.au Domain Administration Limited

Registry Technical Specification

AUGUST 2017

1.0 INTRODUCTION

This document defines the technical requirements of the registry service to be undertaken by the registry operator.

2.0 FUNCTIONAL SPECIFICATIONS

The Registry Access Protocol (RAP) is to be the Extensible Provisioning Protocol (EPP) and associated data objects that have been developed by the IETF. EPP is now an IETF Internet Standard STD 69 (https://tools.ietf.org/html/std69). The reference documents are now available at www.rfc-editor.org:

- 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
- RFC3735 - Guidelines for Extending the Extensible Provisioning Protocol (EPP) – Informational RFC
- RFC3915 – Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)
- RFC5910 – Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol – Proposed Standard

All EPP functionality outside of the base EPP RFCs should be documented in Internet-Draft format following the guidelines described in RFC 3735 and be posted publicly on the registry operator's website. The registry operator will provide and update the relevant documentation of all the EPP Objects and Extensions prior to deployment, and will post such documentation on a public website.

The current documentation for EPP extensions required to implement .au policies (https://www.auda.org.au/policies) is located at: https://github.com/AusRegistry/ar-epp-extensions .

Registry Operator shall offer public IPv6 transport for its registration system, in addition to IPv4.

In addition to the access protocols described above the registry operator must also supply a HTTPS based web site for registrars to administer objects they sponsor within the Registry. This web based interface must support all functionality that is supported within the EPP protocol described above, utilising standards compliant HTML (e.g. HTML 5.1) interfaces that are accessible and functional from a variety of browsers (such as Internet Explorer, Firefox, Google Chrome or Safari).

The Web based interface should support Multi-factor Authentication for user access with at least three factors (i.e. something you know, something you have, and something you are).

The registry operator must also supply a HTTPS based web site providing registrars with additional services including:

a) *Domain Listings*: Registrars should be able to access and download a list of all the domains and their details that they currently sponsor within the registry system;

b) *Contact Listings:* Registrars should be able to access and download a list of all the contacts and their details that they currently sponsor within the registry system;

c) *Host Listings:* Registrars should be able to access and download a list of all the hosts and their details that they currently sponsor within the registry system;

d) *Transfer/Correction of Registrant Tools*: These tools allow a registrar to "update" the .au extensions details of a domain name, to facilitate a correction to registrant details, or a transfer of the domain name licence to a new registrant;

e) *Accounting Reports:* This tool allows registrars to cross-reference their registry invoices.

f) *Searching capability:* ability for a registrar to search all domain names under its management matching a keyword, search all domain names under its management associated with a particular contact name, postal address, phone number or email address, search all domain names under its management associated with a particular nameserver, search all nameservers under its management associated with IP address ranges.

All lists, data extracts, etc. should be made available at a minimum in CSV and XML (with a defined schema) format to allow for automated processing of the data by registrars. The data can also be provided in other formats.

2.1 Registry Access Protocol (RAP)

The purpose of the RAP is to allow registrars to perform various operations which are necessary when creating, renewing, transferring, modifying and deleting domain name registrations. The RAP provides a remote interface into the registry database.

The registry operator is required to operate the .au implementation of the EPP. The current EPP implementation has been built to conform with the RFC specifications for EPP. Where the specifications allow for choice, the choices made by the incumbent registry are outlined in the Server Policy document set out in Appendix B.

Nameservers are established as separate host objects in the registry. The nameserver hosts for domain delegation are specified as references to existing host objects.

The current .au extensions to EPP are set out in Appendix C and are subject to change from time to time. The registry operator is required to maintain those extensions unless revised at any time by auDA. Appendix D identifies some specific requirements for *.edu.au*, and Appendix E identifies requirements for *.gov.au*.

Should inadequacies with the RFC protocol emerge, the registry operator must agree to implement the revised version of the protocol at the request of auDA. The registry operator must implement support for the standard protocol and provide updated software toolkits. A reasonable timeframe for implementing and testing revisions to the protocol will be determined by auDA in consultation with the registry operator and registrars.

2.1.1 EPP Software Development Toolkit

The registry operator must provide registrars with a software toolkit which is capable of supporting the full EPP protocol and allowing the protocol to be integrated with the database and interfaces of the registrar's software system. The following requirements apply to the software toolkit provided by the registry operator:

(a) the toolkit must provide an API that supports at least Java and C++. Additional languages may also be supported;

(b) the origin of the toolkit must be identified in the tender, along with details of the supplier if different to the Tenderer;

(c) the toolkit must be available in source code form under an appropriate open-source licence (as defined at www.opensource.org) and on a royalty and fee free basis. Examples of acceptable open licences include the GPL, the Lesser GPL and the FreeBSD licence;

(d) full documentation describing how a registrar can develop a basic registration system using the toolkit must be included;

(e) the toolkit must be capable of operating with any EPP server implementation conforming to the specified version of EPP.

Where a registry operator has more than one software toolkit available, all such toolkits must be equally available to all registrars.

Provision of the toolkit does not preclude the registry operator providing a fully functional registrar software system on a fee basis, provided that the system utilises one of the toolkits it is providing.

2.1.2 EPP Transport and Security

Within the .au domain, the EPP implementation must use the EPP over TCP transport mechanism (see RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP), using the full Transport Layer Security (TLS) v1.2 encryption protocol (RFC 5246), also see RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0). TLS must be utilised to ensure secure and authenticated message interchange. Suitably strong encryption and authentication must be employed, and the actual cryptographic algorithms and authentication scheme(s) are subject to approval by auDA.

The primary mechanism for registrar authentication must be using the EPP <login> as described in the relevant RFC. The initial client passwords must be assigned by the registry operator and delivered by a secure out-of-band mechanism. This is in addition to any authentication provided at the transport layer.

2.1.3 Other EPP Requirements

Additional restrictions are required for the registry EPP implementation. These include:

(a) the languages supported by the EPP implementation must include English;

(b) the standard RAP operations (<create>, <delete>, etc.) must be identical for all .au domains and for all registrars. Differences must be limited to data content related to rules and policies applying to different domains. In addition, the data collection policy with regard to registry data must be identical for all registrars;

(c) transaction details for all transform commands including transaction identifiers must be logged. Full transaction details for query commands need not be logged however a log of the number and type of query commands per registrar should be maintained;

(d) EPP commands must be restricted to authorised clients and to clients with appropriate requirements, e.g. sponsoring clients, issuing client, requesting and responding clients, etc.;

(e) client identifiers must be globally unique;

(f) contact Repository Object Identifiers (ROIDs) must be prefixed by a local identifier;

(g) performance profiles such as excessive client inactivity, session longevity, delay time for the automatic approval or rejection of transfer request must be documented in a server-specific profile document that describes default server behaviour.

The current EPP implementation settings are described in Appendices B and C, and any future implementation of the registry software should ensure backward compatibility for registrars wherever possible.

2.2 Registration Service

The registry database used in the registration service provided to registrars is to be based on the descriptions which define 'registrar', 'domain', 'contact' and 'host' objects used in the .au implementation of the EPP (see the Server Policy document at Appendix B).

Any future implementation of the registry software should ensure backward compatibility for registrars wherever possible.

The database used in the registry must be configured to be ready to support the full spectrum of UTF-8 encoded characters, in order to support the language requirements of the registry today, as well as meet future requirements with regard to internationalisation and Internationalised Domain Names (IDN) support.

The registry should only accept characters in social data fields (i.e. company names, personal names, address, etc.) within the Unicode code pages of Basic Latin, Latin-1, Latin Ext-A and Latin Ext-B. (U+0000-U+024F). Registered domain names must be restricted to legal names under current auDA policy. The registry system should be adaptable such that should auDA policy change on permissible code points, the new policy is straightforward to adopt.

The registry should accept IDNs as authoritative name server host names, and in email addresses in contact objects. Such domain names must be expressed in their ACE-form as well as (optionally) their IDN-form when displayed by the registry via WHOIS etc.

For example:

```
Registrant Contact Name: David Müller
Registrant Email: david@müller.xy [david@xn--mller-kva.xy]
Name Server: autorité.example.com.au [xn--autorit-
hya.example.com.au]
Name Server IP: 192.168.48.219
```

The actual recording format within the registry database will be implementation dependent.

2.2.1 Registration Service Performance and Availability

The following performance and availability criteria are to be met by the registry database. Definitions for performance criteria are provided in Appendix A:

a) Service availability: At least 99.9% per calendar month;

b) Processing time: At least 95% of queries serviced within 0.5 seconds. At least 95% of create/modify/delete requests serviced within one second;

c) Planned outage: limited to a maximum of 4 hours per calendar month; between 0001 and 1200 AEST Sundays. 3 days notice to be given to Registrars;

d) Extended planned outage: limited to a maximum of 12 hours per quarter; between 0001 and 2400 AEST Sundays. 28 days notice to be given to Registrars.

2.2.2 Testing Registrar

auDA may use a testing registrar for the purpose of measuring the service levels. The registry operator should not provide any differentiated treatment for the testing registrar, other than no billing of transactions.

2.2.3 Registry Lock function

The registry operator must implement a registry lock function to allow registrars to place a registry lock on high value domain names at the request of the registrant. The registry lock will prevent standard registrar API functions from modifying the state of the domain name. The domain name will have a serverDeleteProhbited and serverUpdateProhibited status. Note that domain name expiry and domain name purge lifecycle events will continue as per the configuration of the .au, or second, third, or fourth level names spaces within .au under management of the registry.

The registry operator must provide a mechanism for a registrar to place a name on lock and remove a lock on behalf of their registrants. The mechanisms should incorporate methods to authenticate the requests of the registrar.

The current service is described here:
https://www.ausregistry.com.au/aulockdown

2.2.4 Domain Sync function

The registry operator must implement a *domain sync* function in accordance with the 2010-01 – Domain Renewal, Expiry and Deletion Policy (https://www.auda.org.au/policies/index-of-published-policies/2010/2010-01). This allows a registrar to change the expiry date of a domain name under management to a date before the current expiry date. This facilitates the use case where a registrant may wish to align a group of domain names to a common expiry date, to help facilitate payment and management of the domain name licences.

2.2.5 Reseller ID Support

The registry operator must implement support for a reseller ID as described 2014-09 – Reseller ID Application Form (https://www.auda.org.au/policies/index-of-published-policies/2014/2014-09/). A reseller of a Registrar may apply to auDA for a unique reseller ID.

The Reseller ID is provided to the reseller for the purposes of:

a) associating the Reseller ID with domain names under management, for inclusion in the WHOIS record; and

b) bulk transferring Reseller ID associated domain names from one registrar to another registrar

Once the reseller has provided the Reseller ID to the registrar, the registrar must associate the Reseller ID with any newly created domain names under the reseller's management. The Reseller ID is an additional data element supported via the .au EPP extensions.

2.3 Authoritative Nameserver Service

The registry operator must provide authoritative nameservers for the domain(s) it operates. This will include .au at the top level, as well as the second, third, and fourth level namespaces within .au that are managed by the registry. The registry operator shall comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF), including all successor standards, modifications or additions thereto relating to the DNS and name server operations including without limitation:

- RFC 1034 – Domain names – concepts and facilities (part of STD 13)
- RFC 1035 – Domain names – implementation and specification (part of STD 13)
- RFC 1123 – Requirements for Internet Hosts – Application and Support (part of STD 3)
- RFC 1982 – Serial Number Arithmetic
- RFC 2181 – Clarifications to the DNS Specification
- RFC 2182 – Selection and Operation of Secondary DNS Servers (BCP 16)
- RFC 3226 – DNSSEC and IPv6 A6-aware server / resolver message size requirements
- RFC 3596 – DNS Extensions to Support IP Version 6 (STD 88)
- RFC 3597 – Handling of Unknown DNS Resource Record (RR) Types
- RFC 4343 – Domain Name System (DNS) Case Insensitivity Clarification
- RFC 5966 – DNS Transport over TCP – Implementation Requirements
- RFC 6891 – Extension Mechanisms for DNS (EDNS(0)) – STD 75

DNS labels may only include hyphens in the third and fourth position if they represent valid Internationalized domain names (IDNs) (as specified above) in their ASCII encoding (e.g., “xn--ndk061n”).

The registry operator must also commit to the implementation and operation of DNS extensions in such areas as internationalization, IDNs, security, *et cetera* when these have been adopted by the IETF and have achieved a satisfactory level of community support, and subject to negotiations with auDA.

The registry operator shall be able to accept IPv6 addresses as glue records in its registry system and publish them in the DNS. The registry operator shall offer public IPv6 transport for, at least, two of the .au name servers listed in the root zone with the corresponding IPv6 addresses registered with IANA. The registry operator should follow BCP 91 (RFC 3901) DNS IPv6 Transport Operational Guidelines (https://www.rfc-editor.org/rfc/rfc3901.txt)

and the recommendations described in RFC 4472 - Operational Considerations and Issues with IPv6 DNS**.**

The registry operator shall sign its zone files implementing **Domain Name System Security Extensions ("DNSSEC")**. For the absence of doubt, the registry operator shall sign the zone file of .au, and the second, third and fourth level names spaces managed by the registry and zone files used for in-bailiwick glue for the namespace's DNS servers.

The registry operator shall comply with the following RFCs and their successors:

- RFC 4033 – DNS Security Introduction and Requirements
- RFC 4034 – Resource Records for the DNS Security Extensions
- RFC 4035 – Protocol Modifications for the DNS Security Extensions
- RFC 4509 - Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs),

and follow the best practices described in:

- RFC 6781 – DNSSEC Operational Practices, Version 2

If the registry operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors.

The registry operator shall accept public-key material from child domain names in a secure manner according to industry best practices. The registry shall follow the 2014-08 – DNSSEC Policy and Practice Statement (DPS) for the *.au* top level domain (https://www.auda.org.au/policies/index-of-published-policies/2014/2014-08). The registry operator shall publish its DPS following the format described in RFC 6841 – *A Framework for DNSSEC Policies and DNSSEC Practice Statements* - describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material. DNSSEC validation must be active and use the IANA DNS Root Key Signing Key set (available at https://www.iana.org/dnssec/files) as a trust anchor for the registry operator's registry services making use of data obtained via DNS responses.

Any changes to the host names or IP addresses of any of the authoritative nameservers must be subject to prior notice to the technical contact for the parent domain (e.g.. changes to com.au nameservers must be notified to the .au zone administrator).

2.3.1 Nameserver Reliability

In compliance with the relevant RFCs, the authoritative nameserver service must be implemented using sufficient nameservers to maintain high levels of availability. The registry operator must operate and maintain a minimum of two nameservers within Australia, and a minimum of two additional namservers

outside of Australia, e.g. located in the USA and Europe. auDA will set up measurement points in the Australian capital cities along with key cities around the world, to measure DNS responses to ensure they meet the service levels in section 2.3.4. The master nameserver should reside in Australia. The registry operator may cooperate with other registry operators, carriers, or ISPs to host DNS nameservers. The registry operator will be responsible for achieving the levels of service specified below. It is expected that all registry operator nameservers will be located in a commercial carrier-class data centre, with redundant network connections (through multiple telecommunication carriers) of at least 10 Mbps capacity each, redundant air-conditioning systems, redundant power supplies (including UPS and power backup), fire detection and control systems, and 24-hour manned security systems. It is also permissible to use public cloud based nameservers.

The registry operator should note that geographical and carrier dispersion of nameservers is considered essential for reliability (see RFC2182 *Selection and Operation of Secondary DNS Servers*). Each name server location should operate in a high availability configuration using redundant servers (including network level redundancy, end-node level redundancy and the implementation of a local balancing scheme where applicable). The registry operators must have personnel available at all times to respond to extraordinary occurrences.

The registry operator shall be required to diversify software amongst the nameservers so that at least one nameserver shall run using different operating system and DNS software from the others.

The registry operator must obtain the consent of auDA before deploying any new technologies.

2.3.2 Zone File Maintenance

The registry operator will use the registry database as the authoritative source for creation of zone file information. Registry database updates must be reflected in answer from all authoritative nameservers within 5 minutes of completion.

2.3.3 Provision of Zone Files to auDA and Zone Transfers

A copy of the zone files under management in the registry must be made available to auDA on a daily basis.

All live nameservers must be configured to reject dynamic update requests from outside the registry.

All zone transfers should be securely transferred between nameservers, with a method of both authenticating and validating the source and validating that the zone transfer was not corrupted or modified on its way. An example of one such method of implementing this would be the use of TSIG signed zone transfers, see RFC 2845 - *Secret Key Transaction Authentication for DNS (TSIG).*

2.3.4 DNS Service Performance and Availability

The following performance and availability criteria are to be met by the authoritative nameservers. The registry operator shall arrange independent monitoring and auditing of performance and availability and those monitoring and auditing reports shall be provided to auDA on a monthly basis. Definitions for performance criteria are provided in Appendix A:

(a) Overall DNS service availability: 100% per calendar month;

(b) Service availability per registry operator nameserver site: At least 99% per calendar month;

(c) Processing time - nameserver resolution: At least 95% to be processed in less than 0.25 seconds;

(d) Update delay time: At least 95% of updates to the registry database available to the nameserver service within 5 minutes;

(e) Overall registry operator DNS service planned outages: Nil;

(f) Cross-network nameserver round trip time: Under 300 msecs.

2.3.5 Wildcard Prohibition

For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFCs 1034 and RFC 4592 – *The Role of Wildcards in the Domain Name System* or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a “Name Error” response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the registry operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

2.3.6 Malicious Use of Orphan Glue Records.

Th registry operator shall take action to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

2.3.6 Network Ingress Filtering

The registry operator shall implement network ingress filtering checks for its registry services as described in BCP 38 / RFC 2827 – *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, and BCP 84 / RFC 3704 – *Ingress Filtering for Multi-homed Networks*.

2.4 Registration Data Directory Service

The registry operator must provide auDA with a full data set containing the objects associated with each domain name space within *.au* under management of the registry operator at least once in each 24 hours. The data set is to be provided as a single XML document. Data sets will be XML version 1.0, UTF-8 encoded documents conforming to the specification described in Section 2.2 and a Registration Data Directory document type definition that will be developed by auDA.

2.4.1 Registry-provided Registration Data Directory Service

The registry operator must provide a reliable public Registration Data Directory service (historically called a WHOIS service) for the *.au* name spaces under its management. The registry operator will operate a **WHOIS service** available via port 43 in accordance with RFC 3912 – *WHOIS Protocol Specification*, and a web-based Registration Data Directory Service at <whois.org.au> providing free public query-based access.

The WHOIS service must be fully compliant with RFC 3912 and must conform to auDA's stated policies with regard to each .au name space. See 2014-07 Whois Policy (https://www.auda.org.au/policies/index-of-published-policies/2014/2014-07). In particular, auDA will specify:

(a) the information which may be provided as a result of a WHOIS enquiry. This may vary between .au name spaces;

(b) the nature of the queries that may be serviced, in particular the fields against which searches can be made, and the extent to which “wild-card” searches can be accepted;

(c) the performance and service levels of the WHOIS service.

As well as the port 43 WHOIS service, the registry operator will need to provide a web based WHOIS page for public use in which branding and/or advertising is kept to a minimum, as well as a generic un-branded web based WHOIS interface that registrars can use on their websites. In both cases search keys are to be limited to domain name only.

2.4.2 WHOIS Data Set

The following information is to be available from the registry database as a result of a WHOIS enquiry. Fields within this set may be restricted by auDA policy for some *.au* name spaces.

(a) The fully qualified domain name;

(b) the hostnames of the primary nameserver and at least one secondary;

(c) the corresponding IP addresses of those nameservers;

(d) the identity of the registry operator;

(e) the identity of the registrar;

(f) the name, postal address, email address, voice telephone number, and (where available) fax number of the registrant;

(g) the name, postal address, email address, voice telephone number, and (where available) fax number of the technical contact for the domain name;

(h) the name, postal address, email address, voice telephone number, and (where available) fax number of the administrative contact for the domain name;

(i) the original creation date of the domain and term of the registration; and

(j) the date of the most recent update of any part of this set of information.

The WHOIS service may be provided either directly from the registry database or from a database dedicated to the service. If a dedicated database is used, it must be regularly updated from the registry database (see below for minimum update delays.) The registry operator must be able to demonstrate that integrity will be maintained between the WHOIS files (if any) and the registry database.

2.4.3 WHOIS Enquiries

The public WHOIS service to be provided by the registry operator is to be oriented towards providing information about specific domain names or constrained sets of domain names.

The following search keys are to be accepted by the registry-provided WHOIS services. Searches are to be case insensitive:

(a) the name of the domain;

(b) the hostname of a primary or secondary nameserver;

Repeated public WHOIS enquiries from individual hosts are to be limited to a specific number in a given time period (currently 20 queries/hour, 200 queries/day). Hosts exceeding this limit are to be blacklisted for a set period of 24 hours. These limits may not apply to authorised registrars and other parties authorised by auDA from time to time. Support for larger limits to individual clients is also required.

2.4.4 Format of WHOIS Information

The information to be provided by WHOIS service will consist of multiple lines of UTF-8 text terminated by ASCII CRLF. Each item or group of items as listed above is to be preceded by a short description.

The current WHOIS fields are described in 2014-07 – WHOIS Policy available at: https://www.auda.org.au/policies/index-of-published-policies/2014/2014-07 The registry data available for public display should be a configurable item in the registry software, so that auDA can vary the information made public from time-to-time as a result of policy review processes.

Field Name	Field Description
Domain Name	Registered domain name
Last Modified	Date the domain name record was last modified
Status	Status of the domain name (e.g. "OK", pendingTransfer, pendingDelete)
Registrar Name	Name of the registrar of record
Reseller Name	Name of the recorded reseller (if applicable)
Registrant	Legal Name of the registrant entity (e.g. company name)
Registrant ID	ID number associated with the registrant entity, if any (e.g. ACN for company)
Eligibility Type	Registrant's eligibility type (e.g. Company)
Eligibility Name	Name used by the registrant to establish eligibility, if different from their own legal name (e.g. registered business name or trademark)
Eligibility ID	ID number associated with the name used by the registrant to establish eligibility (e.g. BN for registered business name, TM number for registered trademark)
Registrant Contact ID	Registry code used to identify the registrant
Registrant Contact Name	Name of a contact person for the registrant
Registrant Contact Email	Contact email address for the registrant
Tech Contact ID	Registry code used to identify the technical contact
Tech Contact Name	Name of a technical contact for the domain name (e.g.. Registrar, reseller, webhost or ISP)
Tech Contact Email	Contact email address for the technical contact
Name Server	Name of computer used to resolve the domain name to Internet Protocol (IP) numbers (minimum of 2 name servers must be listed)
Name Server IP	IP number of the name service (IPv4 ad IPv6)
DNSSEC	DNSSEC status (whether the name is signed or unsigned)

The following may be taken as an example of a suitable format:

```
Domain Name: auda.org.au
Last Modified: 10-Oct-2016 00:19:12 UTC
Status: OK
Registrar Name: auDA

Registrant: .au Domain Administration Ltd
Registrant ID: ACN 079 009 340
Eligibility Type: Company

Registrant Contact ID: AUDA
Registrant Contact Name: CEO
Registrant Email: auda.domains@auda.org.au

Tech Contact ID: AUDA
Tech Name: CEO
Tech Email: auda.domains@auda.org.au

Name Server: karl.ns.cloudflare.com
Name Server: ingrid.ns.cloudflare.com

DNSSEC:   signedDelegation
```

2.4.5 WHOIS Service Performance and Availability

The following performance and availability criteria are to be met by the WHOIS service. Definitions for performance criteria are provided in Appendix A:

(a) Service availability: At least 99.9% per calendar month;

(b) Processing time: At least 95% of enquiries serviced within one second;

(c) Update delay time: At least 95% of updates to the Registry Database available to the WHOIS service within 5 minutes;

(d) Planned outage: Limited to a maximum of 4 hours per calendar month; between 0001 and 1200 AEST Sundays. 3 days notice to be given to Registrars;

(e) Extended outage: Limited to a maximum of 12 hours per quarter; between 0001 and 2400 AEST Sundays. 28 days notice to be given to Registrars;

(f) WHOIS limits: Maximum number of matches to be returned in response to a query: 10. Maximum number of queries to be accepted from a single host: 20 per hour and 200 in any 24-hour period. Blacklist period: 24 hours.

2.4.6 Domain Availability check

The registry operator must also provide a mechanism for resellers and public users to perform domain checks. A domain check is a simple, fast text based command response interface where a client connects, sends the domain string and gets an “available” or “not available” response. No information about the domain name is to be returned except its availability status. The incumbent registry currently provides this service through a WHOIS compliant port-43 service operating independently of the regular WHOIS service.

The registry operator shall (subject to approval by auDA) be entitled to take reasonable measures to limit the volume of domain checks to prevent, for example, denial of service attacks.

The registry operator will implement the current method for backward compatibility, but additional methods – e.g via RDAP are also acceptable.

2.4.7 Registry Data Access Protocol (RDAP) service

The registry operator will also implement a **Registry Data Access Protocol (RDAP)** based service.

The RDAP service must implement the following RFCs:

- RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)
- RFC7481 - Security Services for the Registration Data Access Protocol (RDAP)
- RFC7482 - Registration Data Access Protocol (RDAP) Query Format
- RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)
- RFC7484 - Finding the Authoritative Registration Data (RDAP) Service

The RDAP service must be provided over HTTPS only. The RDAP service must use the best practices for secure use of TLS as described in RFC 7525 (BCP 195) - *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* or its successors.

A client must be able to successfully validate the TLS certificate used for the RDAP service with a *TLSA* record from the DNS (RFC 6698 - *The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA* and RFC 7671 – *The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance*) published by the registry operator. The *Certificate Usage* field of the *TLSA* record MUST have a value of 1 or 3.

The TLS certificate used for the RDAP service must be issued by a Certificate Authority (CA) trusted by the major browsers and mobile operating systems such as the ones listed in the Mozilla Included CA Certificate List (https://wiki.mozilla.org/CA:IncludedCAs). The TLS certificate used for the RDAP service must be issued by a CA that follows the latest CAB Forum Baseline Requirements (https://cabforum.org/baseline-requirements-documents).

The RDAP service must support both GET and HEAD types of HTTP methods. HEAD requests are used to verify the existence of an object in the database, as specified in RFC 7480 – HTTP Usage in the Registration Data Access Protocol (RDAP).

The RDAP Operational Profile will be jointly developed by the registry and auDA, in consultation with registrars and the public. It will use as a starting point the operational profile published by ICANN in July 2016 at: https://www.icann.org/resources/pages/rdap-operational-profile-2016-07-26-en. The *.au* operational profile will be consistent with the auDA policy as well as the Australian Privacy Act 1988 (https://www.oaic.gov.au/privacy-law). Amongst other benefits, RDAP will allow for differentiated access (e.g. limited access for anonymous users and full access for authenticated users).

2.5 Legacy Data

A new registry operator will be required to pre-load their registry database, nameserver and WHOIS servers with existing domain name and registrant information prior to commencing operation.

Legacy data will be supplied in standard XML format or such other suitable format as is agreed between the incumbent registry and the registry operator. It will be the responsibility of the registry operator to ensure that the legacy data is converted into an appropriate format suitable for the registry database. It will also be the responsibility of the registry operator to ensure the integrity of the data is maintained throughout the transition process, and that the registry database, zone file and/or WHOIS database are completely synchronised before commencing operations.

2.7 Accreditation of Registrars

The registry operator will be responsible for assessing the technical competency of those applying to be accredited as registrars. They will need to devise a technical test (subject to approval by auDA) to ensure that any applicants being approved to use the registry have demonstrated significant technical ability sufficient to complete all operations required by them. The registry operator will also conduct the .au policy test, on behalf of auDA.

2.8 Registrant Password Recovery

The registry operator must supply a website, for use by registrants to recover their password should it be necessary. This website must operate in accordance with auDA policy, which is currently that the recovery method is to be via email to the registrant contact listed email address.

auDA provides a webpage for access to the password recovery tool at:
https://www.auda.org.au/pw/

3.0 SECURITY REQUIREMENTS

This section of the specification relates to security aspects of the registry system. Due to the critical nature of the information and services to be provided by the registry, adequate protection is required for all aspects of the system and the environment in which it is to operate.

It is a requirement of the specification that the registry system be developed in accordance with the following Security Standards:

a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements. ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.

b) ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. ISO 27002 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment.

As the above security standards are generic and not all areas addressed are relevant to registry operations, auDA will align to the principles of the information security management as documented in the Australian Government Information Security Manual. https://www.asd.gov.au/infosec/ism/
.Registry operators should aim to provide a secure computing environment for reliable and continuous operation of the registry system. Registry operators also should aim to develop or use systems which ensure maximum protection of data against accidental or deliberate changes or corruption.

The security standards cover a variety of development platforms and operational environments. It is recognised that registry operators have a wide range of options when considering solutions for the registry system.

3.1 Security Policy

A clear statement is required from senior management of the registry operator’s commitment to information security.

The following sections describe the security requirements for the registry and associated systems.

3.2 Information Security Risk Management

- *Requirement to adopt a risk management approach* – registry operators are required to adopt a risk management approach and provide auDA as the accountable authority with a holistic understanding of their security posture by aligning the information security practice to auDA's broader risk management practices

- *Information Security Risk Management Process* – implement a risk management approach to information security by identifying, analysing, evaluating and, where appropriate, treating security risks to information and systems.

3.3 Outsourced Information Technology Services

- *Outsourced General Information Technology Services* – maintain the confidentiality, integrity and availability of information by ensuring information technology service providers, including public cloud service providers, implement appropriate security measures to protect registry data.

- *Outsourced Cloud Services* – maintain the confidentiality, integrity and availability of information by applying the Australian Signals Directorate's recommended risk mitigation strategies when using outsourced cloud services. https://www.asd.gov.au/infosec/cloudsecurity.htm

3.4 Roles and Responsibilities

- *Visibility* – provide personnel, including decision makers, with sufficient information to perform their duties by adopting a robust and effective governance framework.

- *Accountability* – ensure duties are undertaken at an appropriate level and conducted accountably by adopting a governance framework with clearly defined roles and responsibilities.

- *Probity* – reduce the likelihood of an actual or perceived conflict of interest by maintaining clear separation of duties.

3.5 Information Security Documentation

Information Security Documentation – apply policy and procedures consistently and accountably by adopting a comprehensive suite of information security documentation, which is regularly reviewed and tailored to specific systems and user roles.

The following suite of documents forms the Information Security Management Framework, as documented in the Australian Government Information Security Management Protocol:

- **Information security policy**. To set the strategic direction for a registry operators information security and allow management to communicate its goals and expectations.
- **Security risk management plan**. To identify security risks and appropriate mitigation measures for systems and determine a risk tolerance threshold, ensuring risks can be managed in a coordinated and consistent manner by a provider.
- **System security plan**. To ensure specific security measures for the implementation and operation of a specific system are adequately communicated and considered.
- **Standard operating procedures**. To assist personnel to follow security procedures in an appropriate and uniform manner, with a minimum level of confusion.
- **Incident response plan**. To communicate which actions to take in response to a cyber security incident, with sufficient flexibility, scope and detail to address the majority of incidents which could arise.
- **Emergency procedures**. To ensure information and systems are properly secured before personnel evacuate a facility, as emergency situations can be exploited as an opportunity for a malicious actor to gain access to systems.
- **Business continuity and disaster recovery plans**. To help maintain security in the face of unexpected events and changes by ensuring critical functions continue to operate when a system is working in a degraded state or reducing the time between when a disaster occurs and critical functions being restored.

To avoid confusion and ensure information security policy and procedures are properly applied, it is essential that all documents work in concert with, and not contradict, each other. Clear and logical wording must be used to ensure the documents are easy to use and effective.

3.6 System Accreditation

- *Accreditation Framework* – ensure that an appropriate level of security is being applied to registry systems, and that any residual risks have been accepted, by adopting a robust accreditation framework.

- *Conducting Security Assessments or Audits* – certify registry systems under the accreditation framework by conducting impartial security assessments, also known as audits.

- *Conducting Certifications* – independently verify the integrity and accept the outcome of an audit by certifying a system as part of the accreditation framework.

- *Conducting Accreditations* – accept that the residual security risks on the registry system are appropriate for the information it processes, stores or communicates by accrediting the system before being put into operation.

3.7 Information Security Monitoring

- *Vulnerability Management* – maintain the security posture of systems by implementing appropriate vulnerability management practices.

- *Change Management* – ensure auDA's approved security risk threshold is maintained when implementing system changes by applying appropriate change management processes.

3.8 Cyber Security Incidents

- *Detection* - reduce the impact and time taken to resolve cyber security incidents by implementing proper procedures and appropriately configured technical measures.

- *Reporting* - maintain an up to date and accurate understanding of the cyber threat environment specific to your network and contribute to the overall cyber threat picture by implementing internal and external cyber reporting procedures.

- *Management* - Enable necessary information to be retained to resolve current, or mitigate future, cyber security incidents by implementing appropriate management procedures.

3.9 Physical Security

Physical Security for Systems – limit access to facilities, servers, network devices, ICT equipment and media to authorised personnel only by applying appropriate physical security controls in accordance with the applicable information security classification.

3.10 Personnel Security

- *Information Security Awareness and Training* - foster an effective security culture within an agency by providing all personnel with ongoing information security awareness and training, tailored to system user roles and responsibilities.

- *Using the Internet* - ensure personnel are able to use Internet services in a responsible, accountable and security conscious manner by adopting effective usage policies and controls.

3.11 Communications Infrastructure

- *Cable Management* - protect registry data by applying appropriate cable management practices.

- *Emanation Security* - Minimise the disclosure of registry data from compromising emanations by implementing appropriate countermeasures.

3.12 Communications Systems and Devices

- *Radio Frequency and Infrared Devices* - Reduce the risk of data spills by implementing measures to prevent, detect and respond to the unauthorised or unsecure use of radio frequency and infrared communications devices, such as Wi-Fi networks and devices.

- *Multifunction Devices* - maintain the confidentiality of official, sensitive information by appropriately configuring, and developing a proper usage policy for printers with fax and scanning capability and other multifunction devices.

- *Telephones and Telephone Systems* - maintain the confidentiality of sensitive information by developing a usage policy governing, and appropriately configuring, telephones and telephone systems.

3.13 Strategies to Mitigate Cyber Security Incidents

Controls to mitigate cyber security incidents – reduce the risk of targeted cyber intrusions by implementing the ASD's **Essential Eight Maturity Model** to mitigate targeted cyber intrusions.

Refer to https://www.asd.gov.au/publications/protect/essential-eight-maturity-model

3.14 Product Security

Product Security Lifecycle - securely select, acquire, install, configure, label, maintain, repair, sanitise and dispose of ICT products that provide information security functionality by applying the Australian Signals Directorate's recommended risk–based processes.

For further information, refer to https://www.asd.gov.au/infosec/epl

3.15 Media Security

Media Handling - establish a removable media policy to provide oversight and accountability for registry information transported or transferred between systems on removable media. Maintain confidentiality by accurately classifying, reclassifying (following appropriate sanitisation or destruction

procedures or changes to data classification), labelling and registering media in accordance with the information it stores.

- *Media Usage* - maintain the confidentiality of stored information by implementing and documenting appropriate standards for connecting, storing and transferring media.

- *Media Sanitisation* - reduce the likelihood of a data spill by implementing proper processes for sanitising—that is, securely overwriting information on—media that is either no longer required or before reuse.

- *Media Destruction* - prevent unauthorised access to stored classified or sensitive information by destroying media that cannot be sanitised—under proper supervision and using documented procedures, appropriate equipment and waste management and transportation processes.

- *Media Disposal* - minimise the likelihood of a data spill when media is released into the public domain by declassification and a formal administrative decision to approve its disposal—by an appropriate authority and according to an agency's documented procedures.

3.16 Software Security

- *Software Security* - maintain the confidentiality, integrity and availability of registry information and protect against the execution and spread of malware by implementing appropriate software security measures on systems.

- *Known Vulnerabilities* - maximise software effectiveness and minimise vulnerabilities by implementing and routinely updating preventative measures, such as applying system and software patches, keeping antivirus signatures up to date and only running supported software.

- *Unknown Vulnerabilities* - maintain the confidentiality, integrity and availability of registry information by removing, disabling and preventing the execution of unauthorised, unused or undesired software or software functionality wherever possible.

- *Databases* - protect database systems and their contents from theft, corruption, loss and unauthorised access by hardening through technical measures, administrator and user policies and regular audits.

3.17 Email Security

Email Security - protect the confidentiality, integrity and availability of information, and ensure information can only be accessed by those intended and authorised to do so, by implementing an email usage policy and applying appropriate security controls to email applications and infrastructure.

3.18 Access Control

- *Identification and Authentication* - ensure that access to a system is limited to users and devices that are authorised to access it by adopting appropriate identification and authentication practices and controls.

- *Authorisation* - protect the confidentiality, integrity and availability of information on systems by limiting authorisation to those with a demonstrated need–to–know.

- *Event Logging and Auditing* - detect and attribute any violations of information security policy—including cyber security incidents, breaches and intrusions—by maintaining, auditing and ensuring the availability and integrity of event logs.

3.19 Secure Administration

Secure Administration - increase the level of assurance that administrator activities and credentials will not be compromised during a malicious cyber intrusion by implementing robust technical controls and processes.

3.20 Network Security

- *Network Management* - ensure all sections of an agency's network comply with information security policies, and that network vulnerabilities are identified and addressed, by adopting appropriate network management practices.

- *Network Design and Configuration* - reduce opportunities for a malicious actor to compromise or gain unauthorised access to sensitive information through the secure design and configuration of agency networks.

- *Network Infrastructure* - maintain the confidentiality, integrity and availability of information by applying a defence–in–depth approach to the secure deployment of network infrastructure.

3.21 Cryptography

- *Protecting Information at Rest* - maintain the confidentiality and integrity of registry data at rest using an appropriate ASD Approved Cryptographic Algorithm.

- *Protecting Information in Transit* - maintain the confidentiality and integrity of registry data in transit using ASD Approved and appropriately configured Cryptographic Protocols implementing an ASD Approved Cryptographic Algorithm.

- *Availability of Information* - ensure encrypted information is accessible to those that require it when they require it by implementing appropriate procedures and controls for data recovery.

- *Management of Cryptographic Systems* - Maintain the integrity of cryptographic systems, and hence the confidentiality and integrity of the information being protected, by applying appropriate governance and personnel and physical security measures.

3.22 Cross Domain Security

- *Gateway Security* - protect the confidentiality, integrity and availability of information on the registry operator's networks by appropriately deploying and configuring gateways.

- *Cross Domain Security* - ensure the secure transfer of information between security domains with a high level of assurance by implementing security–enforcing mechanisms.

- *Maintenance and Review* - identify and mitigate security risks as early as possible by maintaining and regularly reviewing gateway architecture. This includes undertaking routine testing and regular security risk assessments and ensuring that any residual risks are accepted.

3.23 Data Transfers and Content Filtering

- *Data Transfers* - mitigate the risk of data spills of official, sensitive or classified information to systems not accredited to handle the data by having a policy governing data transfers and a procedure in place for authorising and importing or exporting the data to a system.

- *Content Filtering* - implement content filtering techniques to reduce the risk of unauthorised or malicious content transiting a security domain boundary.

3.24 Working Off–Site

- *Acceptable Use* - prevent mobile devices from becoming a security risk to the system or network they connect to by implementing, and educating personnel on, an effective mobile device usage policy.

- *Mobile Device Configuration* - limit situations, or mitigate the consequences of situations, where a user loses control over a mobile device by securely configuring the device and implementing appropriate processes.

- *Wireless Communications and Connectivity* - protect sensitive or classified information from unauthorised access by only enabling wireless communications on a mobile device that are needed and can be secured.

- *Upkeep and Maintenance* - Maintain the integrity and confidentiality of the information stored or communicated on a mobile device by conducting regular audits and security updates.

4.0 BUSINESS CONTINUITY PLAN REQUIREMENTS

This section of the specification relates to the on-going operation of the registry system. Business continuity and disaster recovery are established methodologies which have evolved to provide a planned approach for the re-establishment of services following failures or disasters.

The registry operator will be required to develop and implement a full business continuity plan for the registry system. The plan will detail the processes to be undertaken to ensure the continued operation of the registry in the event of a disaster.

Business continuity planning is considered an addition to the normal operation of a well-designed computer system. The latter includes regular system maintenance and routine back-up and recovery procedures for information files within the system, software maintenance and documentation. Off-site data escrow requirements are described in Section 5.

The following provides an overview of the level of continuity planning considered necessary for the registry system. The first stage of the process is the preparation of the business continuity plan. The second stage is the implementation of the systems and infrastructure required to ensure that the plan executes successfully.

The functions within the registry system are considered to be at two levels: production and maintenance. The production items include the real-time components of the registry system, e.g.. the nameserver and WHOIS services. The maintenance items include the remainder of the system, e.g.. maintenance of data records, reporting and enquiries.

Continuity planning should aim to re-establish operation of the primary or production level of the registry system by the end of the next day – eg. a disaster on Wednesday is recovered by midnight on Thursday, a disaster on Saturday is recovered by midnight on Sunday. The registry system should be fully operational within three business days.

Continuity planning is usually a compromise between what can be achieved and the cost of achieving it. In this case, optimum continuity would be achieved with a solution based on fully duplicated sites at multiple locations (e.g.. one in Melbourne, one in Sydney). The need for continuous operation of the registry system justifies the cost.

Business continuity planning is an established management approach to the recovery of business operations and procedures following a disaster. Disasters can be brought about by nature (e.g.. floods, cyclones, heat waves, flu epidemics), can be accidental (e.g.. fire, building collapse), can be man-made (eg. bombs, sabotage, viruses, activation of sprinkler systems) or due to industrial disputes (e.g.. power strikes). While the variations are numerous, disasters can be categorised as loss of information, loss of access or loss of personnel.

The aim of business continuity planning is to minimise interruptions to operations or services provided by the business, and to resume critical operations or services within a specified time after a disaster. Continuity planning also aims to minimise financial loss within an organisation and to assure clients and the community that their interests are protected. It ensures that management and staff within an organisation understand the implications of disasters on services and provides a positive public image of the organisation.

Business continuity planning requires a study of the operations of a business, identification of areas and facilities which are likely to be affected by disasters, and providing back-up equipment and procedures for re-establishing services in the event of a disaster. For the registry system, the continuity planning stages could be defined as follows.

(a) Business impact analysis: This stage involves an analysis of all aspects of the registry system, including housing, personnel, equipment, communications, procedures and business requirements. The resulting report should include the following:

(i) an audit of business sites, the personnel and equipment located at each site, and the impact of the loss of the sites, personnel and equipment;

(ii) a security assessment of computer and communications equipment within the organisation (as discussed in Section 3) including:

- physical security, including access control
- tasks performed by personnel
- operating procedures
- back-up and recovery procedures
- system development and maintenance
- database security
- personal computers;

(iii) an audit of possible disaster situations likely to impact on the registry system, in particular:

- loss of power (eg. failure or prolonged strike)
- loss of environmental controls (eg. air-conditioning)
- breaches of security (eg. physical, electronic – virus or hack attack)
- loss of internal/external communications
- system failure (eg. computer or disk malfunction)
- Internet communication failure or interruption
- degraded performance;

(iv) file corruption or lost files;

(v) unreliable or incorrect results

(vi) determination of critical resource requirements for disaster recovery;

(vii) recovery strategies and methods to be applied in the event of disasters, and timelines for partial and full recovery;

(viii) cost/benefit analysis for the various recovery alternatives;

(ix) staffing requirements for the various recovery alternatives;

(x) recommended recovery strategy;

The business impact analysis is usually performed once, and subjected to a relatively minor annual review to assess changes introduced during the year.

(b) Business continuity plan: The business continuity plan is an extension of the business impact analysis and effectively documents the procedures to be followed to recover from a disaster situation. Copies of the documents should be kept off-site with appropriate back-up and software files in the event that the primary site is destroyed. The business continuity plan should be written to allow an external organisation or qualified individual to undertake the recovery process. The major components of the business continuity plan are as follows:

(i) Organisational details: This includes details of alternate office locations, contact details and staff trained in the execution of the recovery procedures;

(ii) Disaster declaration procedures for instigating disaster recovery operations: This should define the procedure for commencing the disaster recovery process, including a list of organisations and individuals to be notified;

(iii) Procedures for activating alternate work-sites: Arrangements must be made for alternate work sites in the event that the primary work site cannot continue to be used (eg. destroyed by fire). This may take the form of an initial temporary arrangement at another site until a new site is found, or it may be part of a multi-site plan within the organisation;

(iv) Procedures for recovering vital records and files: Vital records and files must be stored off-site to as part of the disaster recovery procedure. This section should provide a list of such items and where they are located. Procedures should be established to ensure that the required files are stored off-site as part of the site's normal operational procedures, and for checking that they are correctly stored and updated. Procedures

should be documented for the recovery of off-site information (software and data);

(v) Definition of recovery teams and responsibilities: Provide a list of individuals assigned to recovery teams and the tasks to be performed by the teams. This documentation should take the form of a “flowchart” for recovery in any situation. Arrangements could be made with external organisations or qualified individuals to be used as alternatives to in-house staff in the event of a disaster. External staff should be trained in recovery procedures as in (c) below;

(vi) Recovery procedures: This defines the steps involved in the recovery process. The steps should be clearly defined and reviewed during staff training in (c) below and testing in (d) below. This is the key area of the continuity plan;

(vii) Relocation procedures: This section relates to the relocation of the registry system either temporarily or permanently as the result of a disaster situation;

(viii) Resource requirements and procurement: This provides a list of vendors and suppliers who may be required to provide equipment and/or services to assist with the recovery process. The section should also document any arrangements or contracts with vendors to supply equipment at short notice, eg. immediate supply of a replacement computer;

(c) Staff training: Training is required for both in-house staff and external contractors in the execution of the business recovery plan. This section documents the level of training and provides procedures for documenting staff training levels. Training should include a review of the business continuity plan and participation in testing as described in (d) below;

(d) Testing of the business continuity plan: This section documents procedures for testing the business continuity plan to ensure that recovery operations function correctly and that staff are adequately trained. Procedures should be included to evaluate the progress of general staff in following recovery procedures. Tests should be performed at least twice per year and should be used to refine the recovery process;

(e) Effectiveness evaluation and monitoring: An annual review of the entire business continuity process should be conducted and reviewed by senior management.

4.1 Emergency Transition Plan

The registry operator will also work with auDA to develop 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.

auDA may temporarily resume service itself or designate an emergency interim registry operator of the registry for *.au* (an "Emergency Operator") until such time as the registry operator has demonstrated to auDA's reasonable satisfaction that it can resume operation of the registry for *.au* without the reoccurrence of such failure. Following such demonstration, the registry operator may transition back into operation of the registry for *.au* pursuant to the procedures set out in the registry transition process, provided that the registry operator pays all reasonable costs incurred (i) by auDA as a result of the designation of the emergency operator and (ii) by the emergency operator in connection with the operation of the registry for *.au* , which costs shall be documented in reasonable detail in records that shall be made available to the registry operator.

ICANN has documented an emergency transition process at: https://www.icann.org/resources/pages/transition-processes-2013-04-22-en which can be used as a basis to develop an emergency transition plan.

The registry operator shall provide auDA or any such emergency operator with all data (including the data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by auDA or such Emergency Operator. The registry operator agrees that auDA may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to *.au* in the event that an Emergency Operator is designated.

The registry Operator will cooperate with auDA in an annual test of the emergency transition plan with respect to ensuring that all software and data is available to temporarily resume service.

5.0 DATA ESCROW REQUIREMENTS

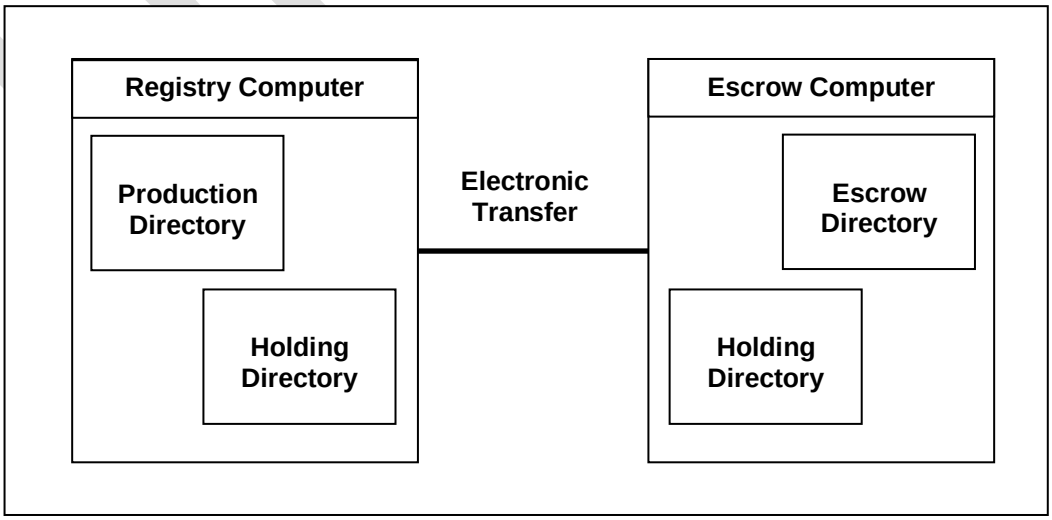
This section of the specification defines the data escrow requirements of the registry system. Data escrow requires the transfer of data from the registry system to auDA, and to be accessible by auDA under limited circumstances, including for the purposes of testing an emergency transition, conducting market studies, detecting DNS Abuse, doing source code independent security reviews, meeting auDA's commitments under the Sponsorship agreement with ICANN, and ensuring full protection of copyright and intellectual property. auDA has obligations with respect to data escrow as described in clause 4.3 of the ccTLD Sponsorship Agreement (.au) with ICANN dated October 2001 (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en).

5.1 Data Escrow Operation

In general terms data escrow needs to be performed on a regular basis and will require the transfer of all data, programs and documentation from the registry system to the nominated site. The data escrow process should be as fully automated as possible.

For example, a job could be scheduled to run at a convenient time (e.g.. midnight) to extract the required data from the registry's database and generate the required files in a nominated directory, together with all required software and documentation files. The contents of the directory would then be electronically transferred to the escrow site and validated.

The following diagram provides a diagrammatic view of such a data escrow operation.



In the above diagram, the holding directories are accessible only to the escrow programs. The data escrow job executes the following tasks:

(a) Lock out database entry, update and delete operations for the duration of the job;

(b) Scan the nominated database tables in the production directory and generate text files of escrow data in the holding directory;

(c) Copy nominated software and documentation files from the production directory to the holding directory;

(d) All of the files in the holding directory are encrypted and signed, using best current practices, prior to transmission;

(e) Transfer the files in the holding directory of the registry computer via the Internet to the holding directory of the escrow computer;

(f) After a file has been transmitted it is verified to ensure that the transfer operation executed correctly. Verification is effected by either:

(i) reading the transferred file from the escrow computer and comparing it with the original file;

(ii) applying a suitable checksum to the transferred file from the escrow computer and comparing it to a checksum generated from the original file; or

(iii) other suitable method specified by the tenderer;

(g) A report of the data escrow operation is printed;

(h) Copy the encrypted files from the holding directory in the escrow computer to the escrow directory in the escrow computer, replacing the previous day's files;

(i) Files in the production computer's holding directory are then deleted;

(j) Files in the escrow computer's holding directory are then deleted;

(k) Re-instate normal database operations.

While this model is somewhat simplistic, it demonstrated the facilities required in the data escrow process. Many variations are possible.

One option could be to re-instate normal data base operation, currently in (k) above, immediately after the required database been transferred to the holding directory in (b) above. This would reduce the time the system was unavailable for normal operation to a few seconds. However, facilities would have to be provided to repeat the data escrow process in the event of a failure in steps (c) through (j) above.

A second option could be to separate the escrow process for program and documentation files so that it is activated on demand (when software or documentation is updated) rather than being part of the routine escrow process.

The escrow data is to be transferred electronically to auDA's escrow server currently located in the AAPT data centre, Richmond, Victoria. auDA currently manages the secure storage of escrow data tapes in an external facility.

5.2 Data Escrow Contents

The escrow process should allow auDA to replicate the original registry environment if necessary under the Emergency Transition plan (see section 4.10).. This means that that the registry operator will be required to include everything necessary to reinstate a fully functioning registry system. Normally this will include the following:

(a) Complete source and executable code of registry, nameserver and WHOIS software;

(b) Database definitions and contents of the database;

(c) Operational and configuration files and information;

(d) Documentation covering the installation, configuration and operation of the system;

(e) Help files, operation and user manuals.

(f) List of third party software licences required to operate the registry software and the ability to use these licences on a temporary basis under appropriate commercial terms

In addition the escrow process should include the computer operating system, compilers and utilities if these are specifically required for registry operation. As an alternative, the registry operator must provide full documentation of the computer hardware, system and database software and utilities to be used in the registry system.

The registry operator is to be responsible for the maintenance of paper records (eg. manuals, printed reports) in accordance with the requirements of the Australian Record Management Standard AS4390.

In addition, the registry operator is required to provide auDA with a licence to run the registry software for a limited period of time in the event that auDA or an organization it designates is obliged tobecome the Emergency Operator.

At registry rollover, there must be a seamless transition between an incumbent registry operator and the new registry operator. The registry operator is required to cooperate in the handover process to ensure continuous service to registrars.

5.3 Data Escrow Format

As part of the data escrow process, all data from the registry database is to be extracted in a CSV and XML (with a defined schema) format and provided with appropriate scripts to facilitate the loading of this data in to a relational database.

6.0 DOMAIN NAME EXPIRY AND DELETION REQUIREMENTS

This section of the specification relates to the expiry and deletion of domain names in the registry.

When domain names are registered the expiry date of the domain name is entered into the registry database, usually as the date registered plus two years The registry operator should support configuration options to allow registration periods in one year increments from 1 to 10 years, as allowed by the currently applicable auDA policy. Domain names may be deleted at the request of the registrant or expire at the end of the registration period unless the registrant pays the required renewal fee. Registrants are given a standard grace period in which to reverse the expiry or deletion.

It is a requirement of the specification that deleted items become available for re-use as soon as possible after the period of grace. The grace period and the procedure for deleting items from the registry are set out in Appendix B.

It is also a requirement of the specification that the registry contains no facilities (accidental or otherwise) which allows the registry operator or a registrar to retain a deleted, expired or unregistered domain name. There should be no facilities for the reserving of domain names by registrars in the registry.

The registry operator and registrars are prohibited from using domain availability information to speculate in any manner on domain names.

Undesirable practices include, but are not limited to:

(a) A registrar or registry operator squatting on domain names pending an increased fee, auction or other market-distorting activity;

(b) A registrar or registry operator who removes a domain name from the market in response to a WHOIS query from a prospective registrant, and attempts to obtain additional fees from the registrant;

(c) A registrar or registry operator who uses business registration information to squat on related domain names to obtain additional fees from the relevant prospective registrant.

7.0 REPORTING REQUIREMENTS

This section describes the information to be provided to auDA in the form of a monthly report of the operation of the registry, or as noted made available to auDA on request. The monthly report must be presented to auDA within the first 7 days of the following month. The following information is required from the registry operator:

(a) **Registrations:**

(i) report the total number of new registrations in the registry system for the given month, and provide a year on year comparison;

(ii) report the total number of create and re-new, transactions recorded in the registry system for the given month;

(iii) report the total number of renewals recorded in the registry system for the given month;

(iv) report the total number of domain name 'drop-offs' recorded in the registry system for the given month;

(v) report the total number of domain names currently in the registry system at the end of the given month;

(vi) report the total number of domain names, by zone currently in the registry system at the end of the given month;

(vii) report the registrar transfer activity on the basis of the number of transfers in/out between each pair of registrars

(viii) report the registrant transfer activity, with a list of transfers made in the month

(ix) provide the above information as a breakdown by registrar;

(b) WHOIS:

(i) provide the facility to gather reports on the number of WHOIS queries recorded in a specified date range;

(ii) provide the above information by zone;

(iii) provide a tool for auDA to generate reports on the number of blacklisted hosts;

(iv) report on suspicious WHOIS activity as required;

(v) service level performance;

(vi) provide a report stating the actual service availability performance for the registry system, the nameservers and the WHOIS service;

(vii) provide the average processing time for each EPP transaction type for the registry system;

(viii) provide the average update frequency for the nameservers;

(ix) provide the planned outage time for the registry system and WHOIS service;

(x) provide the extended planned outage time for the registry system and WHOIS service;

(xi) provide the planned outage notification time for the registry system and WHOIS service;

(xii) provide a tool for auDA to generate reports on the average add time, average modify time, average delete time, average time to query domain, average time for whois query, average time for name server resolution update frequency;

(c) Database:

(i) provide a tool for auDA to generate a report detailing the number of database transactions for a given period;

(ii) provide a tool for auDA to generate a report detailing the average daily transaction rate for a given month;

(iii) provide a tool for auDA to generate a report detailing the registry database size;

(d) Commands:

(i) provide a report that details the number of commands in the registry system for a given month for domains, hosts and contacts. This will include:

- create commands
- info commands
- delete commands
- update commands
- check commands
- transfer commands
- WHOIS commands;

(ii) provide a report that details the number of commands transacted by nameservers for a given month for domains. This will include all nameservers operated by the registry;

(e) Nameservers:

Provide a tool for auDA to generate a report detailing the number of name server queries that return the following:

- successful queries
- referrals
- non existent domains (nxdomain)
- non existent record set (nxrrset)
- failures
- look-ups resulting in recursion;

(f) Average registry response time:

Provide a report that details the average response times recorded in the registry system for:

- WHOIS
- nameservers
- transform
- queries;

(g) Hardware, software and network security issues:

(i) should any hardware, software, network or security issues be encountered during the month, provide an incident report of the steps taken to resolve the issues and ensure that the issues do not reoccur;

(ii) in circumstances where a security breach occurs, provide an incident report detailing the nature, extent of the breach and action taken, at the earliest available opportunity;

(h) Enquiries

Provide on request a report of the number and type of telephone and email support enquiries made to the registry.

The monthly report will be available for viewing or printing. The registry operator will also be required to provide registrars with reports relating to their customer base and other operational information that registrars require to conduct their businesses.

Incident reports should conform with industry best practice for service management as detailed in ISO 20000 (Information Technology – Service Management) and ITIL (Information Technology Infrastructure Library). The registry operator should provide the incident report in a form that is suitable for reporting incidents to Computer Emergency Response Team (CERT) Australia

(https://www.cert.gov.au/) and the Australian Cyber Security Incident Centre (https://www.acsc.gov.au/) .

(a) **DNS Abuse report**

The registry operator will maintain statistical reports on the number of security threats identified with respect to the use of domain names, and the actions taken as a result of the periodic security checks. See section 9.

In addition the registry operator must provide a comprehensive reporting facility to auDA through a secure web based interface which is to include (subject to change at auDA's discretion):

(a) Domain report: Displaying monthly domain statistics for each registrar including:

- total number of domains registered
- domains to expire
- domains created
- domains deleted
- domains renewed
- domains expired
- domains re-registered after expiry;

(b) Policy report: Displaying .au extension policy reason statistics per registrar;

(c) WHOIS service activity report: Displaying the total number of WHOIS queries for the specified period, grouped by namespace;

(d) WHOIS blacklist report: Displaying IP addresses that are blacklisted from performing direct (TCP port 43) WHOIS queries and also web-based queries via any of the registry operator WHOIS web forms. The report shows each address blacklisted during the specified period along with the date on which it was blacklisted;

(e) EPP transaction report: Displaying the number of EPP transactions for each day in the specified period, together with the average daily transaction volume;

(f) Database size report: Displaying the current size of the registry database relative to the capacity of the hardware, and the increase in size during the specified month;

(g) Registrar contact report: Displaying contacts in the registry according to the search criteria; registrar name, contact ID and either create date or date of last update. Results can be sorted by ROID, ID, name, organization, email address, creation date or update date. The output consists of the name of the registrar that created or

updated the contact (according to the criteria specified), along with the records by which the output may be sorted, as listed above;

(h) Registrar domain report: Displaying domains in the registry according to the search criteria. This is similar to the contact report, except that the contact ID search criteria is replaced by the domain name, and the sort and display fields are domain ROID, name, registrar name, creation date, expiry date and update date;

(i) Registrar host report: Displays hosts in the registry according to the search criteria. This is similar to both the contact report and domain report. The host name replaces the contact ID in the search criteria. Results can be sorted by host ROID, name, registrar name, creation date or update date;

(j) Registry outage report: Listing planned and unplanned registry outages for the specified month;

(k) Registry fault report: Listing registry faults for the specified month;

(l) Registrar helpdesk enquiry report: Listing registrar helpdesk enquiries for the specified month;

(m) Full object details: Displaying object details, similar to the EPP object:info command. The supported objects are domain, host and contact. The information provided is not restricted, as it is for non-sponsoring registrars.

8.0 REGISTRAR SUPPORT SERVICES REQUIREMENTS

This section of the specification describes the registrar support services to be provided as part of the registry operation. These services must be managed and operated by the registry operator from within Australia.

The following services are regarded as a minimum:

(a) 7 day, 24 hour emergency support in the form of a registry support telephone number for critical issues giving access to an Australian based registry operator staff member appropriately qualified with experience in DNS and registry operations and capable of providing the necessary technical support;

(b) A registry help desk open weekdays (8am till 7pm AEST), and Saturdays (10am till 4pm AEST) manned by dedicated trained personnel with experience in DNS as well as registry operations;

(c) Email address and telephone number for service requests and enquiries;

(d) Assistance with billing and account management;

(e) Provision of a dedicated registrar website containing information on the following:

- technical information and downloads
- accreditation information
- accounts management
- statistics;

(f) Maintain an OTE testing environment that is an identical implementation of the production environment and maintain a separate research and development test environment for testing new software before placing that software into the production environment;

(g) Provision of a high quality domain name service to registrars and end users.

9 ABUSE MITIGATION

The registry operator shall publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in *.au* and the second, third, and fourth level namespaces within *.au* under management by the registry operator, and will provide auDA with prompt notice of any changes to such contact details.

Domain names within the .au name space, must not be used for distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to Australian law.

The registry operator will periodically conduct a technical analysis to assess whether domains in *.au* and the second, third, and fourth level namespaces within *.au* under management by the registry operator are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. The registry operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement and provide to auDA on a monthly basis.

10. DAILY LOG REPORTS

The registry operator will make available to auDA on a daily basis the following log reports with data/time stamps on the data:

- EPP Transactions – by IP address, registrar, and XML command
- Web portal transactions - by user account and commands
- Database access transactions – by authorised user
- WHOIS queries – by source IP address and query
- Nameserver (including nodes as part of Anycast arrays) queries – by IP address and DNS query. Logging may be suspended in denial of service situations where there is significant load on a nameserver.
- Data centre access – by authorised user for any physical access to registry servers

APPENDIX A: DEFINITION OF TERMS

Full Service Availability means the time, in minutes, that the registry is responding to all registrars.

Partial Service Availability means the time, in minutes, that the registry is responding to one or more of its registrars but not all registrars.

Service unavailable means when a service listed is unavailable to all users, that is, when no user can initiate a session with or receive a response from the registry ("Unavailability").

Service Availability is measured as follows:

Service Availability % = {[(TM - POM) - UOM] / (TM - POM)}*100 where:

TM = Total Minutes in the Service Level Measurement Period (#days*24 hours*60 minutes)

POM = Planned Outage Minutes (sum of (i) Planned Outages and (ii) Extended Planned Outages during the Service Level Measurement Period)

UOM = Unplanned Outage Minutes (Difference between the total number of minutes of Unavailability during the Service Level Measurement Period minus POM).

Planned Outage means scheduled downtime to allow for regular maintenance.

Planned Outage Duration defines the maximum allowable time, in hours and minutes, that the registry operator is allowed to take the registry out of service for regular maintenance.

Extended Planned Outage means an extended maintenance timeframe, which may be required in cases such as software upgrades and platform replacements.

Extended Planned Outage Duration defines the maximum allowable time, in hours and minutes, that the registry operator is allowed to take the registry out of service for extended maintenance.

Processing Time means the time that the registry operator receives a request and sends a response to that request. For example a processing time of 3 seconds for 95% means that 95% of the transactions will take 3 seconds or less from the time the registry operator receives the request to the time it provides a response.

Update Delay Time is measured from the time that the registry confirms an update to the registrar to the time the update appears in the nameserver and WHOIS server. For example, an update delay time of 15 minutes for 95% means that 95% of the updates will be available in the nameserver and WHOIS server within 15 minutes.

Cross-Network Nameserver Performance means the measured round-trip time and packet loss from arbitrary locations on the Internet to the registry.

APPENDIX B: REGISTRY SERVER POLICY DOCUMENT

B1 Introduction

Certain things associated with the AusRegistry EPP server are, according to the EPP specifications, left open to policy decisions by the server operators. This document details all such areas of the AusRegistry EPP server that are extensions beyond the EPP specification. These extensions are based on the policies governing the ccTLDs that we manage and on AusRegistry's own recommendations.

B2 General

Language

The only language that the Registry will accept in any EPP command is English, specified by either 'en' or 'en-US'.

AuthInfo

From auDA policy document 2002-29, DOMAIN NAME PASSWORD POLICY, object *authInfo* MUST meet the following requirements.

"For security reasons, the domain name password must contain:

a) between 6 and 32 characters;
b) at least one letter (a-z) and one number (0-9);
c) no dictionary words., and
d) may not be based on a dictionary word, for example an authInfo of pass1word would not be permitted

The above also applies to contact *authInfo* as well.

Legacy passwords which do not satisfy the above requirements MUST be updated to conform.

Authentication

All the following MUST be met for successful authentication:

- Certificate MUST be signed by AusRegistry
- Certificate MUST match Registrar whose credentials are being used
- Source IP address MUST be the nominated IP address of the Registrar whose credentials and certificates are being used
- Valid Credentials MUST be provided
- Registrar username MUST match the common name of the certificate being presented.

This means:

- a Registrar's Certificate is valid only from a nominated IP address of that Registrar
- Credentials are valid only from a nominated IP address of the Registrar with those credentials
- No other party can use the certificate and credentials of a Registrar should they obtain them, unless they are also able to use a nominated IP address of the corresponding Registrar as well.

Timeouts

The AusRegistry EPP Server will timeout - meaning it will close the session (socket) - if a client is idle for more than ten minutes. The server deems a client to be idle if it is not transmitting any EPP commands to the server.

Invalid Requests

The AusRegistry EPP server will close the socket if it receives an EPP packet header indicating that the EPP command contained within is more than 4000 characters in length. This would usually indicate an invalid or corrupt request.

Maximum Connections

Registrars are limited to a maximum of twenty connections to the EPP system at one time. This includes EPP sessions and connections made through the AusRegistry Admin interface.

Object Disclose

The EPP core protocol requires the server to announce data collection policies to clients (Section 2.4 of RFC3730). In addition to this disclosure requirement, the <obj:disclose> element can be included in certain commands and responses. This element contains data elements that allow a client to identify values that require special server handling which allows or restricts disclosure to third parties.

Although the RFC EPP specification states the use of this element, data disclosure practises are mandated by auDA and not for Registrar (or Registry) modification. Therefore the AusRegistry EPP Registry will not be supporting its use. All attempts to use the disclosure element will result in a 2308 error being returned.

SSL Sessions

The AusRegistry EPP service ENFORCES the use of Transport Layer Security (TLS v1.2) encryption protocol (RFC 5246), no SSLv2, SSLv3 or lower connection attempts will be successful (see RFC 6176 Prohibiting Secure Sockets Layer (SSL) Verion 2.0).
The use of a strong cryptographic transport layer is enforced by the RFC.

Command Authorisation Matrix

The EPP <login> command is used to establish a session with an EPP server in response to a greeting issued by the server. A <login> command MUST be sent to a server, to establish an ongoing session, before any other EPP command. Sessions are ended with a <logout> Further EPP commands must be executed within the context of an established session. The following table applies only to such commands.

Command	*Available to client*	*Additional authorisation*
create	any	
check	any	
domain:info	sponsor (full info)	
domain:info	non-sponsor (full info)	domain authinfo
domain:info	non-sponsor (partial info)*	
contact:info	Sponsor (full info)	
contact:info	non-sponsor (full info)	Contact authinfo
contact:info	non-sponsor (partial info)**	
host:info	any	
delete	sponsor	
update	sponsor	
transfer request	non-sponsor	Domain or associated contact's authinfo
transfer approve	sponsor	Domain or associated contact's authinfo
transfer cancel	non-sponsor	Domain or associated contact's authinfo
transfer query	sponsor	Domain or associated contact's authino
transfer query	non-sponsor	Domain or associated contact's authinfo
domain:renew	sponsor	
poll	any	

*Partial info for domain name includes Roid, Sponsoring Registrar.

**Partial info for contact includes Roid, Status, Sponsoring Registrar, Name, City, Country, Email, Created by and Creation date.

B3 Registrars

Registrar Passwords

Registrar passwords MUST meet the following requirements:

- 8-32 characters
- Contain at least two digits
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain at least two non-alphanumeric characters
- Be NOT based on a dictionary word.

Registrar Identifiers

Every registrar is uniquely identified by a Repository Object IDentifier (ROID) which has the format Rnnnnn-AR where nnnnn is a zero-padded integer assigned by AusRegistry. The AR suffix is an abbreviation for AusRegistry.

B4 Domains

Creation

AusRegistry will only allow the following valid 3rd level domains to be provisioned on the registry system:

- .com.au
- .net.au
- .org.au
- .asn.au
- .id.au

Access restrictions prohibit registrars from actually registering certain domains. They will be rejected and receive a parameter value policy error. Special rules apply for the other ccTLD's in our registry (e.g. gov.au, edu.au, vic.au, nsw.au, tas.au, wa.au, sa.au, qld.au, nt.au).

Period

Registrars are only permitted to register or renew domains for the period or periods specified by the ccTLD governing body (currently 2 years for .au domain names, but expect to change to as part of the .au policy review process). The registry operator should support configuration options to allow registration periods in one year increments from 1 to 10 years, as allowed by the currently applicable auDA policy. The value can be specified as either type='m' or type='y'. The values passed through are dependent on the period of registration or renewal desired. All Domains will have their expiry date initially set to two years from the date of creation. Domains will only have their expiry date extended by the specified time frame at the time of renewal.

Reserved Domains

auDA (.au) have provided AusRegistry with a list of reserved domains, these domains have been loaded into the registry database and are unavailable for provisioning in the registry system.

Minimum Contact objects required

All domains are to be created with a minimum of a registrant and a technical contact. Thus any create which does not provide these contacts (and any update command that will result in these required contacts being removed) will fail. Any number of additional contacts such as technical, billing and admin are able to be associated with a domain at the registrar's free will, however AusRegistry recommends avoiding excessive contact associations.

Minimum Name Servers

Any domain can be created with any number of name servers (0-13). However, only domains that have two or more associated host objects will be provisioned in the DNS. Any time an update to a domain is done that results in it being delegated to fewer than the required number of name servers, the domain will be removed from the zone. The exception is that when a domain has expired, any child hosts will be deleted and any domains delegated partly to any such children will remain in the DNS as long as they are still delegated to at least one internet host. Also, irrespective of how a domain is delegated, there are statuses that cause the domain to be removed from the zone file – these are pendingDelete, clientHold and serverHold.

Extension Policy

.au has strict policies dictating the requirements for each second level domain. The registry will ensure that these policies are enforced to the extent that it can. Please see https://www.auda.org.au/policies for more information regarding the policy. Contacts for au domains that are within Australia (their country code is AU) must have four digit postcodes and have a valid city/state combination.

Eligibility criteria will also be enforced with respect to the zone the domain resides in. The following table details the eligibility types that will be accepted for each zone.

Eligibility Explanation	.com.au	.net.au	.id.au	.org.au	.asn.au	Policy Reason #
Company						1 or 2
Registered Business						1 or 2
Sole Trader						1 or 2
Trademark Owner						1 or 2
Pending Trademark						1 or 2
Incorporated Association						1 or 2
Club						1 or 2
Non-Profit Organization						1 or 2
Charity						1 or 2
Trade Union						1 or 2
Industry Body						1 or 2
Commercial Statutory Body						1 or 2
Religious Church Group						1 or 2
Political Party						1 or 2
Citizen / Resident						1 or 2
Partnership						1 or 2
Research Organization						1 or 2
Other						1 or 2

For the second level namespaces above, the available policy reasons are:

Policy Reason	Explanation
1	All 2LDs – Domain name is exact match, abbreviation or acronym of the registrant's name or trade mark
2	asn.au, com.au, .net.au, .og.au – domain name has been allocated using the close and substantial connection rule

The above rules will be enforced with new registrations and any .au Extension change requests submitted.

Updates to auExtension Elements

To support updates of only extension data, domain update commands are not required to contain any of the <domain:add>, <domain:rem>, or <domain:chg> elements - these are all optional. This is in contradiction to the text of the EPP RFC"s, but not the XML schemas contained within. After

consultation with the RFC author, AusRegistry has determined that the schemas are the authoritative resource. At this point in time, NO updates to auExtension elements are possible via the EPP interface.

Legacy MX Only Domains Policy

MX only domains cannot be updated or renewed under the current system. If a registrant requires updates to their domain of any sort, they must re-delegate their domain. i.e. no MX records are supported in the .au name space zone file. The process for this is:

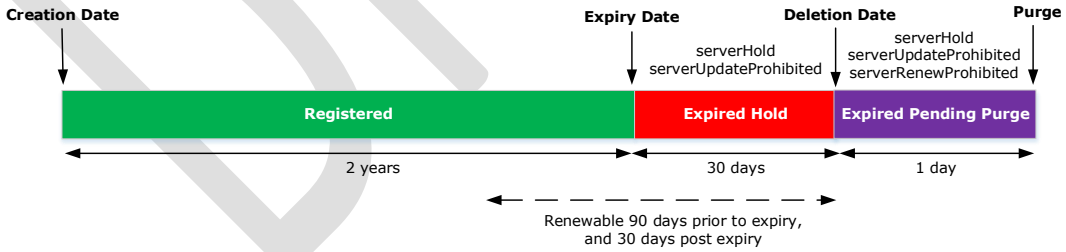
> Select Delete MX from the Domains menu of the Admin interface and enter the domain name in the field provided and click the Remove MX button. This will remove the MX records from the name server and unlock the domain.

Registrars should ensure that registrants have set up the necessary NS and MX records on the server they are pointing their domain to, prior to advising the registry. The Registry is not responsible for any outages due to NS and MX records not set up at the client end.

Order of Processing Updates

The order of processing domain updates is in the order that is specified in the EPP Domain Name Mapping schema (RFC 5731). Additions will always be performed before a removal. Changes are performed last. Registrars should keep this in mind when changing contacts for example and are reminded that at no time is a domain to be without a Technical contact.

Domain Expiry and Renewal



auDA's Domain name Renewal, Expiry and Deletion policy is available at: https://www.auda.org.au/policies/index-of-published-policies/2010/2010-01/

1. Upon creation, a domain's expiry date is set to 23:59:59 on the create date plus the period of registration
2. Periodically the AusRegistry 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 domain will enter the "**Expired Hold**" status, with the statuses serverUpdateProhibited and serverHold applied to the domain (only transfer, transfer-renew and renew commands can be performed at this point)
4. DNS information is also removed after expiry
5. 30 calendar days after the domain has expired, the domain will transition to an "**Expired Pending Purge**" State. This is depicted in the WHOIS by serverHold (Expired), serverRenewProhibited (Expired), and serverUpdateProhibited (Expired). The domain name will be published on the *Official Domain Drop List* (https://www.ausregistry.com.au/official-domain-name-drop-list/). Exactly one calendar day after it enters "Expired Pending Purge" state the domain name will be purged in the Purge Cycle. The Purge Cycle runs at 1.00pm AEST (2.00pm AEDT) on every day, including weekends and public holidays.
6. Domain renewals add exactly the specified interval to the expiry date
7. Domain renewals can happen within the 90 day period prior to the expiry date, or up to 30 days after expiry.
8. There is a 3 calendar day grace period during which a renewal may be cancelled with immediate effect and the registration/renewal fee refunded to the Registrar.

Domain Delete

With reference to auDA's Domain name Renewal, Expiry and Deletion policy available at: https://www.auda.org.au/policies/index-of-published-policies/2010/2010-01/

Domain deleted within three days of creation (add grace period)

- No "pendingDelete" status applied.
- Instant removal from DNS
- Instant purging from the Registry
- Refunded creation fee
- Irreversible

Domain deleted after three days of creation

- "pendingDelete" status applied for three days.

- Instant removal from DNS
- The domain name cannot be updated or transferred
- No refund.
- Can be manually undeleted (via an email request to Registrar Support).
- The domain name will be published on the Official Domain Drop List
- After 3 calendar days, domain name will be purged at the next purge cycle. The Purge Cycle runs at 1.00pm AEST (2.00pm AEDT) on every day, including weekends and public holidays.

Domain deleted for breach of auDA Policy (policy delete)

- "pendingDelete" status applied for fourteen days.
- Instant removal from DNS
- The domain name cannot be updated or transferred
- No refund.
- Can be manually undeleted (via an email request to Registrar Support) on auDA's instruction
- The domain name will be published on the Official Domain Drop List (unless a Community Geographic Domain Name – see https://www.auda.org.au/policies/index-of-published-policies/2008/2008-04/)
- After 14 calendar days, domain name will be purged at the next purge cycle. The Purge Cycle runs at 1.00pm AEST (2.00pm AEDT) on every day, including weekends and public holidays.

Domain Field Descriptions

Field	Min. Occurs	Max. Occurs	Min. Len.	Max. Len.	Validation	Specified by:
Domain Label/Prefix	1	1	2	63	"^[[:alnum:]]([[:alnum:]]|-){0,61}[[:alnum:]]\.ZONE$"	RFC
Password/ authInfo	1	1	6	32	at least one letter ([[:alpha:]]) and one number ([[:digit:]]) and not based on a dictionary word	auDA
Registrant Contact	1	1	3	16	'^[^'||chr(13)||chr(10)||chr(9)||chr(32)||'][^'||chr(13)||chr(10)||chr(9)||']{1,14}[^'||chr(13)||chr(10)||chr(9)||chr(32)||']$'	Server
Technical Contact (s)	1	Un-bounded	3	16	'^[^'||chr(13)||chr(10)||chr(9)||chr(32)||'][^'||chr(13)||chr(10)||chr(9)||']{1,14}[^'||chr(13)||chr(10)||chr(9)||chr(32)||']$'	Server
Admin Contacts	0	Un-bounded	3	16	'^[^'||chr(13)||chr(10)||chr(9)||chr(32)||'][^'||chr(13)||chr(10)||chr(9)||']{1,14}[^'||chr(13)||chr(10)||chr(9)||chr(32)||']$'	Server
Billing Contacts	0	Un-bounded	3	16		Server
Name Servers	0	13	1	255		Schema
auExtension						
Registrant Name	1	1	1	255		au Schema
Registrant ID Type	0	1	3	5		au Schema
Registrant ID Number	0	1	1	255		au Schema
Eligibility Type	1	1	4	25		au Schema
Eligibility Name	0	1	1	255		au Schema
Eligibility ID type	0	1	2	6		au Schema
Eligibility ID number	0	1	1	255		au Schema
Policy Reason	1	1	1	3	Must be between 1 and 2	au Schema

B5 Hosts

Host Identifier

The format for a host Repository Object Identifier (ROID) is Hnnnnnnn-AR where nnnnnnn is a zero-padded integer assigned by AusRegistry. The AR suffix is an abbreviation for AusRegistry. For more information about the host identifier and other fields of a host please refer to the host field descriptions.

Valid Hosts

A valid host is defined as having either:

- a parent domain that exists in the Registry
- or a valid TLD not provisioned by this Registry (such as .info, .biz, etc).

Hosts for Zones Administered by this Registry

- The chosen option for implementation of RFC EPP treats hosts as EPP objects that must be provisioned in the Registry prior to being delegated to (see RFC 5732 https://www.rfc-editor.org/rfc/rfc5732.txt).. The alternative specified by the EPP was to treat hosts as attributes of domains, but this implementation was generally rejected by the au community.
- Any Registrar can create a host for a domain that they do not sponsor.
- If the host creator is not the sponsor of the parent domain, host ownership is automatically transferred to the sponsor of the parent domain.
- Unused hosts are flushed from the database after three months (90 days) of inactivity.
- A host cannot be deleted if they are associated with ANY domains whether the domains are sponsored by the host sponsor or not.
- Only sponsors of parent domains can update hosts or create child host records with IP addresses.

Unused Hosts

Unused hosts are flushed from the database after three months (90 days) of inactivity.

TLD.CC Host Create/Update Permission Tables

Domain Sponsor: Registrar A Host Creator: Registrar A		
Host type	Create	Create with IP
z.2LD.CC y.z.2LD.CC x.y.z.2LD.CC	Yes Yes Yes	Yes Yes Yes

Domain Sponsor: Registrar A Host Creator: Registrar B		
Host type	Create	Create with IP
z.2LD.CC y.z.2LD.CC x.y.z.2LD.CC	Yes Yes Yes	No No No

Where 2LD can be: .com, .net, .org, .id, .asn, .gov, or .edu
Where CC can be: .au

Rule for when a Glue Record is Published

Glue Records will only be published when a host is assigned to its parent domain. No other IP addresses present in a host record will be published under any circumstances.

In addition, the requirement to have glue records is not verified and lame delegations are possible. Registrars should implement checks for this in their own systems.

IPv6 Support

AusRegistry accepts IPv6 host addresses in any valid format however they are stored in their condensed format. This means IPv6 addresses contained in responses to info commands, the WhoIs and the DNS will be in a compressed format. For more information about IPv6 addresses and formats, please consult RFC 4291 IP Version 6 Addressing Architecture (https://www.rfc-editor.org/rfc/rfc4291.txt).

Host Field Descriptions

Field	Min Occurs	Max Occurs	Min Len	Max Len	Validation	Specified By
Host Name	1	1	1	63		RFC 1123
IP Address(es)	0	13	3	45	if type=v4 then [[:digit:]]{1,3}(.[[:digit:]]{1,3}){3} if type=v6 then [0-9a-fA-F]{1-4} (:[0-9a-fA-F]{1,4}){7}	Schema

B6 Contacts

Contact Identifiers

The format for a contact Repository Object Identifier (ROID) is Cnnnnnnn-AR where nnnnnnn is a zero-padded integer assigned by AusRegistry. The AR suffix is an abbreviation for AusRegistry. Contacts also have an additional ID assigned by the Registrar. This is a text field with the only condition enforced that they are unique amongst all contacts within the Registry system.

Unused contacts

Unused contacts are flushed from the database periodically. Notice is given to Registrars before this occurs.

Minimum Contact Information

The Registry system has requirements for minimum information that needs to be populated in a contact (further to the minimum requirements of RFC 5733). Currently these are just an email address. Contacts for au domains that are within Australia (their country code is AU) must have four digit postcodes and have a valid city/state/postcode combination. See the auDA policy on contacts (https://www.auda.org.au/policies/2010-07). For more details please refer to the field descriptions.

Internationalised and Local Address Details

The only types of address details currently accepted by the Registry are those of *type="int".* Any attempt to add or update a contact with address details of *type="loc"* will result in a policy error.

Contact Field Descriptions

Field	Min. Occurs	Max. Occurs	Min. Len.	Max. Len.	Validation	Specified by:
Contact Identifier	1	1	3	16	'^[^'||chr(13)||chr(10)||chr(9)||chr(32)||'][^'||chr(13)||chr(10)||chr(9)||']{1,14}[^'||chr(13)||chr(10)||chr(9)||chr(32)||']$'	Server
authInfo	1	1	6	32	at least one letter ([[:alpha:]]) and one number ([[:digit:]]) and not based on a dictionary word	auDA Policy 2002-29
Postal Information						
Name	1	1	1	255		Schema
Organization	0	1	1	255		Schema
Street	1	3	1	255	1-255 length in each occurrence	Schema
City	1	1	1	255		Schema
State or Province	0	1	1	255		Schema
Postal Code	0	1	1	255	Not NULL if country is AU	Server
Country Code	1	1	2	2		Schema
Contact Information						
Email	1	1	1	255		Schema
Voice (telephone)	0	1	4	17	'^(\+[[:digit:]]{1,3}\.[[:digit:]]{1,14})?$'	Schema
Voice Extension (x=)	0	1	1	10	Must convert to a number	Server
Fax	0	1	4	17	'^(\+[[:digit:]]{1,3}\.[[:digit:]]{1,14})?$'	Schema
Fax Extension (x=)	0	1	1	10	Must convert to a number	Server

B7 Transfers

The transfer process relies on only the Registrant contact for a domain having access to the domain (authInfo) password. The Registrant may obtain the current authInfo for a domain from the current sponsoring Registrar. It is the responsibility of the sponsoring Registrar to verify the authenticity of requests and provide the password only to the appropriate party; emailing the password to the current Registrant contact email address is one suitable mechanism that satisfies the requirements – this of course requires that contact details are kept accurate.

The Registrant MUST provide the password to the Registrar to which they wish to transfer the domain. The Registrar will then send an EPP <transfer> command containing the provided authInfo. Alternatively the Registrant may provide the ROID and authinfo of one of the contact objects associated with the domain, however how the Registrant is to obtain this information is currently unclear and not specified in any auDA policy.

clientTransferProhibited Status

auDA policy prohibits the use of the clientTransferProhibited status on a domain.See https://www.auda.org.au/policies/index-of-published-policies/2013/2013-02/ This means that any update command that attempts to set this status will fail with a parameter value policy error. Similarly, Registrars are NOT able to use a transfer reject command to stop a domain transfer from occurring. Registrars may approve a transfer earlier or it will automatically proceed in 48 hours. A renew can be applied during the transfer process (if the domain is within 90 days of expiry) and the domain will obtain a new expiry date of two years from the date of expiry.

Contacts after a Transfer of Domain

Contacts linked with a domain are not explicitly transferred with the domain (unlike hosts). The gaining Registrar of the transferred domain has the following options:

- Request a transfer of contact from the current sponsoring Registrar to the gaining Registrar. This is done in the same way that domain transfers are done. The gaining Registrar will require the authInfo (password) for the contact. In the .au name space, the passwords of the legacy domains that were involved in the initial data load (transitioned domains) were made to be the same password of the contact associated with it. The transfer of a contact away from a Registrar needs to be approved by the losing registrar; otherwise it will automatically be approved after 48 hours. After this two day period, the gaining Registrar will then be the sponsoring Registrar of the contact and be able to update its details.

- Keep the original contacts as they are, and allow the original sponsoring Registrar for the contact remain so, thus resulting in contacts the gaining Registrar cannot modify.

- Create new contacts and associate them with the domain instead. This way the gaining Registrar will be the owner of the contacts and therefore be able to make whatever changes are necessary to the contact record.

Host Transfers

Host objects are always transferred along with their parent domain from the losing Registrar to the gaining Registrar. This is specified as part of the EPP and this Registry complies with the requirements without modification.

Registrant Transfers

To transfer a domain to a new registrant, the Modify Registrant option under the Domains menu will allow the sponsoring Registrar to submit a change request via the appropriate .au Extensions. . The change request will be manually reviewed by both the Registry and auDA from the Registry's management interface. . A renew is applied during the transfer process and the domain will obtain a new expiry date of two years from the date of transfer approval

Transfers During or After Expiry Date.

Since the whole transfer process can take up to 48 hours, domains can expire during that time. If a domain is to expire during the transfer process, it will not be undelegated. Transfer of a domain after expiry has no effect on the normal expiry process, unless the transfer is a combined transfer/renew command, in which case the serverHold status is removed and the domain is re-inserted into the DNS if appropriate.

B8 Poll Messages

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.

B9 Email Messages sent to Registrars/Registrants

Subject	Body	Conditions
Registrar Transaction Statistics for <<date>>	Dear Registrar,<<CRLF>><<CRLF>>Your domain transaction summary for <<date>> is as follows:<<CRLF>><<CRLF>>Domains Transferred In: <<transfers in>><<CR LF>>Industry Domains Transferred In: <<industry transfers in>><<CRLF>>Domain Transfers Cancelled : <<transfers cancelled>><<CRLF>>Industry Domain Transfers Cancelled : <<industry transfers cancelled>><<CRLF>>Domains Pending Transfer In : <<transfers pending in>><<CRLF>>Industry Domains Pending Transfer In : <<industry pending transfer>><<CRLF>>Domains Transferred Out : <<transfers out>><<CRLF>>Industry Domains Transferred Out : <<industry transfers out>><<CRLF>>Domains Created : <<domain creates>><<CRLF>>Industry Domains Created : <<industry creates>><<CRLF>>Domains Cancelled: <<cancels>><<CRL F>>Industry Domain Cancelled: <<industry cancels>><<CRLF>>Domains Expired : <<expired>><<CRLF>>Industry Domains Expired : <<industry expired>><<CRLF> >Domains Deleted : <<deletes>><<CRLF>>Industry Domains Deleted : <<industry deletes>><<CRLF>>Domains Renewed : <<renews>><<CRLF>>Industry Domains Renewed : <<industry renews>><<CRLF>><<CRLF>><<CRLF>> Kind regards,<<CRLF>>AusRegistry	Sent daily upon completion of update of daily growth statistics.
Registry Activity Statement Details	Dear <<registrar.reg_bill_name>>,<<CRLF>>Your requested Registry Activity Statement Report is now available for download from the following URL.<<CRLF >>https://admin.ausregistry.net.au:10443/DownloadFile?type=reports\&fileName=<<FILENAME>><<CRLF>>Please direct any queries about this report to <<CRLF>>accounts@ausregistry.net.au<<CRLF>>or call the Accounts department on +61.398663710.<<CRLF>>Kind Regards,<<CRLF>>Accounts Department<<CRLF>>AusRegistry<<CRLF>>	Requested by Registrars via Registrar's admin Website.
Pending expiry of domain for a domain sponsored by auDA	Dear Domain Name Holder<<CRLF>><<CRLF>>The domain name <Domain Name> is registered to <Registrant Name> and will expire on <Date>.<<CRLF>><<CRLF>>auDA is the Australian Government endorsed Industry Regulator of the Australian domain space (.au domain names). New rules introduced on 1 July 2002 require all .au domain names to be renewed every 2 years. For more information please see http://www.auda.org.au/news/netau-orgau/.<<CRLF>><<CRLF>>This email explains how you can renew your domain name before it expires on <Date>. Please follow the easy steps below.<<CRLF>><<CRLF>>Step 1<<CRLF>> Get your Domain Name Password (formerly called Registry Key)<<CRLF>>To renew your domain name you will need to know your Domain Name Password. As a security measure, all .au domain names are password protected.<<CRLF>><<CRLF>>You can have your Domain Name Password emailed to you by going to the Recover Password tool at http://admin.auda.org.au/ and following the instructions.<<CRLF>><<CRLF>>Step 2<<CRLF>>Select an auDA Accredited Registrar<<CRLF>>Registrars are accredited by auDA and their job is to manage the domain name by renewing it for you. You must select a Registrar from the list of Registrars at http://www.auda.org.au/registrars/accredited-registrars/. Service offerings and renewal fees vary between Registrars, so you should shop around according to your needs.<<CRLF>><<CRLF>>Step 3<<CRLF>>Renew your Domain Name<<CRLF>>Contact the Registrar that you have selected to renew your domain name. You will need to give them your Domain Name Password and pay the renewal fee. In most cases you will be able to renew your domain name online. The Registrar will be able to assist you with any queries you may have.<<CRLF>><<CRLF>>Please note it is YOUR responsibility to renew your domain name before the expiry date. If you do not renew your domain name, it will be deleted.<<CRLF>>We strongly advise you to take early action to protect your domain name.<<CRLF>><<CRLF>><<CRLF>>Regards<<CRLF>><<CRLF>><<CRLF>><<CRLF>>CEO<<CRLF>>.au Domain Administration Ltd<<CRLF>><<CRLF>> For further information regarding the renewal of your domain name, please contact auDA at:<<CRLF>>Phone 1800 668 019<<CRLF>>Email renewals@auda.org.au <<CRLF>><<CRLF>>*******<<CRLF>>.au Domain Administration Ltd <<CRLF>>ACN 079 009 340 ABN 38 079 009 340<<CRLF>>107 Faraday Street, Carlton Vic 3053<< CRLF>>1800 668 019<<CRLF>>www.auda.org.au<<CRLF>>The first weekday that a domain is sponsored by auDA, this is sent to Registrants to inform them of the expiry policy for .au domain names – only one email is ever sent for any given domain.	The first weekday that a domain is sponsored by auDA, this is sent to Registrants to inform them of the expiry policy for .au domain names – only one email is ever sent for any given domain.
Domains to expire in <<N>> days	Dear Registrar,<<CRLF>>The following domains are listed in AusRegistry's database to expire in <<N>>days<<CRLF>><<domain name list>><<CRLF>>Please ensure you are taking appropriate action in order to	Email sent daily to sponsoring

	have these domains renewed in time and reduce the risk of them being undelegated from the zone files <<CRLF>>Kind regards,<<CRLF>>AusRegistry	Registrars listing all sponsored domains to expire in N days, where N is in (7,14,21,28).
Domain <<domain name>> to expire in <<N>> days	The domain <<domain name>> is due to expire on <<expiry date> and you have yet to choose a new registrar.<<CRLF>>You will need to select a registrar and contact them to make arrangements to transfer and renew your domain name. More information is available at <<info url>><<CRLF>>Should you fail to do this before the expiry of your domain, it will be undelegated and become available for registration 14-21 days after it expires. <<CRLF>>Kind regards ,<<CRLF>>auDA	A domain sponsored by auDA has not been transferred to an accredited Registrar and is due to expire in N days, where N in (7,14,28). This check is run daily.
Closing Balance for <<date>>	Your balance at end of business <<date>> was $<<closing balance>><<CRLF>>Kind regards,<<CRLF>>AusRegistry	Sent daily to each registrar.
Domains to expire in <<N>> days	Dear Registrar,<<CRLF>>The following domains are listed in AusRegistry's database to expire in <<N>> days<<CRLF>><<domain list>><<CRLF>>Please ensure you are taking appropriate action in order to have these domains renewed in time and reduce the risk of them being undelegated from the zone files. <<C RLF>>Kind regards,<<CRLF>>AusRegistry	The list of domains to expire in N days is checked once each day; this email is sent to the Registrars who sponsor any domains that will expire in N days.
Introduction to .au Domain Names	Hello,<<CRLF>>You are receiving this email because you are listed as the registrant<<CRLF>>contact for a new .au domain name <domain>.<<CRLF>><<CRLF>> I am the CEO of auDA, the Australian<<CRLF>>internet domain name regulator. I am writing to you to explain some of<<CRLF >>the things that auDA does to safeguard both <<CRLF>>your domain name and your rights as a domain name registrant. <<CRLF>><<CRLF>>Each domain name in .au is managed by an auDA accredited registrar.<<CRLF>>Registrars and their resellers are bound by a Code of Practice<<CRLF>>(http://www.auda.org.a u/policies/auda-2003-09/).<<CRLF>><<CRLF>>In our role as industry regulator, auDA publishes Consumer Alerts and<<CRLF>>other information that may be relevant to you. If you want to ensure<<CRLF>>that you are kept up to date, you can subscribe <<CRLF>>to our announcements list at<<CRLF>>http://www.auda.org.au/about/announcements/.<<CRLF>><<CRLF>>One of the responsibilities you have as a domain name registrant is to<<CRLF>>ensure that the contact information in your domain name record is kept<<CRLF>>up to date. To check your information go to http://www.mywebname.com.au/<<CRLF>>and do a Whois search. If you need to make changes to the information<<CRLF>>then you should contact your registrar.<<CRLF>><<CRLF>>I hope this information is of use to you. More detailed information can<<CRLF>>be found on our web site, including our online brochure Australian<<CRLF>>Domain Names - An Overview <<CRL F>>at http://www.auda.org.au/pdf/auda-overview.pdf.<<CRLF>><<CRLF>>Please do not reply to this email by using the reply button. If you wish<<CRLF>>to contact auDA, please email info@auda.org.au.<<CRLF>><<CRLF>>Regards<<CRLF>><<CRLF>> <<CRLF>>CEO-auDA <<CRLF>>info@auda.org.au<<CRLF>>www .auda.org.au	Registration of a .au domain.

B10 Response codes

Error #	Response
1000	Command completed successfully
1001	Command completed successfully; action pending
1300	Command completed successfully; no messages
1301	Command completed successfully; ack to dequeue
1500	Command completed successfully; ending session
2000	Unknown command
2001	Command syntax error
2002	Command use error
2003	Required parameter missing
2004	Parameter value range error
2005	Parameter value syntax error
2100	Unimplemented protocol version
2101	Unimplemented command
2102	Unimplemented option
2103	Unimplemented extension
2104	Billing failure
2105	Object is not eligible for renewal
2106	Object is not eligible for transfer
2200	Authentication error
2201	Authorization error
2202	Invalid authorization information
2300	Object pending transfer
2301	Object not pending transfer
2302	Object exists
2303	Object does not exist
2304	Object status prohibits operation
2305	Object association prohibits operation
2306	Parameter value policy error
2307	Unimplemented object service
2308	Data management policy violation
2400	Command failed
2500	Command failed; server closing connection
2501	Authentication error; server closing connection
2502	Session limit exceeded; server closing connection

Server errors

If at any stage you receive a server error in the transaction ID of a command failed response to a command you have sent, please email support@ausregistry.com.au with as much detail as possible. We will require the XML you have sent plus the response you received as well as any timestamps if it is not contained within the XML.

B11 WHOIS

- IP addresses limited 20 WHOIS lookups per hour.
- IP addresses limited to 200 lookups in a 24 hour period
- Blacklist lasts for 24 hours from the time the limit was exceeded.
- Limit of 200 lookups in a single day.

B12 Glossary

The table below contains the terms and abbreviations used within this document:

Term	Description
auDA	.au Domain Administration Limited is the policy authority and industry self-regulatory body for the .au domain space. **http://www.auda.org.au**
DNS	The Domain Name System is the system that translates Internet domain names into IP numbers. A "DNS Server" is a server that performs this kind of translation.
EPP	Extensible Provisioning Protocol (EPP), an XML text protocol that permits multiple service providers to perform object provisioning operations using a shared central object repository.
XML	Extensible Markup Language is the universal format for structured documents and data on the Web.
TLD	Top Level Domain. E.g. .com, .net, .org., .au, .sydney
2LD	2nd Level Domain. For example .com.au, .net.au

APPENDIX C: .AU EXTENSIONS

For a description of EPP command formats see RFC 5730:
https://tools.ietf.org/html/rfc5730

Information about the current .au extensions is available on GitHub at:
https://github.com/AusRegistry/ar-epp-extensions and
http://ausregistry.github.io/doc/au-extensions-1.2/au-extensions-1.2.html

.au Extensions Version 1.2

This document contains explanations of the relevant commands from the RFC EPP documents that are effected by the inclusion of the .au extensions.

The use of extensions will be identified in the <*greeting*> and <*login*> commands.

The extended command/s are <*domain:create*> and <*domain:update*>

The extended response/s are to the <*domain:info*> command.

An additional protocol extension for changing the registrant information associated with a domain name has been defined: <*auext:registrantTransfer*>. This allows auDA to manage policy around the transfer of domain names between registrants.

These extensions are explained below:

Greeting Format

All standard EPP elements apply plus:

- A <svcExtension> element that contains a <extURI> elements that contains namespace URI representing the .au domain extensions

Example greeting with .au extensions specified:

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S:     xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S:     epp-1.0.xsd">
S:  <greeting>
S:    <svID>Example EPP server epp.example.tld</svID>
```

```
S:    <svDate>2000-06-08T22:00:00.0Z</svDate>
S:    <svcMenu>
S:      <version>1.0</version>
S:      <lang>en</lang>
S:      <objURI>urn:ietf:params:xml:ns:domain-1.0</objURI>
S:      <objURI>urn:ietf:params:xml:ns:host-1.0</objURI>
S:      <objURI>urn:ietf:params:xml:ns:contact-1.0</objURI>
S:      <svcExtension>
S:        <extURI>urn:X-au:params:xml:ns:auext-1.2</extURI>
S:        <extURI>urn:X-au:params:xml:ns:audomain-1.1</extURI>
S:      </svcExtension>
S:    </svcMenu>
S:    <dcp>
S:       <access><all/></access>
S:       <statement>
S:            <purpose><admin/><prov/></purpose>
S:             <recipient><ours/>><public/></recipient>
S:              <retention><stated/></retention>
S:        </statement>
S:     </dcp>  S:  </greeting>
S:</epp>
```

EPP <login> Command

The au extensions <extURI> MUST be specified at the time of login.

```
S:       <?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:       <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
$:          xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
S:         <command>
S:             <login>
S:                  <clID>REGISTRAR</clID>
S:                 <pw>p4ssw0rd!</pw>
S:                 <options>
S:                          <version>1.0</version>
S:                          <lang>en</lang>
S:                 </options>
S:                   <svcs>
S:                    <objURI>urn:ietf:params:xml:ns:contact-1.0</objURI>
S:                     <objURI>urn:ietf:params:xml:ns:domain-1.0</objURI>
S:                     <objURI>urn:ietf:params:xml:ns:host-1.0</objURI>
S:                      <svcExtension>
S:                           <extURI>urn:X-au:params:xml:ns:auext-1.2</extURI>
S:                            <extURI>urn:X-au:params:xml:ns:audomain-1.1</extURI>
S:                      </svcExtension>
S:                 </svcs>
S:             </login>
S:          </command>
S:       </epp>]]>
```

EPP <info> Response

In addition to the standard EPP elements found in a domain info command, a domain info command should also conform to the following using the <extension> element that contains the extensions specific to the registry.

- An <auext:infData> element which contains the .au extension information.

- An <auext:auProperties> element which contains the following elements:

- A <auext:registrantName> element MUST be provided. This element MUST contain an English readable string for the registrant's name.

- An OPTIONAL <auext:registrantID> element that represents the identifier for the registrant.

Every <auext:registrantID> element MUST have a "type" attribute which is the enumeration of valid registrant ID values specified in this document. The type attribute identifies the type of registrant ID specified for the <registrantID> element. For example, an Australian Company Number (ACN) would have a *type* of “ACN”.

- An <auext:eligibilityType> element MUST be provided. This element MUST be one of the valid eligibility type values specified by this document.

- An OPTIONAL <auext:eligibilityName> element which is only used if different from the registrant's name.

- An OPTIONAL <auext:eligibilityID> element that represents the identifier for the eligibility name element.

Every <auext:eligibilityID> element MUST have a "type" attribute which is the enumeration of valid eligibility ID values specified in this document. The type attribute identifies the type of eligibility ID specified for the <eligibilityID> element.

- A <auext:policyReason> element MUST be provided. This element MUST be one of the valid policy reasons specified by this document.

Example <info> response for an *authorized* client (which is a registrar requesting information about a domain name under the registrar’s management):

S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>

```
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S:    xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
S:  <response>
S:   <result code="1000">
S:     <msg>Command completed successfully</msg>
S:   </result>
S:   <resData>
S:     <domain:infData
S:      xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S:      xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd”>

S:       <domain:name>example.com.au</domain:name>
S:       <domain:roid> D0000003-AR</domain:roid>
S:       <domain:status s="ok" lang=”en”/>
S:       <domain:registrant>EXAMPLE</domain:registrant>
S:       <domain:contact type="tech">EXAMPLE</domain:contact>
S:       <domain:ns>

S:          <domain:hostObj>ns2.example.com.au</domain:hostObj>
S:          <domain:hostObj>ns2.example.com.au</domain:hostObj>
S:       </domain:ns>
S:       <domain:host>ns1.example.com.au</domain:host>
S:       <domain:host>ns2.example.com.au</domain:host>
S:       <domain:clID>Registrar</domain:clID>
S:       <domain:crID>Registrar</domain:crID>
S:       <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:       <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>

S:       <domain:authInfo>
S:           <domain:pw>0192pqow</domain:pw>
S:       </domain:authInfo>
S:     </domain:infData>
S:   </resData>

S:       <extension>
S:          <auext:infData
S:                xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
S:                xsi:schemaLocation=urn:X-au:params:xml:ns:auext-1.2 auext-1.2.xsd">
S:                <auext:auProperties>
S:                  <auext:registrantName>
S:                        RegistrantName Pty. Ltd.
S:                  </auext:registrantName>
S:                  <auext:registrantID type="ACN">
S:                        123456789
S:                  </auext:registrantID>
S:                  <auext:eligibilityType>
S:                        Other
S:                  </auext:eligibilityType>
S:                  <auext:eligibilityName>
```

```
S:                          Registrant Eligibility
S:                  </auext:eligibilityName>
S:                  <auext:eligibilityID type="ABN">
S:                          987654321
S:                  </auext:eligibilityID>
S:                  <auext:policyReason>2</auext:policyReason>
S:                </auext:auProperties>
S:              </auext:infData>
S:          </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

This .au Extension information is only returned to the sponsoring registrar, all others will receive the data as below:

Example <info> response for an *unauthorized* client (which is a registrar making a query about a domain name managed by another registrar):

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S:     xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S:     epp-1.0.xsd">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
S:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S:       xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0 xsd>

S:       <domain:name>example..com.au</domain:name>
S:       <domain:roid>D0000003-AR</domain:roid>
S:       <domain:clID>Registrar</domain:clID>
S:      </domain:infData>
S:    </resData>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

EPP <create> Command

In addition to the standard EPP elements found in a <domain:create> command, a <domain:create> command should also conform to the following using the <extension> element that contains the extensions specific to the registry.

-

- An <auext:create> element which contains a number of elements that hold the information which is specific to the .au name space.

- An <auext:auProperties> element whuch contains the following child elements:

- An <auext:registrantName> element MUST be provided. This element MUST contain an English readable string for the registrant's name.

- An OPTIONAL <auext:registrantID> element that represents the identifier for the registrant.

Every <auext:registrantID> element MUST have a "type" attribute which is the enumeration of valid registrant ID values specified in this document. The type attribute identifies the type of registrant ID specified for the <registrantID> element.

- An <auext:eligibilityType> element MUST be provided. This element MUST be one of the valid eligibility type values specified by this document.

- An OPTIONAL <auext:eligibilityName> element which is only used if different from the registrant's name, and represents the name of the individual or organization which the eligibility is based on.

- An OPTIONAL <auext:eligibilityID> element that represents the identifier for the eligibility name element.

Every <auext:eligibilityID> element MUST have a "type" attribute which is the enumeration of valid eligibility ID values specified in this document. The type attribute identifies the type of eligibility ID specified for the <eligibilityID> element.

- A <auext:policyReason> element MUST be provided. This element MUST be one of the valid policy reasons specified by this document.

Example <create> command:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C:    xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C:    epp-1.0.xsd">
C:  <command>
```

```
C:    <create>
C:      <domain:create
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C:      xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0 xsd”

C:        <domain:name>example.com.au</domain:name>
C:        <domain:registrant>Registrant</domain:registrant>

C:        <domain:contact type="tech">Tech2</domain:contact>
C:        <domain:authInfo>
C:            <domain:pw>0192pqow</domain:pw>
C:        </domain:authInfo>
C:      </domain:create>
C:      </create>
C:
C:      <extension>
C:             <auext:create
C:                 xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
C:                 xsi:schemaLocation="urn:X-au:params:xml:ns:auext-1.2 auext-1.2.xsd">
C:              <auext:auProperties>
C:                  <auext:registrantName>
C:                      RegistrantName Pty. Ltd.
C:                   </auext:registrantName>
C:                   <auext:registrantID type="ACN">
C:                     123456789
C:                   </auext:registrantID>
C:                   <auext:eligibilityType>
C:                     Other
C:                   </auext:eligibilityType>
C:                   <auext:eligibilityName>
C:                       Registrant Eligibility
C:                   </auext:eligibilityName>
C:                   <auext:eligibilityID type="ABN">
C:                     987654321
C:                   </auext:eligibilityID>
C:                   <auext:policyReason>2</auext:policyReason>
C:                 </auext:auProperties>
C:             </auext:create>
C:          </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C:</epp>
```

EPP <update> Command

In addition to the standard EPP elements found in a <domain:update> command, a <domain:update> command should also conform to the following using the <extension> element that contains the extensions specific to the

registry. All information will be replaced with the new .au extension information.

- An <auext:update> element which contains a number of elements that hold the information which is specific to the .au name space.

- An <auext:auProperties> element whuch contains the following child elements:

- An <auext:registrantName> element MUST be provided. This element MUST contain an English readable string for the registrant's name.

- An OPTIONAL <auext:registrantID> element that represents the identifier for the registrant.

Every <auext:registrantID> element MUST have a "type" attribute which is the enumeration of valid registrant ID values specified in this document. The type attribute identifies the type of registrant ID specified for the <registrantID> element.

- An <auext:eligibilityType> element MUST be provided. This element MUST be one of the valid eligibility type values specified by this document.

- An OPTIONAL <auext:eligibilityName> element which is only used if different from the registrant's name, and represents the name of the individual or organization which the eligibility is based on.

- An OPTIONAL <auext:eligibilityID> element that represents the identifier for the eligibility name element.

Every <auext:eligibilityID> element MUST have a "type" attribute which is the enumeration of valid eligibility ID values specified in this document. The type attribute identifies the type of eligibility ID specified for the <eligibilityID> element.

- A <auext:policyReason> element MUST be provided. This element MUST be one of the valid policy reasons specified by this document.

- A <auext:explanation> element MUST be provided. This element must contain an explanation as to the purpose of the update. For example a correction of a spelling mistake. It should be noted that these explanations are reviewed by the regulator and this update mechanism is NOT provided to facilitate transfer of Registrant.

Example <domain:update> command:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
 <command>
  <update>
   <domain:update
    xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
    xsi:schemaLocation=
    "urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd">
    <domain:name>example.com.au</domain:name>
    <domain:add>
     <domain:contact type="tech">Tech2</domain:contact>
    </domain:add>
   </domain:update>
  </update>
  <extension>
   <auext:update
    xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
    xsi:schemaLocation=
          "urn:X-au:params:xml:ns:auext-1.2 auext-1.2.xsd">
    <auext:auProperties>
     <auext:registrantName>
      New Name
     </auext:registrantName>
     <auext:registrantID type="ACN">
      123456789
     </auext:registrantID>
     <auext:eligibilityType>
      Other
     </auext:eligibilityType>
     <auext:eligibilityName>
      Registrant Eligibility
     </auext:eligibilityName>
     <auext:eligibilityID type="ABN">
      987654321
     </auext:eligibilityID>
     <auext:policyReason>2</auext:policyReason>
    </auext:auProperties>
    <auext:explanation>
     Registrant made spelling mistake during registration.
    </auext:explanation>
   </auext:update>
  </extension>
  <clTRID>ABC-12345</clTRID>
 </command>
</epp>
```

AU Extension EPP <registrantTransfer> command

This command is used to initiate a transfer of registrant of a domain name. A transfer of domain name from one registrant to another also results in a new license period for the domain name. An <auext:registrantTransfer> command is defined as follows:

An <auext:command> element which contains the following child elements:

- An <auext:registrantTransfer> element which contains the following child elements:
- An <auDomain:registrantTransfer> element which contains the following child elements:
    - An <auDomain:name> element MUST be provided which specifies the fully qualifed name of the domain of which the registrant should be transfered.
    - An <auDomain:curExpDate> element MUST be provided which specifies the current expiry date of the domain.
    - An <auDomain:period> element that specifies the period for which the new registrant wants the name to be registered
    - A <auDomain:auProperties> element that contains the following child elements:
        - A <auDomain:registrantName> element MUST be provided. This element MUST contain an english readable string for the Registrant's name.
        - An OPTIONAL <auDomain:registrantID> element that represents the identifier for the Registrant.
            - Every <auext:registrantID> element MUST contain a "type" attribute that identifies the type of the Registrant ID specified by the <registrantID> element.
        - An <auext:eligibilityType> element that contains the Registrant's eligibility type.
        - An OPTIONAL <auext:eligibilityName> element that contains the name of the individual or organisation that represents the Registrant which the eligibility is based on.
        - An OPTIONAL <auext:eligibilityID> element that contains the identifier for the eligibility name.
            - Every <auext:eligibilityID> element MUST have a "type" attribute that identifies the type of the eligibility ID specified for the <eligibilityName> element.

        - A <auext:policyReason> element that contains the policy reason for which the domain object registered under.
    - A <auDomain:explanation> element MUST be provided. This element must contain an explanation as to the purpose of the update For example a correction of a spelling mistake. It should be noted that these explanations are reviewed by the regulator and this update mechanism is NOT provided to facilitate transfer of registrant.
- An OPTIONAL <auext:clTRID> element which contains the client supplied identifier for the transaction.

Example <auext:registrantTransfer> command:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
 <extension>
  <auext:command
   xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
   xsi:schemaLocation="urn:X-au:params:xml:ns:auext-1.2
   auext-1.2.xsd">
   <auext:registrantTransfer>
    <auDomain:registrantTransfer
     xmlns:auDomain="urn:X-au:params:xml:ns:audomain-1.1"
     xsi:schemaLocation="urn:X-au:params:xml:ns:audomain-1.1 audomain-1.1.xsd">
     <auDomain:name>domain.com.au</auDomain:name>
     <auDomain:curExpDate>2000-04-03</auDomain:curExpDate>
     <auDomain:period unit="y">2</auDomain:period>
     <auDomain:auProperties>
      <auDomain:registrantName>
                New Name
      </auDomain:registrantName>
      <auDomain:registrantID type="ACN">
                123456789
      </auDomain:registrantID>
      <auDomain:eligibilityType>
                Other
      </auDomain:eligibilityType>
      <auDomain:eligibilityName>
                Registrant Eligibility
      </auDomain:eligibilityName>
      <auDomain:eligibilityID type="ABN">
                987654321
      </auDomain:eligibilityID>
      <auDomain:policyReason>2</auDomain:policyReason>
     </auDomain:auProperties>
     <auDomain:explanation>
```

```
          Previous registrant has sold the business
        </auDomain:explanation>
      </auDomain:registrantTransfer>
    </auext:registrantTransfer>
    <auext:clTRID>ABC-12345</auext:clTRID>
  </auext:command>
 </extension>
</epp>
```

---

au Extensions <registrantTransfer> Response

TOC

The following response will be returned from the au extensions <registrantTransfer> command:

- An <auext:response> element that contains the same child elements as the epp:response type does (see EPP RFC).

The resData section of this response contains the following:

- An <auDomain:rtrnData> element that contains the following child elements:
  - A <auDomain:name> element that contains the fully qualified name of the domain to which the registrant transfer was applied.
  - A <auDomain:exDate> element that contains the new expiry date of the domain after the registrant transfer.

Example <auext:registrantTransfer> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
 <extension>
  <auext:response
   xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
   xsi:schemaLocation="urn:X-au:params:xml:ns:auext-1.2 auext-1.2.xsd">
  <auext:result code="1000">
   <auext:msg>Command completed successfully</auext:msg>
  </auext:result>
  <auext:resData>
   <auDomain:rtrnData
       xmlns:auDomain="urn:X-au:params:xml:ns:audomain-1.1"
       xsi:schemaLocation="urn:X-au:params:xml:ns:audomain-1.1 audomain-1.1.xsd">
    <auDomain:name>domain.com.au</auDomain:name>
    <auDomain:exDate>2005-04-03T22:00:00.0Z</auDomain:exDate>
   </auDomain:rtrnData>
```

```
  </auext:resData>
  <auext:trID>
   <auext:clTRID>ABC-12345</auext:clTRID>
   <auext:svTRID>2389742981742</auext:svTRID>
  </auext:trID>
 </auext:response>
</extension>
</epp>
```

Formal Syntax

XML Schema [urn:X-au:params:xml:ns:auext-1.2]

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="urn:X-au:params:xml:ns:auext-1.2"
      xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
      xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
      xmlns:epp="urn:ietf:params:xml:ns:epp-1.0"
      xmlns="http://www.w3.org/2001/XMLSchema"
      elementFormDefault="qualified">

   <!--
   Import common element types.
   -->
   <import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
         schemaLocation="eppcom-1.0.xsd"/>
   <import namespace="urn:ietf:params:xml:ns:epp-1.0"
         schemaLocation="epp-1.0.xsd"/>

   <annotation>
      <documentation>
         .au Extensions to the Extensible Provisioning Protocol v1.2 schema.
      </documentation>
   </annotation>

   <!--
   Protocol extension framework elements.
   -->
   <element name="command" type="auext:commandType"/>

   <!--
   Protocol extension type definitions.
   -->

   <complexType name="commandType">
      <sequence>
         <choice>
            <element name="registrantTransfer"
                  type="epp:readWriteType"/>
         </choice>
         <element name="clTRID" type="epp:trIDStringType"
               minOccurs="0"/>
      </sequence>
   </complexType>

   <!--
   Command-response framework extension elements.
   -->
```

```
<element name="create" type="auext:createType"/>
<element name="update" type="auext:updateType"/>
<element name="infData" type="auext:infDataType"/>

<!--
.au update command extension
-->

<complexType name="updateType">
   <sequence>
      <element name="auProperties"
            type="auext:auPropertiesType"
            minOccurs="1"/>
      <element name="explanation" type="auext:explanationType"
            minOccurs="1"/>
   </sequence>
</complexType>

<!--
.au create command extension
-->

<complexType name="createType">
   <sequence>
      <element name="auProperties"
            type="auext:auPropertiesType" minOccurs="1"/>
   </sequence>
</complexType>

<!--
.au info response extension
-->

<complexType name="infDataType">
   <sequence>
      <element name="auProperties"
            type="auext:auPropertiesType" minOccurs="1"/>
   </sequence>
</complexType>

<!--
the .au extension domain properties
-->

<complexType name="auPropertiesType">
   <sequence>
      <element name="registrantName" type="eppcom:labelType"
            minOccurs="1"/>
      <element name="registrantID"
```

```
                type="auext:registrantIDType" minOccurs="0"/>
            <element name="eligibilityType" type="eppcom:labelType"
                minOccurs="1"/>
            <element name="eligibilityName" type="eppcom:labelType"
                minOccurs="0"/>
            <element name="eligibilityID"
                type="auext:eligibilityIDType" minOccurs="0"/>
            <element name="policyReason" type="integer"
                minOccurs="1"/>
        </sequence>
    </complexType>

    <!--
    the explanation type
    -->
    <simpleType name="explanationType">
        <restriction base="normalizedString">
            <maxLength value="1000"/>
        </restriction>
    </simpleType>

    <!--
    registrant id type is used for registrantID
    -->

    <complexType name="registrantIDType">
        <simpleContent>
            <extension base="eppcom:labelType">
                <attribute name="type" type="token" use="required"/>
            </extension>
        </simpleContent>
    </complexType>

    <!--
    eligibility id type is used for eligibilityID
    -->

    <complexType name="eligibilityIDType">
        <simpleContent>
            <extension base="eppcom:labelType">
                <attribute name="type" type="token" use="required"/>
            </extension>
        </simpleContent>
    </complexType>

    <!--
    End of schema.
    -->
</schema>
```

XML Schema [urn:X-au:params:xml:ns:audomain-1.1]

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="urn:X-au:params:xml:ns:audomain-1.1"
      xmlns:auDomain="urn:X-au:params:xml:ns:audomain-1.1"
      xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
      xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
      xmlns:auext="urn:X-au:params:xml:ns:auext-1.2"
      xmlns="http://www.w3.org/2001/XMLSchema"
      elementFormDefault="qualified">

   <!--
      Import common element types.
   -->

   <import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
         schemaLocation="eppcom-1.0.xsd"/>
   <import namespace="urn:ietf:params:xml:ns:domain-1.0"
         schemaLocation="domain-1.0.xsd"/>
   <import namespace="urn:X-au:params:xml:ns:auext-1.2"
         schemaLocation="auext-1.2.xsd"/>

   <annotation>
      <documentation>
         .au Domain Extensions to the Extensible
         Provisioning Protocol v1.0. schema.
      </documentation>
   </annotation>

   <!--
      Protocol extension framework command elements.
   -->

   <element name="registrantTransfer"
          type="auDomain:registrantTransferType"/>

   <!--
      Protocol extension framework response elements.
   -->
   <element name="rtrnData" type="auDomain:rtrnDataType"/>

   <!--
      Type definitions.
   -->

   <complexType name="registrantTransferType">
      <sequence>
         <element name="name" type="eppcom:labelType"
               minOccurs="1"/>
         <element name="curExpDate" type="date" minOccurs="1"/>
```

```
            <element name="period" type="domain:periodType"
                  minOccurs="0"/>
            <element name="auProperties"
                  type="auDomain:auPropertiesType" minOccurs="1"/>
            <element name="explanation" type="auext:explanationType"
                  minOccurs="1"/>
         </sequence>
      </complexType>

      <!--
         the .au extension domain properties
      -->
      <complexType name="auPropertiesType">
         <sequence>
            <element name="registrantName" type="eppcom:labelType"
                  minOccurs="1"/>
            <element name="registrantID"
                  type="auext:registrantIDType" minOccurs="0"/>
            <element name="eligibilityType" type="eppcom:labelType"
                  minOccurs="1"/>
            <element name="eligibilityName" type="eppcom:labelType"
                  minOccurs="0"/>
            <element name="eligibilityID"
                  type="auext:eligibilityIDType" minOccurs="0"/>
            <element name="policyReason" type="integer"
                  minOccurs="1"/>
         </sequence>
      </complexType>

      <complexType name="rtrnDataType">
         <sequence>
            <element name="name" type="eppcom:labelType"
                  minOccurs="1"/>
            <element name="exDate" type="dateTime" minOccurs="1"/>
         </sequence>
      </complexType>

      <!--
         End of schema.
      -->
   </schema>
```

APPENDIX D: EDU.AU REQUIREMENTS

D 1.0 Summary of Requirements Specific to .edu.au

Education Services Australia (ESA) is the registration body for the .edu.au domain (http://www.domainname.edu.au/) which:

- licenses domain names to education and training organisations eligible under policies set and implemented by the .edu.au Domain Administration Committee (eDAC) and the .au Domain Administration Limited (auDA)
- provides services to customers to maintain current domain names information
- implements the domain policies determined by eDAC and 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, CRICOS (Commonwealth Register of Institutions and Courses for Overseas Students) code, approved provider number 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
4. A number of business rules and processes that relate to legacy auDA policies are still in place or applied to .edu.au domains

D 1.1 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.

D 1.2 Eligibility Types

Below is a list of all eligibility types as they currently appear in the AusRegistry 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
Government Body	Added in 2015
Government School	
Higher Education Institution	
Industry Association	Added in 2015
National Body	Removed in 2015
Non-Governmental school	
Non-profit organization	Removed in 2015
Other	
Parent and Professional Association/Organization	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 eDAC, in accordance with the 2015-03 Policy Change Process Policy
http://www.domainname.edu.au/pdf/change_process.pdf

D 1.3 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.

D 1.4 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 eDAC, in accordance with the 2015-03 Policy Change Process Policy http://www.domainname.edu.au/pdf/change_process.pdf

D 1.4.1 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.

D 1.4.2 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.

D 1.4.3 Transfer of Registrant

Transfer of registrant requests that fall within 6 months of the domain name initially being registered are flagged as requiring regulatory approval for .edu.au. 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.

D 2.0 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 E: GOV.AU REQUIREMENTS

E1 Background of gov.au

See: https://www.domainname.gov.au

1. The gov.au Domain Name Policies (the 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 Digital Transformation Agency (DTA) (https://www.dta.gov.au/) within the Prime Minister and Cabinet portfolio of the Australian Government holds a sub-sponsorship agreement with .au Domain Administration (auDA), the industry self-regulatory body, for management of the gov.au domain.
5. The DTA manages the gov.au policies and administration in consultation with an inter-jurisdictional Domain Consultative Committee comprising of representatives from each jurisdiction.
6. All new policies and major policy changes are endorsed by the Online and Communications Council. Membership of the Online and Communications Council comprises the Australian Government Minister for Broadband, Communications and the Digital Economy (Chair), a senior Minister from each State and Territory and the President of the Australian Local Government Association.
7. Each jurisdiction may apply additional domain policies, standards and guidelines in assessing domain applications.
8. 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.
9. 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.

E2 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 **tas.gov.au** and **nt.gov.au** are not managed by the registry, and are managed with the DNS name service for tas.gov.au and nt.gov.au. There are no WHOIS entries for names at the fourth level of tas.gov.au and nt.gov.au. They effectively operate like a government department website within gov.au – like dta.gov.au.

E3 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).

E4 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.

E5 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.

E6 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 AusRegistry 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
8. Renewals are non-refundable transactions.

E7 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.