check the reason for a domain name being on serverHold or clientHold.

4.9.18. Search the Resellers objects configured in the system.

4.9.19. Search the audit log (i.e. 'transaction history').

4.9.20. View and acknowledge poll messages.

4.9.21. View and download files from the file repository.

4.9.22. View current account balance, set thresholds for warning emails and poll messages, view a billing statement and access invoices.

4.10. The Registry HTTPS Interface must provide the following administrative functionality (Administrator and Registry Operator) as a minimum:

4.10.1. Domain Update Expiry.

4.10.2. Domain functionality (e.g. 'policy delete', 'policy undelete', 'lock', 'unlock', 'policy suspension').

4.10.3. Domain reset Registrant email.

4.10.4. Bulk domain name operations (e.g. 'policy delete', 'policy undelete', 'policy suspension').

4.10.5. Manage pending domain names (e.g. list domains 'pending create' and 'renew' or 'pending Registrant transfer', approve or reject).

4.10.6. Manage reserved and restricted domain names.

4.10.7. Manage resellers objects configured in the system (for Reseller ID).

4.11. The Registry HTTPS Interface must provide the following administrative functionality to the Registry Operator as a minimum:

4.11.1. Account management ('search', 'create', 'update', 'update details', 'adjust permissions', 'adjust zone access').

4.11.2. Manage zone configuration and pricing information.

4.11.3. Manage WHOIS 'black list' and 'white list'.

4.11.4. Manage files in the file repository.

4.11.5. Perform a bulk 'move' of domains from one account to another (when requested to do so by the Administrator).

4.11.6. Manage account balances, invoices and accounting information.

4.12. Other requirements

4.12.1. All search results must be able to be downloaded as a CSV.

4.12.2. The Administrator and Registry Operator must have the ability to perform actions on behalf of other accounts, either by selecting the account, using impersonation or equivalent functionality. The relevant object sponsor should be notified by means of a poll message that the object has been modified by someone other than themselves.

4.12.3. Accounts should have the option to specify that all changes, even those performed by themselves, utilising the Registry HTTPS Interface are notified via poll messages to facilitate keeping local database systems synchronised.

4.12.4. Poll messages notifying about object changes should include the relevant data such that the event can be identified. It is acceptable to require a Registrar to perform an object 'info' command to obtain the new full details of the object.

4.12.5. Registrar searches are limited to domain names that they sponsor; Administrator and Registry Operator can choose to filter by account or search system wide for all namespaces covered under this technical specification.

5. Domain Lookup Service – WHOIS

The Domain Lookup – WHOIS must be available through two interfaces:

The port-43 WHOIS interface (*whois.auda.org.au*); and

The web-based interface (https://whois.auda.org.au/).

The requirements for each are below, as are the common requirements.

5.1. Domain Lookup – WHOIS Query and Response specifications

5.1.1. The system must support the query and response formats as described in Appendix A.

5.1.2. The format may be different depending on which interface is used to make the query.

5.1.3. The precise output may also be different for each namespace under management.

5.1.4. The output of the Domain Lookup – WHOIS must be easily configurable to accommodate changes to the policy in a timeframe specified by the Administrator.

5.2. Rate Limiting

5.2.1. The system must include a rate limiting mechanism to protect against data mining.

5.2.2. The rate limits will be specified by the Administrator, currently these are set at no more than 20 queries in a 1-hour period per IP.

5.2.2.1. The system must be configurable to allow modification of rate limit parameters, being

5.2.2.1.1. Modification to number of queries in a time period (increase or decrease)

5.2.2.1.2. Modification to the time period (increase or decrease)

5.2.2.1.3. Modification to total number of queries per day

5.2.2.1.4. Capable of combining any of the above (.i.e 10 queries per hour, Maximum 30 per day)

5.2.2.1.5.

5.2.3. Once an IP address is 'black listed' they are barred from making queries for 24 hours.

5.2.4. Any query attempt during the 'black listed' period must be answered with the following response:

> BLACKLISTED: You have exceeded the query limit for your network or IP address and have been blacklisted.

5.2.5. A mechanism must exist for the Registry Operator, or the Administrator, to remove an entry from the 'black list' earlier than the 24-hour period as appropriate.

5.2.6. The removal after 24 hours should be an automated process.

5.2.7. It is acceptable that after a reasonable number of times a 'black listed' IP address receives the 'black listed' response they may be blocked using network controls for the remainder of the 24-hour period.

5.2.8. A mechanism must be in place to allow configuring a 'white list' of IP addresses that are able to perform a higher number of queries before breaching the limits, this may potentially be an unlimited amount of queries. These should be configurable on a per IP basis and per subnet basis, where the queries for all subnets are counted together when determining if the limits have been breached.

5.2.9. The 'white List' is intended to be used to provide Registrars, the Administrator and other entities approved by the Administrator with increased access to the Domain Lookup – WHOIS system.

5.2.10. 'White list' entry holders are prohibited from using the 'white list' to provide increased Domain Lookup – WHOIS access to anyone else other than their own internal use, i.e. they cannot allow anyone else to use their 'white List' entries, including by placing a WHOIS lookup service on their own website. The HTTPS 'brandable' interface described in Section 5.4 is intended to be used for this purpose.

5.2.11. The 'black listing' / 'white listing' mechanisms are intended to work across all Domain Lookup – WHOIS interfaces so the limits apply no matter which interface is used for the queries, including a mixture.

5.3. Port 43 WHOIS Interface

5.3.1. The Registry System must provide a programmatic domain name information lookup API at *whois.auda.org.au* utilising the IETF's WHOIS Protocol as defined in RFC3912 – WHOIS Protocol Specification: https://tools.ietf.org/html/rfc3912

5.3.2. The query format for the Port 43 Domain Lookup – WHOIS is as follows:

```
<query string>\r\n
```

Where \r and \n represent the ASCII carriage-return (15) and newline(12) characters respectively; e.g. to retrieve the information about the domain name auda.org.au a client would connect to port 43 and issues the following query input:

```
auda.org.au\r\n
```

5.3.3. To increase the ease of use of the service the Domain Lookup – WHOIS Service should also accept commands that are terminated with just a newline (12).

5.3.4. The input data should be interpreted as, and the returned data should be encoded in, the Unicode Consortiums UTF-8 encoding scheme.

5.3.5. The response should be as specified above, each line terminated by a carriage return (12) and newline sequence (15):

```
<line>\r\n
```

5.3.6. The appropriate WHOIS SRV DNS records should be published in the DNS zones for each namespace covered by this technical specification.

5.4. HTTPS based interface

5.4.1. The Domain Lookup – WHOIS Service must also be provided as a simple HTTPS based web interface; currently https://whois.auda.org.au/.

5.4.2..The Administrator will control the domain name used for the WHOIS service, including the SSL certificate. The service will be delegated to, and operated by, the Registry Operator.

5.4.3. The Domain Lookup – WHOIS Service web interface must only be available over HTTPS and utilise a certificate provided by the Administrator.

5.4.4. The input data should be interpreted as, and the returned data should be encoded in the Unicode Consortiums UTF-8 encoding scheme

5.4.5. This Domain Lookup – WHOIS HTTPS interface must be available as two versions

5.4.5.1. Branded as the Administrator, currently available at the following link: https://whois.auda.org.au/ and

5.4.5.2. An 'AJAX style' API version with corresponding JavaScript library suitable for integration into the Administrator or a Registrars website

5.4.5.3. All versions must ensure that the true source IP address of the query is known and still subject to rate limits. It is not sufficient for the Registry Operator to rely on the user to send through the IP address as a parameter

5.4.5.4. The CAPTCHA requirement described in Section 5.4.65.4.6 applies to these interfaces and must be implemented by the Registry System.

5.4.5.5. These HTTPS versions must hyperlink the following elements:

5.4.5.6. The Registrar Name to the Registrar URL stored in the Registry Database and able to be managed by the Registrar;

5.4.5.7. The Reseller Name to the Reseller URL stored in the Registry Database and able to be managed by the Administrator;

5.4.5.8. Any Contact ID, Contact Name, Host ID, Host Names, Registrar ID, Registrar Name and Domain ID, Domain Name to the corresponding object WHOIS query; and

5.4.5.9. Status Reason fields to describe the meaning behind the status. The Administrator to provide the approved text.

5.4.6. The Domain Lookup – WHOIS HTTPS interface must be protected by a modern CAPTCHA or equivalent (reCAPTCHA/hCAPTCHA) functionality.

6. Domain Lookup Service – RDAP

RDAP was created as a successor to the WHOIS. The Administrator is yet to determine how RDAP should be implemented in the namespaces referenced by this specification however, ICANN requires contracted gTLD registries to implement RDAP and as momentum shifts this will flow on to ccTLDs.

The Domain Lookup Service – RDAP will require the Registry Operator to work with the Administrator in defining the requirements for the service. After which the Administrator and Registry Operator will work together on an implementation plan to deploy an RDAP system during the Registry Licence Agreement period. The following RDAP specifications are to be read as minimum expectations for the implementation of RDAP.

6.1. The Registry Operator must, within a timeframe agreed with the Administrator, provide a Domain Lookup – RDAP Service utilising the IETF's

Registration Data Access Protocol (RDAP) as defined in the following IETF Documents:

RFC7480 – HTTP Usage in the Registration Data Access Protocol (RDAP): https://tools.ietf.org/html/rfc7480

RFC7481 – Security Services for the Registration Data Access Protocol (RDAP): https://tools.ietf.org/html/rfc7481

RFC9082 – Registration Data Access Protocol (RDAP) Query Format: https://www.rfc-editor.org/rfc/rfc9082.html

RFC9083 – JSON Responses for the Registration Data Access Protocol (RDAP): https://www.rfc-editor.org/rfc/rfc9083.html

RFC9224 – Finding the Authoritative Registration Data Access Protocol (RDAP) Service: https://www.rfc-editor.org/rfc/rfc9224

6.2. The Registry Operator should additionally be familiar with, and remain current on, the following RFCs and drafts relating to RDAP

- RFC7485 – Inventory and Analysis of WHOIS Registration Objects: https://www.rfc-editor.org/rfc/rfc7485
- RFC8056 – Extensible Provisioning Protocol (EPP)and Registration Data Access Protocol (RDAP) Status Mapping**:** https://www.rfc-editor.org/rfc/rfc8056
- RFC8521 – Registration Data Access Protocol (RDAP) Object Tagging: https://www.rfc-editor.org/rfc/rfc8521.html
- draft-ietf-regext-rdap-openid-20 – Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect: https://www.ietf.org/id/draft-ietf-regext-rdap-openid-20.html

6.3. HTTPS Interface

6.3.1. The RDAP service must be provided as a simple HTTPS based web interface on a domain name to be determined by the Administrator

6.3.2. The Administrator will control the domain name used for the RDAP service, including the SSL certificate. The service will be delegated to, and operated by, the Registry Operator

6.3.3. The RDAP service web interface must only be available over HTTPS and utilise a certificate provided by the Administrator

6.3.4. The input data should be interpreted as, and the returned data should be encoded in the Unicode Consortiums UTF-8 encoding scheme

6.3.5. The RDAP service must be available for anonymous and authenticated clients. Anonymous clients will be restricted to a very limited response set. Authenticated clients will be permitted access to subsets of data based on authentication profiles

6.3.6. The Registry Operator implementation must be capable of managing multiple authentication and access profiles.

6.4. Rate Limiting

6.4.1. The system must include a rate limiting mechanism to protect against data mining.

6.4.2. The rate limits will be specified by the Administrator and may be profile of source IP based

6.4.3. Once a profile or IP is 'black listed' it is to be barred from making queries for 24 hours.

6.4.4. Any query attempt during the 'black listed' period must be answered with a HTTP 429 Response Code

6.4.5. A mechanism must exist for the Registry Operator, or the Administrator, to remove an entry from the 'black list' earlier than the 24-hour period to be used as appropriate.

6.5. The removal after 24 hours should be an automated process

7. Domain Availability Check Service

The Registry System must provide a programmatic domain name availability check lookup API at *domaincheck.auda.org.au* utilising the IETF's WHOIS Protocol as defined in RFC3912 – WHOIS Protocol Specification, which can be found at the following link: https://www.rfc-editor.org/rfc/rfc3912

7.1. The query format for the Domain Availability Check is as follows:

```
<domain name>\r\n
```

Where \r and \n represent the ASCII carriage-return (15) and newline (12) characters respectively. For example, to check the availability of the

domain name auda.org.au a client would connect to port 43 and issues the following query input:

```
auda.org.au\r\n
```

7.2. To increase the ease of use of the service the Domain Availability Check Service should also accept commands that are terminated with just a newline (12)

7.3. The input data should be interpreted as, and the returned data should be encoded in, the Unicode Consortiums UTF-8 encoding scheme.

7.4. The response for an available domain name should be:

```
Available
```

7.5. The response for an unavailable domain name (due to registration, reservation or any other reason) should be:

```
Not Available
```

7.6. The response for a .au direct domain name that is in contention should be *Priority Hold*.

7.7. The response for a domain name that is on the reserved list should be: *Reserved by Registry*.

7.8. This Domain Availability Check Service should be free of any query limits. However, this does not prohibit the Registry Operator from taking any actions necessary to protect the security and/or stability of the system if the Domain Availability Check Service is being abused.

7.9. The Domain Availability Check Service should also be provided as a simple HTTPS based web interface.

7.10. The Domain Availability Check Service web interface should only be available over HTTPS utilising a certificate from a well-known Certificate Authority. The SSL certificate will be provided by the Administrator.

8. Registrant Password Recovery Service

The Registry System must provide a HTTPS based web interface, currently https://pw.auda.org.au, that allows a Registrant to recover the password

('authinfo') using the Registrant contact email address and view the expiry date of their domain name.

8.1. The Registrant Password Recovery Service web interface should only be available over HTTPS utilising a certificate from a well-known Certificate Authority. The SSL certificate will be provided by the Administrator.

8.2. The Administrator will control the domain name used for the Registrant Password Recovery service, including the SSL certificate. The service will be delegated to, and operated by, the Registry Operator

8.3. The input data should be interpreted as, and the returned data should be encoded in the Unicode Consortiums UTF-8 encoding scheme

8.4. This Registrant Password Recovery should be available as two versions:

8.4.1. Branded as the Administrator

8.4.2. An 'AJAX style' API version with corresponding JavaScript library suitable for integration into the Administrators or a Registrars website

8.4.3. All versions should ensure that the true source IP address of the client is known and still subject to all protections. Relying on the user to send through the IP address as a parameter is not an acceptable mechanism.

8.4.4. The interface must be protected by a modern CAPTCHA or equivalent (reCAPTCHA/hCAPTCHA functionality

8.5. The Registrant Password Recovery service currently works as follows

8.5.1. A user accesses a web interface and must provide the domain name and a requestor name. The service must ensure that the user passes a CAPTCHA style test.

8.5.2. A response page is to be returned containing the following text including obscuring the email address:

> Thank you for your request. An email has been sent to a**********r@auda.org.au with a link to recover your password.

8.5.2.1. The email sent to the registrant does not (must not) contain the Domain Name Password (EPP authInfo) in plain text. Instead it (must) provide further instructions on how to retrieve the domain password and view the expiry date. The method and instruction are to be agreed upon with the Administrator

8.5.2.2. The email should appear to originate from the Administrator;

8.5.2.3. The email should include Administrator branding and details; and

8.5.2.4. The Registry Operator should liaise with the Administrator and ensure that the appropriate SPF records are in place to enable the Registry Operator to send emails on behalf of the Administrator.

8.5.3. The email sent to the user contains a time limited one-time URL (as noted in the 8.6 requirement below) to display the domain name, domain name password and the domain name expiry date.

8.6. The method for retrieving the domain name password and viewing the expiry date must be valid for a limited time (~ 30 minutes). This must be clearly communicated in the email. The link must also be one time use only

9. Registry Lock Service

The Registry Lock Service is a domain name security feature which requires a registrar to complete additional authorisation steps ("unlock") to modify the state of a domain name record. The "locked" status of a domain name is recorded by applying serverDeleteProhibited, serverUpdateProhibited, and serverTransferProhibited statuses to the domain name at the Registry.

The registry lock will prevent standard registrar API functions from modifying the state of the domain name.

9.1. The Registry Operator must provide a mechanism for a registrar to place a domain name on Registry Lock and remove a domain name from Registry Lock on behalf of their Registrants.

9.2. The Registry Operator must provide a mechanism for out of band communication with a Registrar to facilitate the activation and deactivation of the Registry Lock Service.

9.3. This mechanism must not be automated

9.4. This mechanism must require human intervention from the Registry Operator.

9.5. When the Registry Lock Service is requested by a Registrar the Registry Operator must apply the following status codes to the domain name:

9.5.1. serverDeleteProhibited,

9.5.2. serverUpdateProhibited, and

9.5.3. serverTransferProhibited.

9.6. The Registry Lock service must apply to host data if applicable.

9.7. Regardless of the Registry Lock function the domain name lifecycle must proceed as per the Administrator policy.

9.7.1. The domain name must expire if not renewed.

9.7.2. The domain name must be deleted if placed into policy delete.

9.7.3. The domain name must purge as per the timeframes stated in the Administrator policies.

9.7.4. The Registry Lock must remain in place through the expiry, delete and purge timeframes and is only removed upon purge.

9.8. The Registry Lock service must allow the domain name to be renewed whilst in the Registry Lock status.

9.9. The WHOIS and RDAP service must display the status codes noted in 9.5 as well as a Status Reason of Registry Lock

9.10. The Registry Operator must permit unlimited lock/unlock requests from Registrars.

9.11. The Registry Operator must be able to provide a Registrar with a report upon request, listing domain names with Registry Lock

10. Domain Drop List Service

The Domain Drop List Service is a public service that provides a list of soon to be released expired and deleted domains.

10.1. The Registry System must provide a HTTPS based web interface that allows a member of the public to retrieve a list of soon to be released expired and deleted domain names and the specific UTC timestamp they become eligible for release.

10.2. The Domain Drop List Service web interface must only be available over HTTPS utilising a certificate from a well-known Certificate Authority.

10.3. This Domain Drop List should be available as two versions

10.3.1. Branded as the Registry Operator.

10.3.2. An 'AJAX style' API version with corresponding JavaScript library suitable for integration into the Administrators or a Registrars website.

10.4. The output should include a timestamp indicating the time that the list was generated from the authoritative data source, a list of domain names purging that are unrecoverable and the UTC timestamp they become eligible for purge, and a list of domain names purging that are recoverable and the UTC timestamp they become eligible for purge.

11. Domain Statistics Service

The Domain Statistics Service enables the Administrator to use an API to retrieve and publish statistical data about the registry. Currently the Administrator uses the API to obtain a count of registered names in the namespaces. This is displayed on the front page of the auDA website (https://www.auda.org.au/).

11.1. The service must be on an endpoint with an AllowList that verifies credentials and issues a token.

11.2. The service must allow the Administrator to access predetermined services, currently only Domains Under Management count is utilised.

11.3. The service must be configurable to provide additional statistical information access as requested by the Administrator.

12. Integration with Administrator API

The Administrator intends to develop a validation engine that enables the Administrator to perform in-path validation of domain name registrants' eligibility credentials at the time of domain name creation, renewal, registrant transfer, or registrar transfer. The validation engine and its rule set will be securely managed by the Administrator**.**

12.1. The Registry System will be required to have the capability to connect to the Administrators API.

12.2. The Administrator will provide a specification to the Registry Operator once it has been defined and the Administrator will consult with the Registry Operator on an appropriate implementation method.

13. .au direct priority contention resolution

In 2022 the Administrator introduced .au Direct Registrations. The policy defining the priority rules and implementation of registrations in .au direct can

be read at https://www.auda.org.au/policy/auda-rules-au-direct-priority-implementation.

13.1. The Registry Operator must provide a system to support the .au domain names that remain in Priority Hold. The system must be capable of:

13.1.1. Providing a mechanism for the general public to check the priority status of a domain name via HTTPS (see https://www.auda.org.au/tools/priority-status-tool).

13.1.2. Provide a mechanism to check the priority status of a domain name via an API (via https://api.auda.ltd/au/application-status/<label> , where label is the label in front of the .au domain.)

13.1.3. Renewing a priority application (all applications have an anniversary date of 20 September UTC time each year).

13.1.4. Updating an applicant's registration information when the registrant information is updated for the matching eligible domain (e.g., if the registrant information is updated for forexample.com.au, the corresponding application for forexample.au must also be updated). This information will be provided by the Registrar.

13.1.5. Remove an application from Priority Hold where the matching eligible domain is purged from the registry as a result of domain name expiry or a policy delete process for compliance reasons.

13.1.6. Provide a mechanism for an applicant to withdraw an application by sending a link to the registrant contact email address (see https://priority.auda.org.au/).

13.1.7. Provide a mechanism for a registrar to withdraw an application.

13.1.8. Provide a mechanism allowing Registrars to obtain a list of applications under management.

14. DNS Signing and Publication Service

The system must provide a DNS Signing and Publication Service that facilitates changes in relevant Registry data being propagated to the Authoritative DNS Service.

14.1. The update mechanism should utilise DNS Dynamic Updates as described in

- RFC2136 – Dynamic Updates in the Domain Name System (DNS UPDATE: https://www.rfc-editor.org/rfc/rfc2136; and
- RFC3007 – Secure Domain Name System (DNS) Dynamic Update: https://www.rfc-editor.org/rfc/rfc3007,

to update the zone data in real time.

14.1.1. Alternative mechanism to Dynamic Updates are acceptable provided they yield the same high speed updates to the Authoritative DNS network.

14.2. The DNS Signing and Publication service must DNSSEC sign the zone prior to publishing to the Authoritative DNS Service.

14.3. The DNS Signing and Publication System must be located in Australia.

14.4. The DNS Signing and Publication Service must not be directly connected to the Internet, and must use intermediate publication servers that serve no other function other than to publish the DNS changes to the Authoritative DNS and to a server managed by the Administrator as part of the Data Repository Environment requirements.

14.5. The publication servers must only be allowed to communicate with, and allow zone transfers to, known Authoritative DNS and related services.

14.6. All zone transfers must also use TSIG authentication as defined in RFC8945 – Secret Key Transaction Authentication for DNS (TSIG): https://www.rfc-editor.org/rfc/rfc8945

14.6.1. TSIG keys must use a minimum algorithm of hmac-sha256

14.6.2. TSIG secrets must be shared out of band or via encrypted channels with the Administrator for the Data Repository Environment nameserver

14.7. The proposed DNSSEC implementation, key sizes, algorithms, rotation frequencies etc. must be documented in a DNS Practices Statement (DPS) as defined in RFC6841 – A Framework for DNSSEC Policies and DNSSEC Practice Statements which can be found at the following link: https://www.rfc-editor.org/rfc/rfc6841. auDA DNSSEC *Policy Practice Statement* is available at: https://www.auda.org.au/about-auda/corporate-strategies-values-and-policies .

14.7.1. The DPS must be approved by the Administrator.

14.7.2. The Key Signing Key (KSK) and Zone Signing Key (ZSK) minimum key size must be RSA 2048-bit keys

14.7.3. The Key Signing Key (KSK) and Zone Signing Key (ZSK) minimum algorithm type must be 8 (RSA/SHA-256)

14.8. The publication mechanism must include a 'gating' mechanism that prohibits the publication of incorrectly signed, or invalid DNSSEC data.

14.9. A mechanism must be in place that can validate the contents of the zone files against what is implied by the Registry Data Store and alert administrators should any discrepancies be found.

14.10. A mechanism must be in place that is capable of generating the zone files, 'from scratch', based on the information contained in the Registry Data Store.

14.11. The DNSSEC KSK and ZSK, for each managed namespace listed in the specification, must be stored and backed up securely.

14.12. The KSK, for each managed namespace listed in the specification, must be stored securely offline or in a HSM when not actively being used.

14.13. For the .au zone file the Registry Operator must be capable of supporting an offline KSK managed by the Administrator.

14.13.1. The Registry Operator will provide a Key Signing Request (KSR) to the Administrator. The Administrator will sign the request with the KSK it holds and return a Signed Key Request (SKR) to the Registry Operator for inclusion in the .au zone file.

14.13.2. The KSR and SKR must be transmitted out of band and over encrypted channels.

14.13.3. The Administrator and the Registry Operator must ensure sufficient overlap of key and signing procedures to prevent the namespace going BOGUS.

14.13.4. The Administrator and Registry Operator must define a key rollover plan for both the KSK and ZSKs in the .au namespace.

14.13.5. For clarity, the KSK and ZSK for all other namespaces mentioned in this specification are the responsibility of the Registry Operator.

14.14. Delegation Signer (DS) records must be published using the minimum of SHA-256 Algorithm. DS records using SHA1 Algorithm must not be used.

14.14.1. The Administrator is responsible for managing the .au DS records with the parent zone operator.

14.15. The Administrator understands the balance between securing the ZSK and operating a 'real-time', high-performance DNS publication environment and expects the Registry Operator to put in place an appropriate plan for ensuring the securing and protection of the ZSK and the KSK. Such plan must be approved by the Administrator.

14.16. The Administrator may require the Registry Operator to pre-publish KSK and ZSK DNSSEC key records, generated by the Administrator, in each zone mentioned in this specification to meet the requirements of the Administrators Business Continuity Plan.

15. DNS Resolution Metrics

The Administrator operates a DNS Metrics Service that collates DNS log data from all providers of .au authoritative DNS resolution. This allows the Administrator to gain detailed visibility of all .au authoritative DNS services for both reporting and security purposes.

15.1. The Registry Operator must provide the Administrator logging data of all queries and responses that their authoritative DNS service processes. There is some flexibility available for how this data is produced and sent and is documented in 15.12.

15.2. Latency, Retention and Timeliness

15.2.1. The DNS Metrics data made available by the Registry Operator must be complete and error free. There are no allowances available to handle amended/updated/corrected versions of data files.

15.2.2. The Registry Operator will not resubmit amended, versioned or re-issued files.

15.2.3. The most recent data made available must not be any older than 2 hours at any time.

15.2.4. 14 Days of historical data is the minimum amount of data that must be always made available.

15.3. File Transport

15.3.1. The preferred transport method is to make the data available on an AWS s3 bucket or equivalent or push the data files to the Administrators designated S3 bucket.

15.4. Time zones and Formats

15.4.1. UTC must be used everywhere a time or date is represented. This includes

15.4.1.1. All filenames

15.4.1.2. Timestamps

15.4.2. Date and time strings must be ISO 8601 formatted

15.4.2.1. Dates must be in year-month-day order (eg YYYY-MM-DD or YYYMMDD).

15.4.2.1.1. All year strings must be the full four characters (no year abbreviations).

15.4.2.1.2. All day and month values must be zero padded to 2 characters.

15.4.2.2. Time must be in 24-hour-clock format [hh]:[mm]:[ss]

15.5. File naming and directory structures

15.5.1. The Registry Operator must explicitly indicate the time period that each file represents.

15.5.2. All data must be identifiable by file name, or directory structure. It must be possible to identify files for any period of time.

15.5.3. Each and every file produced over time should have a globally unique name.

15.6. File names and or directory structure must specify:

15.6.1. Time period the file represents include date.

15.6.2. If the file contains data from a single node/datacentre.

15.6.3. A version identifier.

15.7. Filenames, directory structure, formatting and periods must be consistent across all files produced.

15.7.1. If no DNS queries were served within a period, an empty file must be produced. There must always be a file for every period.

15.7.2. Individual files should not contain more than 10 minutes of data.

15.8. Data Record Fields - For the record of each DNS request/response the Registry Operator must supply:

15.8.1. Timestamp of the query and of the response

15.8.2. Whether the record is the query, the response, or combined.

15.8.3. Requesting IP

15.8.4. ip_protocol (tcp/udp)

15.8.5. ip_version (v4/v6)

15.8.6. query_type (A, AAAA, etc. Ideally as the numeric value)

15.8.7. query_text (domain being queried)

15.8.8. response_code (NXDOMAIN, etc. Ideally as the numeric value)

15.8.9. size of request & response (you must specify how this size is calculated)

15.8.10. DoBit present in packet.

15.8.11. OP Code

15.8.12. EDNS Present in query.

15.9. Within the file or directory structure the following must be included:

15.9.1. The node name, co-location name, or location identifier that served the query.

15.9.2. A version number (this is to allow the Administrator to handle changes to the format overtime)

15.9.2.1. Example: <**node name**>_<**location**>_queries_**v1**_20220109-051501.bz2

15.10. The query text portion must be explicit of UTF-8 or *punycode (RFC3492)*. These formats must not be mixed.

15.11. Documentation

15.11.1. The Registry Operator must provide detailed documentation explaining their solution to allow the Administrator to assess how it will interface with the Registry Operators data. The documentation must:

15.11.1.1. Give a detailed explanation of each data field.

15.11.1.2. Explain file naming formats.

15.11.1.3. Explain the timeliness of data, how it is produced and when it becomes available.

15.11.2. How the data can be access by the Administrator

15.12. Data Feed Options

15.12.1. Text Logs - A text format in either CSV, JSON or Parquet, with one record per line. To minimise the amount of data being shipped between systems the files must be compressed.

15.12.1.1. Text Logs must not contain XML

15.12.2. Packet Capture (PCAP's) - To minimise the amount of data being shipped between systems the pcap's must be compressed. Unrequired data should be excluded or filtered from the pcap to minimise size and processing time.

15.12.3. API – The Registry Operator may provide data via a HTTPS API. All of the same requirements as file-based data feeds must be met where it makes sense to do so. It also must:

15.12.3.1. Be highly available.

15.12.3.2. Comfortably support more than one consumer at a time (ie: queried by multiple machines simultaneously and handle re-request's of data).

15.12.3.3. Allow a request of data in time-chunks (eg 00:00-00:05) without ambiguity and without missing data in the gaps.

15.12.3.4. Built with a common web API technology (eg HTTP+REST+JSON|HTTP+CSV,etc)

15.12.3.5. Explicitly define how to query the API to be sure the time window is a complete and accurate dataset.

15.12.4. To minimise the data transfer between systems the connection must use HTTP compression.

15.13. Data Feed - Multi query / Chained queries

15.13.1. If the Registry Operator service supports multiple DNS lookups within a single request, (e.g. requesting A and MX records simultaneously, multiple domains) the log data must include all request data. It is acceptable to represent these queries as more than one data records (e.g. multiple lines in a log file), as-if the query had been made in

individual separate requests, however it must be flagged so as the Administrators system can differentiate whether a request/response was a traditional single lookup, or part of a multi-query.

Authoritative DNS Service

16. Authoritative DNS Service

The Registry Operator must provide an Authoritative DNS Service compliant with the following specifications:

16.1. Standard 13 (STD13): https://www.rfc-editor.org/info/std13

- RFC1034 – Domain Names – Concepts and Facilities: https://www.rfc-editor.org/rfc/rfc1034
- RFC1035 – Domain Names – Implementation and Specification: https://www.rfc-editor.org/rfc/rfc1035

16.1.1. RFC 6891 – Extension Mechanisms for DNS (EDNS(0)) (STD 75): https://www.rfc-editor.org/rfc/rfc6891

The Registry Operator should be familiar with, and take into account, the following proposed, Best Current Practice and informational RFCs:

- RFC 1982 – Serial Number Arithmetic: https://www.rfc-editor.org/rfc/rfc1982
- RFC 2181 – Clarifications to the DNS Specification: https://www.rfc-editor.org/rfc/rfc2181
- RFC 2182 – Selection and Operation of Secondary DNS Servers (BCP 16): https://www.rfc-editor.org/rfc/rfc2182
- RFC 3226 – DNSSEC and Ipv6 A6-aware server / resolver message size requirements: https://www.rfc-editor.org/rfc/rfc3226
- RFC 3596 – DNS Extensions to Support IP Version 6 (STD 88): https://www.rfc-editor.org/rfc/rfc3596
- RFC 3597 – Handling of Unknown DNS Resource Record (RR) Types: https://www.rfc-editor.org/rfc/rfc3597
- RFC3901 – DNS IPv6 Transport Operational Guidelines: https://www.rfc-editor.org/rfc/rfc3901
- RFC4343 – Domain Name System (DNS) Case Insensitivity Clarification: https://www.rfc-editor.org/rfc/rfc4343
- RFC4697 – Observed DNS Resolution Misbehaviour: https://www.rfc-editor.org/rfc/rfc4697

- RFC RFC4786 – Operation of Anycast Services: https://www.rfc-editor.org/rfc/rfc4786
- RFC7720 – DNS Root Name Service Protocol and Deployment Requirements: https://www.rfc-editor.org/rfc/rfc7720
- RFC7766 – DNS Transport over TCP – Implementation Requirements: https://www.rfc-editor.org/rfc/rfc7766

Additionally the registry operator may find it useful to review all the IETF RFCs related to DNS of which a list can be found at https://powerdns.org/dns-camel/

16.2. The Authoritative DNS Service must support DNSSEC and comply with the following RFC's and their successors

- RFC4033 – DNS Security Introduction and Requirements: https://www.rfc-editor.org/rfc/rfc4033
- RFC4034 – Resource Records for the DNS Security Extensions: https://www.rfc-editor.org/rfc/rfc4034;
- RFC4035 – Protocol Modifications for the DNS Security Extensions: https://www.rfc-editor.org/rfc/rfc4035

And follow best practices described in

- RFC4509 - Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs), https://www.rfc-editor.org/rfc/rfc4509
- RFC6781 – DNSSEC Operational Practices, Version 2, https://www.rfc-editor.org/rfc/rfc6781 .

16.3. The Authoritative DNS Service must be a highly redundant DNS solution, utilising Anycast and capable of sustaining multiple points of failure.

16.4. The Registry Operator must operate and maintain Authoritative DNS nameservers in every capital city within Australia.

16.5. All Australian nameserver sites must have a connection with at least one Tier 1 Internet Service Provider. This may be a primary connection or peering arrangement.

16.6. In addition to the nameserver sites within Australia the Registry Operator must maintain at least one nameserver site on each continent.

16.7. Each physical location must utilise a reputable, secure data centre meeting the Uptime Institute's Tier 3 (or better) rating.

16.8. Where a cloud provider is utilised to provide DNS Authoritative Service the cloud provider must, at a minimum, have

16.8.1. Multiple Zone availability

16.8.2. Multiple Region availability

16.8.3. Minimum 99.95% uptime at a single zone

16.8.4. Minimum 99.99 uptime across zones and regions.

16.9. Each delegation 'NS' record must be provided utilising both an IPv4 and IPv6 address.

16.10. The Administrator will provide the naming scheme for the nameserver DNS entries. The Registry Operator is responsible for all IP assignments.

16.11. Each location must have access to a minimum of 100Mbps of bandwidth.

16.11.1. Bandwidth should be assessed for each location and increased to 1000Mbps minimum in developed countries.

16.12. The overall network must have a demonstrated QPS capacity of at least 10 million QPS.

16.13. The Registry Operator must utilise multiple peering services to further improve the reliability of the system.

16.14. The Registry Operator must ensure that the Authoritative DNS Service is provided using a diverse architecture including:

16.14.1. Routers, switches, servers and other equipment from multiple vendors;

16.14.2. The use of multiple different operating systems; and

16.14.3. The use of multiple different authoritative DNS server software implementations.

16.15. The Registry Operator must put in place a detailed plan and associated mechanisms for detecting and responding to large scale DOS/DDOS attacks.

16.16. The Registry Operator must ensure that monitoring includes the ability to tell if all individual DNS servers that comprise the Authoritative DNS Service have the latest version of the DNS zone files.

16.17. The Registry Operator must include a mechanism by which the Registry Operator can determine which nameserver is answering DNS queries for a specific Internet location.

Data Repository Environment (DRE)

17. Data Repository Environment

The Administrator will maintain a data repository environment that enables it to store copies of the Registry Operators registry software source code, a complete replication of the registry data and all ancillary software source code. The purpose of this requirement is to allow the Administrator to perform security reviews of the software, facilitate an emergency transition, as well as perform data analysis without impacting or compromising the Registry System.

17.1. The Registry Operator must provide the Administrator with, and keep up to date:

17.1.1. Binary versions of all custom-built Registry components.

17.1.1.1. All updates to the binaries must be provided to the Administrator within 24 hours of the component being utilised in production;

17.1.2. If cloud infrastructure is utilised for the Registry System the Administrator will require all source code of the infrastructure builds including all code for automation configuration.

17.1.3. Source code for all custom-built Registry System components including, but not limited to, the database schema;

17.1.3.1. All updates must be provided to the Administrator within 24 hours of the component being utilised in production.

17.1.4. A near real-time copy of the Registry Database(s);

17.1.5. Near real-time copies of the zone files for all namespaces subject to this specification;

17.1.6. Instructions on how each component in the Registry System fits together to produce a functional Registry;

17.1.7. Instructions on how to build the binary versions from source code;

17.1.8. Information about what 'off-the-shelf' software, including operating systems, are required and current versions in use;

17.1.9. Documentation, help files, operational manuals and user manuals;

17.1.10. Network design documentation identifying number of each component required for a functional Registry System

17.1.11. Documentation describing how the Registry System scales either when under load or to increase capacity.

17.1.12. Binaries, source code and documentation should be uploaded to a secure upload server provided by the Administrator utilising Blob Storage.

17.2. The real time copy of the Registry database can be provided utilising database replication technology. The Administrator will be responsible for snapshotting and backing up its copy.

17.3. Zone files can be provided to the Administrator by allowing the Administrator's stealth name server to zone transfer the zones from the Registry System DNS servers. The Administrator will be responsible for snapshotting and backing up its copy.

17.4. The Administrators 'receiving' servers will not be directly connected to the Internet and the Administrator will directly connect with the Registry System infrastructure and or tunnel over the internet.

17.5. Regardless of connectivity method, traffic between the Registry Operator and the Administrator must traverse all potentially insecure networks in an IPSEC (or similar) tunnel.

17.6. Where feasible, all items should be encrypted and digitally signed by the Registry Operator and instructions on how to decrypt and verify the integrity of said files shall be provided to the Administrator by the Registry Operator.

17.7. The Registry Operator must provide the Administrator with scripts capable of performing basic verification of object counts and other important metrics that verify the integrity of the transfer.

17.8. Any alternative methodology by which the above items are delivered must be approved by the Administrator.

17.9. The Registry Operator must grant the Administrator a license to use their Intellectual Property for the purposes of Registry continuity for a period of six months after termination of the Registry License Agreement including all source code.

17.10. The Registry Operator must provide a list of all Third-Party software licences required to operate the Registry System, and the ability to use these licences on a temporary basis under appropriate commercial terms.

Business Continuity Planning Environment (BCPE)

18. Business Continuity Planning

This section extends the DRE section above enabling the Administrator to operate its own disaster recover environment. The Administrator must be able to replicate the original Registry Environment for the purposes of Disaster Recovery, Emergency Transition planning and demonstrated capability that the Administrator has all the required components to meet these obligations.

18.1. The Administrator will maintain a separate BCPE to the DRE

18.2. The BCPE is not intended to be an exact replica of the Registry Operator's production environment. Instead, the Administrator will use container virtualisation to deploy a scaled version of the Registry System.

18.3. The Registry Operator must provide the Administrator with the information required to scope and cost the size and licensing requirements of the Registry System.

18.4. The Registry Operator must provide the Administrator with schema and other documentation to help the Administrator understand the data structure of the data store and where each piece of information is stored. Such documentation must be kept up to date with software release with

new version supplied to the Administrator as changes are released to production.

18.5. Where requested, the Registry Operator must provide technical support/assistance to the Administrator technical team to debug deployment issues due to changes/modifications in the Registry System software.

18.6. The Registry Operator must provide the Administrator with a dedicated user account for use during the BCPE build and test processes.

18.7. The Registry Operator must provide the Administrator with any scripts/code used to compile, deploy, monitor the build process.

18.8. The Registry Operator must ensure that all software deployments take this system into account.

18.9. The Registry Operator must provide basic training to the Administrator on querying the system and using the query tools.

18.10. It is noted that the Administrator will have to appropriately secure the replicated system to ensure data leaks do not occur. The Registry Operator may be asked to provide advice to the Administrator or how to properly secure the system.

Emergency Transition Plan

19. Emergency Transition Plan

The Administrator is required to have an Emergency Transition Plan for situations where the Registry Operator is unable to execute on its business continuity plan or the Registry Operator is in breach of its agreement.

19.1. The Registry Operator must work with the Administrator to develop an emergency transition plan.

19.2. The Registry Operator and Administrator should use the ICANN emergency transition process, https://www.icann.org/resources/pages/transition-processes-2013-04-22-en, as a guide for developing the emergency transition plan.

19.3. In the event of a Registry Operator failure. The Registry Operator must assist and facilitate the Emergency Transition Plan from which the Administrator may take the following actions:

19.3.1. The Administrator may temporarily resume service itself;

19.3.2. The Administrator may designate an emergency interim Registry Operator of the Registry System for .au (**Emergency Operator**)

19.4. Where action is taken under 19.3, the Registry Operator must demonstrate to the Administrator reasonable satisfaction that it can resume operation of the Registry System without the reoccurrence of such failure.

19.5. At the discretion of the Administrator the Registry Operator may transition back into operation of the Registry System pursuant to the procedures set out in the registry transition process, provided that

19.5.1. The Registry Operator pays all reasonable costs incurred by the Administrator as a result of the designation of the Emergency Operator;

19.6. The Registry Operator and Administrator will co-ordinate regular testing of the emergency transition plan with respect to ensuring that all software and data is available to temporarily resume service.

Miscellaneous Functions

20. Miscellaneous functions

The Registry Operator must deliver the following miscellaneous functions.

20.1. Administrator 'Welcome' Email

20.1.1. The Registry Operator must ensure that for each new, unique Registrant email linked to a new domain name registration a 'welcome email' in a format, and with content, provided by Administrator is sent to the Registrant email address.

20.1.2. The format and content of this email should be configurable, and changes easily be implemented at the request of the Administrator.

20.1.3. The email should appear to be sent from the Administrator.

20.1.4. All appropriate technical configuration (e.g. SPF records) need to be put in place (or work with the Administrator to put in place) to give the email the best chance of being properly delivered.

20.2. Administrator Communications

20.2.1. The Registry Operator must maintain the functionality to send emails to all or part of the contact information maintained in the Registry Data Store on behalf of the Administrator.ie: bulk email

20.2.2. The format and content of this email should be configurable, and changes easily be implemented at the request of the Administrator.

20.2.3. The email should appear to be sent from the Administrator.

20.2.4. All appropriate technical configuration (e.g. SPF records) need to be put in place (or work with the Administrator to put in place) to give the email the best chance of being properly delivered.

20.3. Domain Watchlist

20.3.1. The Registry Operator must implement the functionality to monitor, on behalf of the Administrator, for the registration of domain names that match a list provided by the Administrator.

20.3.2. The list must support wildcards.

20.3.3. Upon observing a registration that matches a domain name on the list, the Administrator should be notified via email.

20.3.4. The email should include details of the domain name registration.

20.4. Registry Operator Website Registrar List

20.4.1. The Technical Registry Operator should maintain on their Registry website a list of all accredited Registrars for the public namespaces subject to this technical specification;

20.4.2. This list should include the name and logo of each Registrar;

20.4.3. Each list item should be hyperlinked to the Registrars website;

20.4.4. This URL should be configurable by the Registrar in the Registry HTTPS Interface; and

20.4.5. The order of the list should be randomised each time it is displayed.

Reporting Functions

21. Reporting Functions

At a minimum the following Reporting functions are required:

- Monthly, Quarterly and Yearly Scorecards;
- Registry License Fee Report; and
- On-demand Business Intelligence (BI) / Reporting capability.

21.1. Monthly, Quarterly and Yearly Scorecards

21.1.1. A reporting service providing the Administrator and Registrars with monthly, quarterly and yearly reports in PDF or similar format containing statistical information about the state of the namespace

21.2. auDA Fee Report

21.2.1. The Registry Operator must generate, monthly, at a time specified by the Administrator a report and corresponding financial calculations in order to support the Administrator invoicing the Registry Operator for the monthly auDA Fee as specified in the Registry License Agreement (RLA).

21.3. On demand Business Intelligence / Reporting Capability

21.3.1. The Registry Operator must provide the Administrator with access to on demand reporting and Business Intelligence (BI) capabilities based on data contained with the Registry System.

21.3.2. The Administrator can request custom reports to be developed that are one-off or delivered at regular intervals, e.g. daily, monthly, quarterly, and annually.

21.3.3. Reports should be deposited on a central repository that has access controls applied.

21.3.4. Reports should be viewable in standard formats like CSV/XLS/PDF or as requested by the Administrator.

21.3.5. The Registry Operator and Administrator should agree upon the delivery SLAs at the time of any new report request based on the complexity of the report type.

Registrar Technical Support Functions

22. Registrar Technical Support Functions

This section of the specification describes the Registrar support services to be provided as part of the Registry operations. These services must be managed and operated by the Registry Operator from within Australia.

The following technical support functions are required:

- Registrar Toolkits;
- Registrar Portal
- Documentation;
- Registrar Accreditation Service;
- Informational 'Public' Website; and
- Technical Support Desk.

22.1. Registrar Toolkits

22.1.1. The Registry Operator must supply a Registrar Toolkit that Registrars can use to help them interface with the Registry Access API.

22.1.2. The Registrar Toolkit must include support for all custom extensions support by the Registry System even if use of those extensions by Registrars is optional.

22.1.3. The Registrar Toolkit must be available in at least one of Java, Python, Ruby, C/C++, PHP or NodeJS.

22.1.4. The Registrar Toolkit must be available in source code under an appropriate open-source license approved by the Administrator..

22.1.5. The Registrar Toolkit must be provided fee-free for all Registrars to use.

22.1.6. The Registry Operator must provide full documentation, including API documentation that specifies how the Registrar Toolkit can be utilised to build a basic Registrar system.

22.1.6.1. Example code demonstrating the usage of the Registrar Toolkit must be included in this documentation.

22.1.7. The Registrar Toolkit must be capable of being used with any standards compliant EPP server.

22.1.8. The Registrar Toolkit and related documentation should be hosted on a public source code repository.

22.1.9. Custom EPP extensions developed should be hosted in public source code repository with appropriate documentation.

22.2. Registrar Portal

22.2.1. The Registry Operator must publish a Registrar Portal that provides Registrars with HTTPS access to:

22.2.1.1. Technical documentation about how the Registry System functions;23;

22.2.1.2. Links to the toolkits and the toolkits documentation;

22.2.1.3. Links to relevant RFCs and internet drafts in the IETFs authoritative repository;

22.2.1.4. Links to custom EPP Extensions and associated documentation;

22.2.1.5. Server policy / acceptable use documents;

22.2.1.6. Technical Support Desk contact details;

22.2.1.7. Environment details for the Registry System environments; and

22.2.1.8. Documentation and requirements about the technical accreditation test including how a provisional Registrar can perform a 'practice run';

22.2.2. Access to the Registrar Portal can be restricted by the Registry Operator however, at a minimum, Registrars (both provisionally accredited and fully accredited) as well as the Administrator must be granted access.

23. Documentation

23.1. The Registry Operator must provide, at a minimum, the following documentation. The number of documents required is left to the Registry Operator to determine, however the following must be covered:

23.1.1. Poll message reference;

23.1.2. Response and error code reference;

23.1.3. Permissions and Conditions matrix for command authorisation;

23.1.4. Full context specific help on the Registry HTTPS Interface;

23.1.5. User manuals for all Registry System services;

23.2. Server policy documents that detail access information and controls such as:

23.2.1. rate limits,

23.2.2. acceptable use,

23.2.3. excessive client activity,

23.2.4. penalties for breach of server policies,

23.2.5. connection limits

23.2.6. Transfer authorisation mechanism; and

23.2.7. User manual for the Registrars and the Administrator.

24. Registrar Accreditation Service

24.1. The Registry Operator must implement a Registrar Accreditation Testing Service to evaluate technical capability and compliance of provisionally accredited Registrars

24.2. The test suite is to be documented and approved by the Administrator.

24.3. Registry Operator may choose to accept 'demonstrable prior experience' as a substitute for conducting technical assessment as long as such policy is documented and applied consistently to all provisionally accredited Registrars.

24.4. Testing requirements are to be adjusted as changes to the Registry System or broader environment necessitates – updates or changes to testing criteria including any substitute policies must be approved by the Administrator prior to coming into effect.

24.5. A provisionally accredited Registrar shall be entitled to attempt the tests three times before to the Registry Operator notifies the Administrator of the provisionally accredited registrars deficiencies.

24.5.1. After each attempt the Registry Operator must provide the provisional Registrar with results and an explanation for failed components.

24.5.2. Results must be available within 48 hours after the provisional Registrar completes the test.

25. Informational Public Website

25.1. The Registry Operator must provide an information public HTTPS website that serves as the 'home' for the Registry.

25.2. This website should include access or links to Domain Lookup – WHOIS, Domain Availability Check, Domain Drop List, the Registrar List, general public information, Administrator policy, Information about becoming a Registrar, the Registrar Information Centre and the Technical Support Desk.

26. Technical Support Desk

26.1. The Registry Operator must operator a technical support desk for Registrars and the Administrator.

26.2. The Technical Support Desk must be available 24 hours a day, 7 days a week.

26.3. From 8am to 8pm Australian Eastern Standard Time (AEST), 5 days a week, excluding public holidays, the Technical Support Desk must be delivered by a team located within Australia.

26.3.1. Outside these hours the Technical Support Desk may be supplied from anywhere in a 'follow-the-sun' arrangement.

26.4. The Technical Support staff must be appropriately qualified and experienced with Registry operations, the DNS and the Registry System.

26.5. The Technical Support Desk must operate a free-call phone number within Australia.

26.6. The Technical Support Desk must utilise a reputable ticketing system and all interactions with the service desk should be logged in said ticketing system.

26.7. During general business hours the Technical Support Desk must support telephone, email and ticketing system contact methods.

26.8. Outside the general hours a 24 hour, 7 days a week emergency support line available for critical issues.

26.9. The Registry Operator must develop a policy describing what is considered a critical issue which must be approved by the Administrator.

26.10. The Technical Support Desk must produce the following monthly reports for the Administrator

26.10.1. Support cases opened categorised by method (email/phone/ticket system)

26.10.2. Support cases closed categorised by method (email/phone/ticket system)

26.10.3. Support case types

26.10.4. Support cases by customer type (Administrator/Public/Registrar Name)

26.10.5. Any other reasonable request by the Administrator .

26.11. The language for all communications with the Technical Support Desk will be English.

26.12. The Technical Support Desk should only action requests that have been submitted by authorised representative(s) of Registrars and the Administrator.

26.12.1. In order to improve the service and ensure customer satisfaction the Registry Operator should conduct regular feedback collection exercises (e.g. a survey). The results of these should be included in the Technical Service Desk reporting to the Administrator.

Hosting Environments

The Registry Operator must provide the following Registry System environments.

27. User Acceptance Testing Environment

27.1. The User Acceptance Testing environment must be utilised when providing new functionality to the Administrator for review and acceptance prior to production release.

27.2. The User Acceptance Testing environment need only be available when requested by the Administrator as part of a change request.

27.3. The User Acceptance Testing environment does not need to be deployed in a highly available configuration.

28. Operation Testing and Evaluation 1 Environment

28.1. The Operation Testing and Evaluation 1 (OTE1) environment must be consistent with the software versions and configurations of the production environment.

28.2. OTE1 is to be used by Registrars to conduct tests of their own software updates and deployments prior to release into production.

28.3. OTE1 should regularly, at least once per calendar quarter, have its data 'refreshed' from the production environment.

28.4. OTE1 must be secured in the exact same manner as the production environment.

28.5. OTE1 does not need to configured with the same 'redundancy' as the production environment, some downtime is acceptable, please see Section 'Performance Levels'.

28.6. The Registry Operator is to consider the OTE1 environment as a production environment.

29. Operation Testing and Evaluation 2 Environment

29.1. The Operation Testing and Evaluation 2 (OTE2) environment is used to provide Registrars and the Administrator with a preview of upcoming software releases prior to deployment into the production environment.

29.2. OTE2 will be used by Registrars to conduct tests of their own software updates and deployments to ensure they are functioning correctly with updated Registry System releases from the Registry Operator

29.3. OTE2 need not be available when there are no upcoming software changes, subject to the Section 'Performance Levels'.

29.4. OTE2 should regularly, at least once per calendar quarter, and each time the environment is redeployed or updated with a new Registry System release, have its data 'refreshed' from the production environment.

29.5. OTE2 must be secured in the exact same manner as the production environment.

29.6. OTE2 does not need to be configured with the same 'redundancy' as the production environment, some downtime is acceptable, see Section 'Performance Levels'.

29.7. The Registry Operator the OTE2 environment is to be considered a production environment.

29.8. At a minimum the OTE2 environment must include all critical Registry services including a DNS updating / synchronisation mechanism, DNSSEC signed zone and name server that can be queried.

30. Production Environment

30.1. The production environment must be fully redundant and deployed in a highly available configuration.

30.2. The production environment must be deployed in at least two independent and geographically separated sites meeting all general requirements outlined in this technical specification.

31. Environment Platform

Regardless of the preferred environment platform that the Registry Operator selects it must be approved by the Administrator.

The Registry Operator is responsible for securing all attributes of the environment including logical and physical regardless of whether or not third

parties are involved. This leads to a design requirement that protects all assets regardless of whether physical access has been compromised.

The locations used for hosting the Registry System and associated systems must meet the following standards:

31.1. Each physical location must utilise a reputable, secure data centre meeting the Uptime Institute's Tier 3 (or better) rating or equivalent standard including:

31.2. Redundant air conditioning;

31.3. Redundant power;

31.4. Fire detection and control systems; and

31.5. 24-hour manned security systems.

The locations used for Registry System redundancy must be situated within Australia, in different states or territories and be at least 500 kilometres apart from each other.

31.6. Registry Operator Owned and Managed Bare Metal

It is required that the equipment is housed in a facility that restricts physical access to the Registry Operator's equipemtn to employees and contractors only. It should not be possible for a third party to gain physical access to the equipment such as in the scenario of a shared rack with multiple customers. Physical security measures should be enforced on monitoring the staff of the facility if they are to gain unsupervised access to the equipment.

31.7. Cloud services

The Registry Operator must abide with the ACSC advice relating to the selection of Cloud Service Providers (CSP), their services and infrastructure design. This includes the advice in the 'Cloud Computing Security for Tenants' publication.

https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-tenants

32. Environment Design

The infrastructure located at each of the Registry System data centres must be;

32.1. Identical, such that the system can operate out of either location and still meet the Performance Levels defined in the Section 'Performance Levels'.

32.2. Have a fully redundant n+1 design such that the failure of any one component will not impact the availability of the Registry System.

32.3. Utilise multiple upstream transit providers.

33. Authoritative DNS Sites

The requirements for DNS sites are detailed in Section 16.

Performance Levels

34. Industry Expectations

The Registry Operator shall provide systems and services that will meet the SLAs defined in this specification at the following anticipated volumes:

Number of Registrars: 33

Anticipated Registrar increase year on year: ~2 additional Registrars

Number of query commands per month: ~60 million with a peak of ~1,500 Transactions Per Second (TPS)

Number of transform commands per month: ~20 million with a peak of ~125 TPS

Number of domain names: ~4.2 million (as at January 2023)

Anticipated domain name growth increase month on month:~1%

Number of WHOIS queries per month: ~100 million with a peak of ~2000 Queries per Second (QPS)

35. Domain Name Registry Service

35.1. Interface - Service Levels

Interface		Registry Access API	Registry HTTPS Interface	Domain Lookup Service - WHOIS	Domain Lookup Service - RDAP*	Domain Check Service	Registrant Password Recovery Service	DNS Signing and Publication Service
Availability		100% Per Month	100% Per Month	100% Per Month	100% Per Month	100% Per Month	100% Per Month	
Performance	**Query**	95% Serviced Within 500ms	95% Serviced Within 1000ms	95% Serviced Within 500ms	95% Serviced Within 1000ms	95% Serviced Within 500ms	95% Serviced Within 1000ms	
	Transform	95% Serviced Within 1000ms	95% Serviced Within 2000ms				95% Serviced Within 2000ms	
	Session	95% Serviced Within 2000ms	95% Serviced Within 2000ms					
	Update Frequency	Must Use Registry Data Store Directly	Must Use Registry Data Store Directly	Registry Data Store Updates published within 5 Minutes for 95% of the Month	Registry Data Store Updates published within 5 Minutes for 95% of the month	Registry Data Store Updates published within 5 Minutes for 95% of the Month	Must Use Registry Data Store Directly	Registry Data Store Updates published within 5 Minutes for 95% of the Month

35.2. Disaster Recovery - Service Levels

Restore Time Objective	Restore Point Objective
4 hours	No Data Loss Allowed

35.3. Scheduled Maintenance - Service Levels

Planned Maintenance Maximum Allowance	Planned Maintenance Notification	Planned Maintenance Window	Extended Planned Maintenance Maximum Allowance	Extended Planned Maintenance Notification	Extended Planned Maintenance Window
4 Hours Per Month	3 Days' Notice	Sunday 00:01 AEST Through Sunday 23:59 AEST	12 Hours Per Month	28 Days' Notice	Sunday 00:01 AEST Through Sunday 23:59 AEST

Note: The Administrator may approve maintenance outside of the allowed service window on a case by case basis.

36. Authoritative DNS Service

36.1. Interface - Service Levels

Interface		DNS Service
Authoritative DNS Service Availability		100% Per Month for Overall Service 99.9% Per Month for Individual Anycast Node (NS Record)
Performance	**UDP DNS Resolution**	95% Serviced Within 400ms
	TCP DNS Resolution	95% Serviced Within 1500ms
	Update Frequency	DNS Updates Published to All Servers Within 5 Minutes for 95% of the month

36.2. Disaster Recovery - Service Levels

Restore Time Objective	Restore Point Objective
No Down Time Allowed	No Data Loss Allowed

36.3. Scheduled Maintenance - Service Levels

Scheduled Maintenance	None Allowed

37. Data Repository Environment

Registry Database	No More than 15 Minutes Out of Date
Zone Files	No More than 5 Minutes Out of Date
Other Artefacts	No more than 24 hours behind the deployment into production

38. Reporting Functions

Scorecards	Must be Delivered No Later than 14 Days After the End of the Period to Which They Relate
Administrator Registry Database (DRE)	No More Than 2 Hours Out of Date

39. Performance Level Measurement

Service Levels will be measured as follows:

39.1. Availability

39.1.1. The Administrator will measure availability by performing relevant functions against the Registry System, and the Authoritative DNS Service from various probe locations around the world. The Registry Operator may be required to provide specific user accounts in the Registry System and whitelist IP addresses to facilitate the Administrators measurement tools Probe measurement:

39.1.2. Registry System

39.1.2.1. Registry Access API: Probes will perform a Registry Access API Command on the Registry Access API at a frequency no less than once per five minutes. Any Probe that is unable to connect to the Registry Access API, or does not receive a response from the Registry Access API within a maximum of five times the allowable Service Level, will consider the parameter being measured to be un-reachable from that Probe until it is time to make a new Registry Access API Command

39.1.2.2. Registry HTTPS Interface: Probes will perform a Registry HTTPS Interface Command on the Registry HTTPS Interface at a frequency no less than once per five minutes. Any probe that is unable to connect to the Registry HTTPS Interface, or does not receive a response from the Registry HTTPS Interface within a maximum of five times the allowable Service Level, will consider the parameter being measured to be un-reachable from that probe until it is time to make a new Registry HTTPS Interface Command

39.1.2.3. Domain Lookup Service - WHOIS: Probes will query the Domain Lookup Service - WHOIS at a frequency no less than once per five minutes. Any Probe that is unable to connect to the Domain Lookup Service - WHOIS, or does not receive a response from the Domain Lookup Service - WHOIS within a maximum of five times the allowable Service Level will consider the parameter being

measured to be un-reachable from that Probe until it is time to make a new query.

39.1.2.4. Domain Lookup Service - RDAP: Probes will query the Domain Lookup Service - RDAP at a frequency no less than once per five minutes. Any Probe that is unable to connect to the Domain Lookup Service - RDAP, or does not receive a response from the Domain Lookup Service - RDAP within a maximum of five times the allowable Service Level will consider the parameter being measured to be un-reachable from that Probe until it is time to make a new query

39.1.3. Domain Availability Check Service:

39.1.3.1. Probes will query the Domain Availability Check Service at a frequency no less than once per five minutes. Any Probe that is unable to connect to the Domain Availability Check Service, or does not receive a response from the Domain Availability Check Service within a maximum of five times the allowable Service Level will consider the parameter being measured to be un-reachable from that Probe until it is time to make a new query.

39.1.4. Authoritative DNS Service:

39.1.4.1. Probes will query each Anycast Node at a frequency no less than once per minute. Any Probe that is unable to connect to an Anycast Node, or does not receive a response from that Anycast Node within a maximum of five times the allowable Service Level, will consider the parameter being measured to be un-reachable.

39.1.5. Unavailability will be determined as follows:

39.1.5.1. Each test should be conducted against the IPv4 and the IPv6 interface of the service under test.

39.1.5.2. In the case of the Authoritative DNS service the test must be conducted against both the UDP and TCP interface of each of the IPv4 and IPv6 interfaces

39.1.5.3. At least 50% of the Probes must detect the parameter being measured to be un-reachable in order for the parameter to be considered 'unavailable'.

39.1.5.4. If either of the IPv4 or Ipv6 interface (over either UDP or TCP for the Authoritative DNS service test) for the service is 'unavailable' then the overall availability for that service is considered 'unavailable' for that period.

39.1.5.5. Periods of maintenance are NOT included in the Service Level calculation.

39.2. Performance

39.2.1. In addition to the availability checks described in this section, each probe will also record the relevant Round Trip Time (RTT) for the parameter being measured.

39.2.2. For all the periods where the service is considered reachable by the Probes, the relevant percentage of queries and/or transactions must be answered in the prescribed time frame.

39.2.3. This calculation will be made on a monthly basis.

39.3. Update Frequency

39.3.1. Registry System

39.3.1.1. Update time is measured by making a relevant change to the Registry System and measuring how long it takes to view the change in the relevant interface under test. This test must be performed no less than once every 5 mins. Where the change appears in the relevant interface in or under the required time the system is counted as performing appropriately for that time period.

39.3.2. Authoritative DNS Service:

39.3.2.1. Update time is measured by making a relevant change to the DNS data and measuring how long it takes to view the change on all DNS servers. This test must be performed no less than once every 5 mins. Where the change appears in the DNS servers in or under the required time the system is counted as performing appropriately for that time period.

40. Technical Support Functions

40.1. Issue Severity Levels And Response Time Frames

40.1.1. The Registry Operator must provide a response and resolution to any reported issue in accordance with the timeframes listed in the following table.

Classification	Severity of Incident	Response Timeframe	Update Frequency	Resolution Target
Severity 1	An incident that involves total failure of the system to operate, or complete interruption of a service, for which a workaround does not exists	15 mins	1 hour	1 hours
Severity 2	An incident that involves service degradation. Note that an incident that would otherwise qualify as a Severity 1 incident for which a workaround exists would be a Severity 2 incident.	30 mins	1 hour	2 hours
Severity 3	An incident that has a limited or minor adverse effect on operations and does not substantially impair the functionality of the service. A workaround may be available.	2 hours	8 hours	8 hours
Severity 4	General usage questions regarding the service and general requests for clarification or information.	4 hours	16 hours	24 hours

40.1.2. Response Time Frame refers to the timeframe within which initial response to a request will be provided.

40.1.3. Resolution Target refers to the time within which the request will be resolved after the initial response.

40.1.4. Should an update be required, it will be provided in the intervals stipulated above, following the initial response.

40.1.5. Technical Support Desk (Incident) Report must be provided no more than 14 calendar days after an incident.

40.2. The Administrator expects the Registry Operator to provide the 24/7 phone numbers for key management and senior technical operations staff to aide escalation in those incidents that would fit a severity 1 or 2 definition. The Administrator will also provide the 24/7 phone numbers for its key management and technical operations staff.

41. System Upgrades and Testing

The Registry Operator may from time to time be required to make modifications that will modify, revise, or augment the features of the Registry System.

41.1. Minor Modifications – 30 Days' Notice

41.1.1. Such updates will be available in the OTE1 environment for a minimum of 4 weeks before deployment to the production system.

41.2. Substantial Modifications – 90 days' notice

41.2.1. Such updates will be available in the OTE1 environment for a minimum of 4 weeks before deployment to the production system.

Operational Functions

42. General

42.1. The Registry Operator must have employees located in Australia who are capable of managing, modifying or resolving issues with the Registry System, Authoritative DNS, WHOIS service, and other associated systems..

42.2. The Registry Operator must have administrative operations staff located in Australia.

42.3. The system must be scalable and always maintain a 'safety margin' of immediately available capacity to ensure that unexpected spikes of a reasonable size can be accommodated.

43. Monitoring

43.1. The Registry Operator must have a fully redundant monitoring system in place monitoring all aspects of the systems.

43.2. The monitoring system must not only look at system level parameters like CPU, memory and disk utilisation but must also perform external checks 'as the user sees the system'. Such checks should include application-level verification of the end-to-end functionality of the system, including making a change in the Registry System and verifying the change is propagated through to the authoritative DNS.

43.3. The Registry Operator should maintain their own external Probes for the purposes of availability and performance checks as well as monitoring and reporting on adherence to SLAs. The Administrator will share notifications from its monitoring probes with the Registry Operator.

43.4. Systems staff must be available 24/7 to respond to issues detected by the monitoring system.

43.5. The Registry Operator must provide the Administrator technical staff with Read Only access to the Registry Operators monitoring systems that relate to the .au namespaces.

44. Time

44.1. All systems must have their time zone set to UTC.

44.2. All systems must have their time securely synchronised with at least two *Stratum 1* time servers (See RFC 5905).

45. Reverse DNS

45.1. All services must have correctly configured 'reverse DNS' lookup mechanisms in place.

46. DNS Recursors

46.1. All recursive DNS servers used by the Registry System infrastructure must perform DNSSEC validation and block access to responses that do not correctly validate.

46.2. All domain names utilised by the Registry System service must have DNSSEC in place chaining all the way to the IANA root.

46.3. The principals outlined in BCP140 – RFC5358 – Preventing Use of Recursive Nameservers in Reflector Attacks must be considered

47. Email

47.1. All mail servers used by the Registry Operator must have appropriate *Sender Policy Framework* (SPF) records as per RFC7208 in place.

47.2. All domain names used for emails associated with this service must have a *Domain-based Message Authentication, Reporting and Conformance* (DMARC) configuration in place as per RFC 7489 with appropriate review and actions being taken on incoming reports.

47.3. All outbound email from the Registry Operator on matters related to the services provided under this technical specification must utilise *Secure/Multipurpose Internet Mail Extensions* (S/MIME) as per RFC 8551 and be authenticated with a digital certificate issued by a reputable authority.

48. IPv4 and IPv6 Internet Protocol Addresses

48.1. All interfaces must be available over both IPv4 and IPv6 addresses.

49. General Security

49.1. All interfaces to the DNS and Registry System must be monitored for abuse, intrusion, data mining, data exfiltration and have appropriate protections in place.

49.2. The Registry Operator must monitor for domain name specific undesirable practices. The Registry Operator must report occurrences of undesirable practices to the Administrator. Practices include, but are not limited to:

49.2.1. Registry and Registrar squatting on names

49.2.2. Using WHOIS, RDAP or Domain Availability Checks to 'front run' potential registrations,

49.2.3. The use of domains names as command and control points for botnets,

49.2.4. Fast flux hosting

49.3. All credential exchanges with users of the system must either be performed over a secure mechanism with someone whose identity has already been asserted or, for example, in establishing an initial interface, by a secure, out of band mechanism, with validation of the recipient.

49.4. All interactions with the Technical Support Department that are requesting access to sensitive information (non-general information) or any modification to information must be securely authenticated, and all such information must be communicated over a secure channel – standard email is not considered a secure channel.

49.5. All accounts to all interfaces must be subject to expiry on non-use, locking out after failed authentication attempts and forced periodic password changes.

49.6. The Registry Operator must have *Distributed Denial Of Service* (DDOS) detection and mitigation mechanisms in place.

50. General rules for all HTTPS interfaces

50.1. All HTTP services covered under this specification must be delivered over *Hypertext Transfer Protocol Secure* (HTTPS) (as per RFC 9110).

50.1.1. If a HTTP interface must exist it must do nothing except immediately redirect to the HTTPS interface.

50.2. All HTTPS interfaces must implement proper security mechanisms based on resources such as the *Open Web Application Security Project* (OWASP).

51. Secure Interfaces

51.1. All secure Registry System interfaces must use a minimum of TLS 1.3 and comply with RFC8446 *The Transport Layer Security (TLS) Protocol Version 1.3*.

51.2. The list of allowed cipher suites, and key sizes accepted by the Registry System is to be proposed by the Registry Operator and approved by the Administrator..

51.3. With the exception of the Registry Access API such interfaces must use digital certificates from known reputable Certificate Authorities, the Registry Access API may utilise a Registry specific Certificate Authority.

51.4. With the exception of the Registry Access API, all other systems that require authentication must, beyond any requirements specified in the services specific Section of this technical specification, use *One-Time Password* (OTP) style multi-factor authentication.

51.5. OTP authentication must also be required for:

51.5.1. Changing own or resetting someone else's password or authentication information;

51.5.2. Generating digital certificates; and

51.5.3. Changing data in the Registry System that can result in impacts to Registrants.

52. Daily Log Reports

The Administrator will provide a *Log Ingestion Specification* as an annexure of this Technical Specification. The Log Ingestion Specification will define the format and elements of log data the Administrator requires the Registry Operator to provide. The Log Ingestion Specification will include log data with time and date stamps for:

- EPP Transactions;
- Web portal transactions;
- Database access transactions;
- WHOIS queries;

In addition the Registry Operator may be requested, by the Administrator, to provide log data, on a per request basis, that relates to:

- Data centre access (if a physical co-location is used); and
- Intrusion Detection System (IDS) logs.

53. Quality Controls

53.1. The organisation must obtain and maintain ISO9001:2015 *Quality Management Systems* or any successor accreditation with a scope that includes all services described in this specification.

54. Security and Operational Controls

54.1. The Registry Operator must implement and maintain a comprehensive security program of technical and organisation measures in compliance with

the Australian Cyber Security Centre's (ACSC) *Strategies to Mitigate Cyber Security Incidents* – also known as the *Essential Eight*.

54.2. The Registry Operator must obtain and maintain *ISO27001:2022 Information security, Cybersecurity and privacy protection accreditation* , or any successor accreditation with a scope that includes all services described in this specification. In addition, the following security controls/documents must be in place:

54.2.1. Overarching security policy with support from senior management;

54.2.2. Third party risk controls covering all third parties involved in the supply of service under this technical specification;

54.2.3. Asset classification and control;

54.2.4. Personnel security;

54.2.5. Physical and environmental security;

54.2.6. Equipment security;

54.2.7. Cabling security;

54.2.8. Equipment disposal;

54.2.9. Communications procedures;

54.2.10. Development security controls;

54.2.11. Capacity planning and controls;

54.2.12. Protections against malicious software, virus' and malware;

54.2.13. Application control (Application whitelisting) process

54.2.14. Disaster recovery, including testing;

54.2.15. Media lifecycle, handling and disposal;

54.2.16. Access control, IAM, privileged access management;

54.2.17. User access review process

54.2.18. System standards, network segmentation standards;

54.2.19. Patch management and Vulnerability detection process

54.2.20. Annual external penetration testing

54.2.21. Network access controls;

54.2.22. Data Loss Detection & Prevention controls; (consider WHOIS and Registry API data mining for example)

54.2.23. Monitoring standards;

54.2.24. Intrusion detection, integrity monitoring;

54.2.25. Security incident detection and management;

54.2.26. Mobile and BYO device management policies and procedures;

54.2.27. Cryptographic controls;

54.2.28. Centralised logging controls;

54.2.29. Security in development and support processes; and

54.2.30. CIS top 18 controls, which can be found at the following link: https://www.cisecurity.org/controls/cis-controls-list

54.3. Cryptography Controls

54.3.1. The Registry Operator must put in place a policy that specifies which encryption and hashing algorithms are appropriate to use in all aspects of the Registry System and DNS systems.

54.3.2. Such policy should also consider algorithms in use in digital certificates as well as encryption protocols.

54.3.3. The policy should also, where relevant, establish the minimum acceptable key size for each algorithm.

54.3.4. The policy must comply with the ASD Approved Cryptographic Algorithm requirements as outlined in the Australian Government *Information Security Manual* which can be found at the following link: https://www.cyber.gov.au/sites/default/files/2022-12/Information%20Security%20Manual%20%28December%202022%29.pdf

54.3.5. Only Suite B SECRET level algorithm and parameters are approved for use.

54.3.6. TLS must be implemented in compliance with the Australian Government ISM control requirements.

54.4. The following operational controls/process/documents, based on *Information Technology Infrastructure Library* (ITIL) or equivalent principals must be in place:

54.4.1. Incident Management, including notification to the Administrator of incidents - security or otherwise;

54.4.2. Problem Management, including provisions for 'outage' or Root Cause Analysis (RCA) reports to be provided to both Registrars and the Administrator;

54.4.3. Change Control;

54.4.4. Release Management;

54.4.5. Risk Identification and Management – results of which should be shared with the Administrator which may result in changes to the service; and

54.4.6. A full capacity management plan must be in place, including monitoring of system capacity and an understanding of system limitations confirmed by realistic testing;

55. Disaster Recovery (DR) and Business Continuity Planning (BCP)

55.1. The Registry Operator must obtain and maintain ISO22301:2019 *Business Continuity Management Systems*, or any successor accreditation, with a scope that includes all services described in this certification.

55.2. The Disaster Recovery Plan must be tested at least once every six months. The Administrator's technical staff are to participate as an observer in each test.

55.3. The results of such tests must be kept and made available to the Administrator upon request.

55.4. The Registry Operator should demonstrate effective Disaster Recovery by testing the switching between the two Registry System sites at least twice a year.

55.5. The DR and BCP documentation must be made available to the Administrator.

55.6. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must meet those outlined in Section 35.2.

56. Risk Management

56.1. The Registry Operator must develop, implement and maintain a comprehensive risk management framework in compliance with *ISO 31000* –

Risk Management to identify and mitigate potential threats to the Registry System, the WHOIS directory server, and the DNS server infrastructure.

56.2. The Registry Operator must develop a written risk management program that complies with the requirements for a *Critical Infrastructure Risk Management Program* (CIRMP) as required under the *Security of Critical Infrastructure Act 2018* (SOCI Act).

57. External Audit and Testing

57.1. The Registry Operator must at least once a year conduct an external audit on all the Security and Business Continuity controls put in place to address the requirements of this specification.

57.2. The results of such audit must be provided to the Administrator including an action plan to address any findings.

57.3. The audit must be conducted by an organisation with demonstrated experience in performing such audits and approved by the Administrator.

57.4. The audit report should follow SSAE SOC2 Type2 or an equivalent format.

57.5. This audit is independent of any required ISO accreditation audits described in Section 53, or Section 54..

57.6. The Registry Operator must, at least once a year, have an independent penetration test performed on the Registry System.

57.6.1. The scope of the penetration test must be approved by the Administrator.

57.6.2. The results and any remediation plans must be provided to the Administrator.

Administrator Relations

58. Working with the Administrator

58.1. The Registry Operator must commit to working co-operatively with the Administrator. Some of the required participation includes, but is not limited to:

58.1.1. Advice / consultancy on future policy requirements and the business and technical feasibility/implications of such decisions.

58.1.2. Customisation to the system:

58.1.2.1. Small changes and/or configuration changes should be performed at no cost; and

58.1.2.2. Larger changes can be quoted and negotiated with the Administrator.

58.1.3. Provide general technical advice and advice on industry trends to the Administrator on domain name related matters.

58.1.4. Participate in Administrator policy panels and other policy development mechanisms where such participation is appropriate.

58.1.5. Participate as a technical specialist in government meetings / discussions as required by the Administrator.

Appendix A. : Domain Name Lookup – WHOIS Query and Response Format

WHOIS query format:

```
[ <keyword> ] [ <modifier> ] [ <searchType> ] <searchString>
```

Where:

keyword is optional and one of 'domain', 'contact', 'host' or 'Registrar'

modifier is optional and one of 'full','fu','=','summary','sum' or '$'

searchType is optional and one of 'name' or 'id'

searchString is a single search string, no whitespace allowed (note this means you can only match against fields containing spaces by using wildcard – this should be addressed)

Note: 'full','fu' and '=' indicate that full results should be returned
'summary', 'sum' and '$' indicate that summary results only should be returned

'keyword': the keyword specifies what object type to search for

'modifier': the modifier specifies whether to return full (all allowed configured information) or summary (summary information only)

For domains the full modifier returns the configured WHOIS output for that namespace, the currently configured options are as follows:

Domain Name:	<domain name>
Registry Domain ID:	<The domain name Registry Object Identifier >
Registrar WHOIS Server:	<URL of the Registrars own whois sevice>
Registrar URL:	<domain sponsoring Registrar home page>
Last Modified:	<last modification date>
Registrar Name:	<domain sponsoring registrar full name>
Registrar Abuse Contact Email:	<domain sponsoring registrar abuse contact email>
Registrar Abuse Contact Phone:	<domain sponsoring registrar abuse contact phone>
Reseller:	<associated reseller object name>
Status:	<domain EPP status> [(<domain EPP status reason>)]*

Status Reason:	<description of Status*
Registrant:	<domain registrant name>
Registrant Contact ID:	<domain registrant contact id>
Registrant Contact Name:	<domain registrant contact name>
Registrant Contact Email:	<domain registrant contact email>**
Tech Contact ID:	<domain tech contact id>***
Tech Contact Name:	<domain tech contact name>***
Tech Contact Email:	<domain tech contact email>**,***
Name Server:	<domain name server name>****
Name Server IP:	<domain name server IP>****,*****
DNSSEC:	<domain DNSSEC status>******
Registrant:	<au extension registrant name>
Registrant ID:	<au extension registrant ID type> <au extension registrant ID>
Eligibility Type:	<au extension elig. type>
Eligibility Name:	<au extension elig. name>
Eligibility ID:	<au extension elig. ID type> <au extension elig. ID>

Note: * this field is repeated for each status value, the brackets and reason are optional and not included if the status does not have a reason associated with it

** through the port 43 interface the email addresses must not be returned and can be omitted or replaced with the following text:
Visit <WHOIS server address> for Web based WHOIS

*** where more than one tech contact is associated with the domain, only the first tech contact is returned

****where more than one name server is associated with the domain, then this section is repeated for each name server

*****this field is repeated for each IPv4 and IPv6 IP address associated with the name server

******if DNSSEC information is associated with the domain in the Registry System this field contains the text 'signedDelegation' otherwise this field contains 'unsigned'

Port 43 Current Example

Domain Name: AUDA.ORG.AU

Registry Domain ID: D407400000002227050-AU

Registrar WHOIS Server:	whois.auda.org.au
Registrar URL:	https://www.auda.org.au/about-auda/contact-us
Last Modified:	2021-08-05T15:18:22Z
Registrar Name:	auDA
Registrar Abuse Contact Email:	
Registrar Abuse Contact Phone:	+61.383414111
Reseller Name:	
Status:	serverDeleteProhibited https://afilias.com.au/get-au/whois-status-codes#serverDeleteProhibited
Status Reason:	Registry Lock
Status:	serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serverRenewProhibited
Status Reason:	Not Currently Eligible For Renewal
Status:	serverTransferProhibited https://afilias.com.au/get-au/whois-status-codes#serverTransferProhibited
Status Reason:	Registry Lock
Status:	serverUpdateProhibited https://afilias.com.au/get-au/whois-status-codes#serverUpdateProhibited
Status Reason:	Registry Lock
Registrant Contact ID:	AUDA
Registrant Contact Name:	CEO
Tech Contact ID:	AUDA
Tech Contact Name:	CEO
Name Server:	KARL.NS.CLOUDFLARE.COM
Name Server:	INGRID.NS.CLOUDFLARE.COM
DNSSEC:	signedDelegation
Registrant:	au Domain Administration Ltd
Registrant ID:	ACN 079 009 340
Eligibility Type:	Company

>>> Last update of WHOIS database: 2023-01-23T09:20:57Z <<<

Web WHOIS Example

Domain Name: AUDA.ORG.AU
Registry Domain ID: D407400000002227050-AU
Registrar WHOIS Server: whois.auda.org.au
Registrar URL: https://www.auda.org.au/about-auda/contact-us
Last Modified: 2021-08-05T15:18:22Z
Registrar Name: auDA
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone: +61.383414111
Reseller Name:
Status: serverDeleteProhibited https://afilias.com.au/get-au/whois-status-codes#serverDeleteProhibited
Status Reason: Registry Lock
Status: serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serverRenewProhibited
Status Reason: Not Currently Eligible For Renewal
Status: serverTransferProhibited https://afilias.com.au/get-au/whois-status-codes#serverTransferProhibited
Status Reason: Registry Lock
Status: serverUpdateProhibited https://afilias.com.au/get-au/whois-status-codes#serverUpdateProhibited
Status Reason: Registry Lock
Registrant Contact ID: AUDA
Registrant Contact Name: CEO
Registrant Contact Email: auda.domains@auda.org.au
Tech Contact ID: AUDA
Tech Contact Name: CEO
Tech Contact Email: auda.domains@auda.org.au
Name Server: KARL.NS.CLOUDFLARE.COM
Name Server: INGRID.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
Registrant: .au Domain Administration Ltd
Registrant ID: ACN 079 009 340
Eligibility Type: Company

>>> Last update of WHOIS database: 2023-01-23T09:23:02Z <<<

The summary modifier returns the following for each matched domain object:

Domain Name: <domain name>

For example:

Domain Name: auda.org.au

For contacts the full modifier returns the following:

Contact ID:	<contact id>
Contact Name:	<contact name>
Contact Email:	<contact email address>*

Note: * through the port 43 interface the email addresses must not be returned and can be omitted or replaced with the following text:
Visit <WHOIS server address> for Web based WHOIS

Port 43 Example

Contact ID:	AUDA
Contact Name:	CEO
Contact Email:	Visit whois.auda.org.au for Web based WHOIS

Web WHOIS Example

Contact ID:	AUDA
Contact Name:	CEO
Contact Email:	auda.domains@auda.org.au

The summary modifier returns the following for each matched contact object.

Contact ID:	<contact ROID>
Contact Name:	<contact name>

For example:

Contact ID:	C12345-AU
Contact Name:	CEO

For hosts the full modifier returns the following:

Host ID:	<host ROID>
Host Name:	<host name>
IP Address: <	host ip address>*

Note: * this field is repeated for each IPv4 and IPv6 address

For example:

Host ID:	H123456-AU
Host Name:	ns1.auda.org.au
IP Address:	2001:db8:0:0:0:0:0:2
IP Address:	192.0.2.2

The summary modifier returns the following for each matched host object:

Host ID:	<host ROID>
Host Name:	<host name>

For example:

Host ID:	H12345678
Host Name:	ns1.auda.org.au

For Registrars the full modifier returns the following:

Registrar ID:	<registrar EPP Client Id>
Registrar Name:	<registrar full name>
Registrar URL:	<registrar URL>
Street 1:	<registrar street 1>

Street 2:	<registrar street 2>
Street 3:	<registrar street 3>
City:	<registrar city>
State/Province:	<registrar state/province>
Postal Code:	<registrar postal code>
Country:	<registrar ISO country ID>
Status:	<registrar status>
Created On:	<create date>
Last Updated On:	<last update date>

For example:

Registrar ID:	auDA
Registrar Name:	.au Domain Administration
Registrar URL:	www.auda.org.au
Street 1:	Lv 19 8 Exhibiton Street
City:	Melbourne
State/Province:	VIC
Postal Code:	3000
Country:	au
Status:	Active
Created On:	01-Jan-1970 00:00:00 UTC
Last Updated On:	04-Dec-2015 06:30:43 UTC

The summary modifier returns the following for each matched registrar object:

Registrar ID:	<registrar EPP Client Id>
Registrar Name:	<registrar name>

For example:

Registrar ID:	auDA

In all cases the field values should be aligned to at least one tab past the longest field label.

Additionally, in all cases if the referenced object does not contain a referenced value then the field label should be omitted from the response as well.

'searchType': the searchType specifies whether to match the searchString against the id or name field of the object

for domains the id searchType is invalid and the name searchType matches the domain name

for contacts the id searchType matches the contact ROID and if no match found then attempts to match the contact ID and the name searchType matches the contact name

for hosts the id searchType matches the ROID and the name searchType matches the host name

for Registrars the id search Type matches the Registrar EPP client ID and the name searchType matches the Registrar full name

'searchString': the searchString may use the '%' character as a wildcard, however there must be at least 5 characters prior to the appearance of the first wildcard character. If a wildcard appears in the search string (explicitly or implicitly) and more than one result is matched, then the summary modifier is to be assumed regardless of which actual modifier appeared in the query string. In all cases a maximum of 10 results is to be returned for a wildcard match. All search strings are to be matched in a case insensitive manner.

If the query is a summary query the searchString contains no wildcard character then the searchString should be treated as if it contains a trailing wildcard character

Defaults:

the default keyword is domain

the default search type is name

the default modifier is full

if the keyword contact is found, the default search type becomes id

If the query is invalid, incomplete, or unable to be properly parsed then the response should be:

Invalid request

Nothing in this specification prohibits the WHOIS response being prefixed and/or postfixed with appropriate legal disclaimers or other notices for users. Such prefix and/or postfix must be approved by the Administrator

Appendix B. : Domain Name Lifecycle

See the Domain Renewal, Expiry and Deletion Policy (2010-01) for a summary of the domain name lifecycle. The table below provides a summary of the various states for a domain name.

Registry Status	Explanation
Cancelled	A domain name application that was pending was cancelled by the requesting account, or a Domain name has been deleted during its refundable period.
Deleted	The domain name has been removed from the Registry System.
Expired	The domain name has passed its expiry date.
Expired Deleted	The expired domain name has been purged from the Registry System. When a domain name goes into this status, the subordinate hosts go into Pending Delete status.
Expired Hold	The domain name has passed its expiry date and been withheld from DNS.
Expired Pending Purge	The domain name has passed its expiry date, has been removed from the Registry System and is no longer eligible for renewal.
Legacy	The domain name was migrated from a legacy system without policy-compliant eligibility information and as a result is subject to constraints on transformation until the domain name is made policy compliant or the Administrator otherwise approves the validity of the domain name registration.
Legacy Expired	The domain name is a legacy domain name (see Legacy status) and has since expired (passed its expiry date).
Legacy Expired Hold	The domain name is a legacy domain name (see Legacy status), has passed its expiry date and is now withheld from DNS as a result of expiry.
Legacy Pending Registrant Transfer	The domain name is a legacy domain name (see Legacy status) and is pending registrant transfer as a result of a registrant transfer request. Transition from this state is dependent on review by the Administrator.
Pending Create	The domain name has been created and requires Administrator approval before the registration is completed.
Pending Delete	A deletion request has been made against the domain name and it is within the deletion grace-period. When a domain name goes into this status, the subordinate hosts go into Pending Delete status.
Pending Delete Expired	The domain name has passed its expiry date and there is an outstanding delete request against it.
Pending Delete Expired Hold	The domain name has passed its expiry date, was removed from the Registry System and there is an outstanding delete request against it.
Pending Delete Expired Pending Purge	The domain name has passed the expiry date, was removed from the Registry System, is no longer eligible for renewal and has an outstanding delete request.
Pending Policy Delete	The domain name has been policy deleted and is within the policy deletion grace period.

Pending Registrant Transfer	A request has been made to transfer domain name from one registrant to another and is awaiting approval, rejection or cancellation.
Pending Registration	A create request for the domain name was received by the Administrator and is awaiting approval.
Pending Renew	A renewal request for the domain name was received by the Administrator and is awaiting approval.
Pending Transfer	A transfer request has been made for the domain name and is awaiting approval, rejection or cancellation.
Pending Transfer Renew	The domain name has performed a combined transfer of ownership and registration renewal request.
Policy Deleted	The domain name has been policy deleted and has been removed from the Registry System.
Registered	The domain name is fully operational within the Registry System.
Rejected	The pending domain name application was rejected by the Administrator.

Appendix C. : EDU.AU Requirements

C.1. Summary of Requirements Specific to edu.au

Education Services Australia (**ESA**) is the auDA accredited registrar for the *edu.au* domain (http://www.domainname.edu.au/) which:

- licenses domain names to education and training organisations eligible under policies approved by .au Domain Administration Limited (**auDA**), with the advice of the edu.au Advisory Committee ;
- provides services to customers to maintain current domain name information; and
- implements the domain policies approved by auDA.

With the exception of specific values for eligibility type and policy reason . edu.au uses the same standard fields under the .au EPP extension as .com.au, in the same or very similar way. For example:

- Registrant Name (entity's legal name)
- Registrant Type and ID (ABN, ACN or other form of incorporation/registration type)
- Eligibility Type
- Eligibility Name (typically business name, trading name, trademark, or project/program name used to meet the allocation criteria under schedule 2, section 1 of the .edu.au registration policy)
- Eligibility ID Type and ID (for edu.au, typically set as "Other" for type and either RTO (*Registered Training Organization*) code, ACECQA (*Australian Children's Education & Care Quality Authority*) code, CRICOS (*Commonwealth Register of Institutions and Courses for Overseas Students*) code, TEQSA (*Tertiary Education Quality and Standards Agency*) code, or other form of accreditation code for the ID)
- Policy Reason

The eligibility, allocation and composition criteria under the edu.au registration policy are assessed manually by the Registrar on receipt of an application and prior to the Registrar submitting the data to the registry system. The data submitted for new registrations is listed above, and otherwise the Registrar uses the standard

registry and web portal functions to update, renew, synchronize, delete and process transfer of registrant requests for .edu.au domains.

The key differences for the .edu.au domain space compared to .com.au are:

1. The inclusion of child zones in edu.au for each of the states and territories (as well as three specific jurisdictions) resulting in domain names being registered at the third, fourth, and fifth levels;
2. edu.au has its own set of eligibility types under the .au EPP extension, which were updated in the 2015 review;
3. edu.au has its own set of policy reason codes under the .au EPP extension; and
4. A number of business rules and processes that relate to legacy auDA policies are still in place or applied to edu.au domains.

C.2. Child Zones

For.edu.au, domain names can be registered using the following extensions at the following levels:

- *domainname***.edu.au** (third level)
- *domainname***.act.edu.au** (fourth level, state/territory based)
- *domainname***.nsw.edu.au** (fourth level, state/territory based)
- *domainname***.nt.edu.au** (fourth level, state/territory based)
- *domainname***.qld.edu.au** (fourth level, state/territory based)
- *domainname***.tas.edu.au** (fourth level, state/territory based)
- *domainname***.vic.edu.au** (fourth level, state/territory based)
- *domainname***.wa.edu.au** (fourth level, state/territory based)
- *domainname***.catholic.edu.au** (fourth level, child zone for the catholic education sector)
- *domainname***.eq.edu.au** (fourth level, child zone for Education Queensland)
- *domainname***.schools.nsw.edu.au** (fifth level, child zone for the NSW government school sector)

The last three child zones (catholic.edu.au, eq.edu.au and schools.nsw.edu.au) were created as a result of migrated registries. Further details on this process can be found in the following edu.au policies:

- Creation of New Child Zones Policy (http://www.domainname.edu.au/pdf/child_zones.pdf)
- Unauthorized Registries Policy (http://www.domainname.edu.au/pdf/unauthorised_registries.pdf)

Registration at the fifth level is prohibited under the .edu.au registration policy (schedule 2, section 3.8) with the exception of .schools.nsw.edu.au which is considered grandfathered.

C.3. Eligibility Types

Below is a list of all eligibility types as they currently appear in the current registry operator's web portal.

It is worth noting that a number of eligibility types were either added or removed as part of the 2015 .edu.au public policy review.

Eligibility Type	Status
Body Serving Overseas Students	Added in 2015
Child Care Centre	Removed in 2015
Education and Care Services (Child Care)	Added in 2015
Education Institution	
Government Body	Added in 2015
Government School	
Higher Education Institution	
Industry Association	Added in 2015
National Body	Removed in 2015
Non-Government school	
Non-profit organization	Removed in 2015
Other	
Parent and Professional Association/Organisation	Added in 2015
Pre-school	
Provider of Non-Accredited Training	Added in 2015
Research Organization	
Training Organization	

Any changes to eligibility types need to be approved by auDA, in accordance with the 2015-03 Policy Change Process Policy

http://www.domainname.edu.au/pdf/change_process.pdf

C.4. Policy Reason Codes

For policy reason codes, .edu.au currently uses 101 - 106, which map to the allocation criteria under schedule 2 of the 2016-02 .edu.au registration policy available at: http://www.domainname.edu.au/pdf/registration.pdf

Policy Reason	Policy Criteria/Requirement
101	.edu.au Registration Policy, Schedule 2, section 1.2(a)(i)
102	.edu.au Registration Policy, Schedule 2, section 1.2(a)(ii)
103	.edu.au Registration Policy, Schedule 2, section 1.2(a)(ii)
104	.edu.au Registration Policy, Schedule 2, section 1.2(a)(ii)
105	.edu.au Registration Policy, Schedule 2, section 1.2(b) and 4.1
106	.edu.au Registration Policy, Schedule 2, section 2.1(f)

Unlike .com.au, .edu.au still requires there be a direct connection between the proposed domain name and either the name of entity applying or the name of project or program the entity owns or administers. Furthermore, domain names using the word "*university*" require approval from the Minister for Education. These connections are tracked via these policy reason codes, and used for reporting of trends to eDAC.

C.5. Business Rules

There are a number of processes and business rules in the current registry system for .edu.au (including its child zones) that differ from the other .au extensions. Any changes to eligibility types need to be approved by auDA, in accordance with the 2015-03 – *Policy Change Process Policy*

http://www.domainname.edu.au/pdf/change_process.pdf.

C.5.1. Renewal Grace Period

For.edu.au, the current renewal grace period is **60 days** after the expiry date as opposed to the 30 days after the expiry for the open .au extensions.

C.5.2. Pending Purge / Domain Deletion

After the renewal grace period, .edu.au domain names are deleted from the registry at random as opposed to the current process for open .au extensions, where the deletion is scheduled according to the drop list.

C.5.3. Transfer of Registrant

The current registry operator software does not allow Transfer of registrant requests that fall within 6 months of the domain name initially being registered, without separate approval from auDA. Note the .edu.au domain space has its own 2015-08 – *Edu.au Transfers (Change of Registrant) policy* http://www.domainname.edu.au/pdf/transfers.pdf that does not have this 6 month requirement, so a new registry operator can remove this restriction.

C.6. Host Create/Update Permissions

The following rules apply to hosts created in edu.au and child zones

Domain Sponsor: Registrar A Host Creator: Registrar A		
Host Type	**Create**	**Create with IP/Update**
z.state.edu.au	Yes	Yes
y.z.state.edu.au	Yes	Yes
x.y.z.state.edu.au	Yes	Yes

Domain Sponsor: Registrar A

Host Creator: Registrar B

Host Type	**Create**	**Create with IP/Update**
z.state.edu.au	Yes	No
y.z.state.edu.au	Yes	No
x.y.z.state.edu.au	Yes	No

Appendix D. GOV.AU Requirements

D.1. Background of gov.au

See: https://www.domainname.gov.au

1. The gov.au Domain Name Policies (**gov.au policies**) apply to third level domains at the Australian Government level (e.g. example.gov.au) and fourth level domains at the State/Territory/Local Government levels (e.g. example.act.gov.au).
2. Gov.au policies have been developed to facilitate the registration and administration of domain names used by Australian, State, Territory and Local Government jurisdictions.
3. Gov.au policies are formally reviewed every 2 years.
4. The Australian Government's Department of Finance (https://www.finance.gov.au/) holds a sub-sponsorship agreement with .au Domain Administration (**auDA**), the industry self-regulatory body, for management of the gov.au domain.
5. The Department of Finance manages the gov.au policies and administration in consultation with an inter-jurisdictional Domain Consultative Committee comprising of representatives from each jurisdiction.
6. Each jurisdiction may apply additional domain policies, standards and guidelines in assessing domain applications.
7. A single agency in each jurisdiction, known as the Domain Provider, has the delegated authority to assess individual domain name applications for that jurisdiction. A list of Domain Providers, and relevant contacts, is available at www.domainname.gov.au/contact-us.
8. Domain Providers
    a. reserve the right to remove a gov.au domain name from the registry if it is considered to be in breach of gov.au policies or the gov.au Registrant Agreement; and
    b. reserve the right to reject an application for a domain name.

D.2. Child Zones

For.gov.au, domain names can be registered using the following extensions at the following levels:

- *domainname***.gov.au** (third level)
- *domainname***.act.gov.au** (fourth level, territory based)
- *domainname***.nsw.gov.au** (fourth level, state based)
- *domainname***.qld.gov.au** (fourth level, state based)
- *domainname***.vic.gov.au** (fourth level, state based)
- *domainname***.wa.gov.au** (fourth level, state based)
- *domainname***.sa.gov.au** (fourth level, state based)

Within gov.au zone, there is a record for http://www.gov.au , and there are "www" entries for the other states and territories.

Domains at the fourth level of **nt.gov.au** are not managed by the registry and are managed with the DNS name service for **nt.gov.au**. There are no WHOIS entries for names at the fourth level of **nt.gov.au**. They effectively operate like a government department website within gov.au – like dta.gov.au.

D.3. Eligibility Types

The only valid eligibility type for all gov.au and children domains is "Other".

The eligibility and naming rules are available at:
https://www.domainname.gov.au/domain-policies/eligibility-and-allocation-policy

The Registrant must be an organisation established by an Act of Parliament or government regulation as a government department or agency; a local government entity; a statutory authority; or other defined government body.

Some educational bodies are also government bodies: educational bodies are encouraged to register domain names in the domain name space provided for that sector (edu.au).

D.4. Policy Reason Codes

Not documented.

1. Gov.au domain names must only be used for the official business of the Registrant.

2. The Registrant Contact must state the purpose of the domain name in their application.
3. The domain name must be used specifically and exclusively for the stated purpose for the duration of the licence period.
4. Only one domain name per stated purpose is allowed. Domain Providers reserve the right to waive this rule where there is a compelling business reason for multiple domain names.

D.5. Business Rules

There are a number of processes and business rules in the current registry system for .gov.au (including its child zones) that differ from the other .au extensions.

D.6. Expiry Procedure

The rules for gov.au (and children) domain expiry are different to that of the other .au zones.

The following steps will apply:

1. On creation a domain's expiry date is set to 23:59:59 on the create date plus the period of registration;
2. Periodically the current registry operator's database runs a job that expires all domains for which the expiry date and time has passed. This job can take anywhere from a few seconds to ten minutes to run. Due to the point above, most domains will expire at 23:59;59 UTC (which is approximately 09:59:59(AEST));
3. Upon expiry, the status of serverUpdateProhibited will be added to the domain with a reason of "Domain Expired". The domain will not be removed from the DNS. Only the renew command can be performed at this point;
4. After **six months** the status serverHold is applied to the domain with reason "Domain Expired". At this point only transfer, transfer-renew and renew commands can be performed. DNS information will be removed;
5. After 14 days the status of pendingDelete will replace serverHold (DNS information will still not be published) and in a random zero to seven day time the domain will be purged from the Registry (no commands can be performed on the domain at this point);
6. Domain renewals add exactly the specified interval to the expiry date;
7. Domain renewals can happen within 90 days of the expiry date, or 14 days afterwards; and
8. Renewals are non-refundable transactions.

D.7. Host Create/Update Permissions

The following rules apply to hosts created in gov.au and child zones:

Domain Sponsor: Registrar A Host Creator: Registrar A		
Host Type	**Create**	**Create with IP/Update**
z.state.gov.au	Yes	Yes
y.z.state.gov.au	Yes	Yes
x.y.z.state.gov.au	Yes	Yes

Domain Sponsor: Registrar A Host Creator: Registrar B		
Host Type	**Create**	**Create with IP/Update**
z.state.gov.au	Yes	No
y.z.state.gov.au	Yes	No
x.y.z.state.gov.au	Yes	No

Where state can be act, nsw, qld, sa, vic and wa.