.au Domain Administration

Registry Technical Specification

DRAFT FOR COMMENT

March 2005

1.0 Introduction 1
2.0 Functional Specifications 2
2.1 Registry Access Protocol 2
2.1.1 EPP Software Development Toolkit 2
2.1.2 EPP Transport and Security 3
2.1.3 Other EPP Requirements 3
2.2 Registry Database 4
2.2.1 Database Service Performance and Availability 5
2.3 Authoritative Nameserver Service 5
2.3.1 Nameserver Reliability 5
2.3.2 Zone File Maintenance 6
2.3.3 Provision of Zone Files to auDA 6
2.3.4 DNS Service Performance and Availability 6
2.4 Public WHOIS Service 7
2.4.1 7
Registry-provided Public WHOIS 7
2.4.2 WHOIS Data Set 8
2.2.3 WHOIS Enquiries 8
2.2.4 Format of WHOIS Information 9
2.4.5 WHOIS Service Performance and Availability 10
2.5 Legacy Data 10
2.6 Functional Specification Response 11
3.0 Security Architecture 12
3.1 Security Policy 12
3.2 Security 13
3.3 Asset Classification and Control 13
3.4 Personnel Security 14
3.5 Physical and Environmental Security 15
3.5.1 Secure Area 15
3.5.2 Equipment Security 16
3.5.3 Cabling Security 16
3.5.4 Disposal of Equipment 17
3.6 Communications and Operational Management 17
3.6.1 Operational Procedures 17
3.6.2 System Planning and Acceptance 18
3.6.3 Protection against Malicious Software 18
3.6.4 Housekeeping 19
3.6.5 Network Management 19
3.6.6 Media Handling and Security 20
3.6.7 Exchanges of Information and Software 20
3.7 Access Control 21
3.7.1 Access Control Policy 21
3.7.2 User Access Management 21
3.7.3 User Responsibilities 22
3.7.4 Network Access Control 22
3.7.5 Operating System Access Control 23
3.7.6 Application Access Control 24
3.7.7 Monitoring System Access and Use 24

3.7.8 Mobile Computing and Teleworking 24
3.8 System Development and Maintenance.. 25
3.8.1 Security Requirements of Systems 25
3.8.2 Security in Application Systems 25
3.8.3 Cryptographic Controls.. 26
3.8.4 Security of System Files 26
3.8.5 Security in Development and Support Processes........................ 27
3.9 Business Continuity Management.. 28
3.10 Compliance.. 28
4.0 Business Continuity Plan... 30
5.0 Data Escrow Requirements.. 35
5.1 Data Escrow Operation.. 35
5.2 Data Escrow Contents... 37
5.3 Data Escrow Format.. 38
5.4 Data Escrow Proposal 38
6.0 Domain Name Expiry and Deletion 39
7.0 Reporting Requirements.. 40
8.0 Registrar Support Services... 43
Appendix A: Definition Of Terms 44

1.0 INTRODUCTION

This document defines the technical requirements of the Registry Service to be undertaken by a Registry Operator. The Technical Specification forms part of the Request for Tender. auDA may choose to amend any or all of the Specification from time to time in order to address new or changing requirements. When amendments are made to the Specification, the version number of the document will be updated.

Each section provides details of the minimum requirements which must be met by prospective Registry Operators. Tenderers are free to nominate higher performance or service levels, or specify additional functionality in any or all aspects of the Specification. However this is not necessary in order to be considered to have met the technical requirements.

Tenderers must respond where they have been asked to supply additional information. Tenderers that do not have or do not intend to address a particular item should respond with ‘Not applicable’.

In a number of locations in the Specification the phrase ‘to be determined by auDA’ or similar has been used. This indicates that the particular information is currently unknown or still under development. The correct information will be inserted into the Specification when it becomes available. It is not expected that this information will impact on the Tenderers ability to respond to these requirements.

2.0 FUNCTIONAL SPECIFICATIONS

The Registry Access Protocol and the Registry Database are to be based on the Extensible Provisioning Protocol (EPP) and associated data objects that have been developed by the IETF ‘provreg’ group. EPP is now an RFC. The reference documents are now available at www.rfc-editor.org:

- RFC3730 - Extensible Provisioning Protocol (EPP)
- RFC3731 - Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC3732 - Extensible Provisioning Protocol (EPP) Host Mapping
- RFC3733 - Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC3734 - Extensible Provisioning Protocol (EPP) Transport Over TCP
- RFC3735 - Guidelines for Extending the Extensible Provisioning Protocol (EPP)

2.1 Registry Access Protocol

The purpose of the Registry Access Protocol (RAP) is to allow Registrars to perform various operations which are necessary when creating, modifying and deleting domain name registrations. The RAP provides a remote interface into the Registry Database.

Registry operators are required to implement and operate the IETF Extensible Provisioning Protocol (EPP) RFC Version 1.0, as referenced above.

Should inadequacies with the RFC protocol emerge, Registry Operators and Registrars must agree to implement the revised version of the protocol. Registry Operators must implement support for the standard protocol and provide updated Software Toolkits. A reasonable time frame for implementing and testing revisions to the protocol will to be determined by auDA in consultation with Registry Operators and Registrars.

2.1.1 EPP Software Development Toolkit

Registry Operators 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 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 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. In this case, the full Transport Layer Security (TLS) protocol [IETF RFC2246] must be utilised to ensure secure and authenticated message interchange. RFC2246 caters for a range of cryptographic algorithms and authentication schemes. Suitably strong encryption and authentication must be employed, and the actual cryptographic algorithms and authentication scheme(s) identified in the Tender and approved by auDA.

The primary mechanism for Registrar authentication must be using the EPP <creds> element. 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

A number of 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, including transaction identifiers must be logged;

(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 object identifiers 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 Tenderer is required to demonstrate how they will deliver the following; (procedures developed should be consistent with procedures currently in use by the incumbent)

(a) a full permission and condition matrix for command authorisation;

(b) an appropriate authorisation mechanism for completing a Registration <transfer> operation;

(c) the format for contact object prefixes;

(d) the format for client identifiers.

2.2 Registry Database

The Registry Database is to be based on the schema descriptions which define ‘registrar’, ‘domain’, ‘contact’ and ‘host’ objects. Initial schema descriptions can be found in the mapping documents (above).

The intended schema definitions should be supplied by the Tenderer as part of their response. Additional data items beyond those defined in the EPP ‘domain’, ‘contact’ and ‘host’ schemas should be specified to account for local policies within the .au domain. A ‘registrar’ object should also be defined.

In addition, the Tenderer will need to conform with the current set of refinements as supported by the incumbent (see Server Policy document at Appendix B). This includes such things as mandating UTF-8; mandating State and Postcode elements; mandating the number of registrant and contact objects permitted for domains; and determining the context in which certain status indications will be permitted.

The actual recording format within the Registry Database will be implementation dependent.

2.2.1 Database 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 99.5% per calendar month;

(b) **Processing time**: At least 98% of enquiries serviced within 1.5 seconds. At least 95% of create/modify/delete requests serviced within 3 seconds;

(c) **Planned outage**: limited to a maximum of 8 hours per calendar month; between 0001 and 1200 AEST Sundays. 3 days notice to be given to Registrars;

(d) **Extended outage**: limited to a maximum of 18 hours per calendar month; between 0001 and 2400 AEST Sundays. 28 days notice to be given to Registrars.

2.3 Authoritative Nameserver Service

Each Registry Operator must provide an authoritative nameserver for the domain(s) it operates. The nameservers must comply with IETF standards for the Domain Name Service (RFC1035, RFC2181 and RFC2182). Registry Operators must also commit to the implementation and operation of DNS extensions in such areas as internationalisation, security, etc. when these have been adopted by the IETF and have achieved a satisfactory level of community support.

2.3.1 Nameserver Reliability

In compliance with the relevant RFCs, the authoritative nameserver service must be implemented using a number of nameservers to maintain high levels of availability. The Registry Operator must operate and maintain a minimum of one primary nameserver within Australia, and two secondary nameservers, one located in a different state of Australia from the primary server and one located in the USA or Europe. In addition the Registry Operator must ensure that there are an additional minimum of five secondary name servers provided by external parties pursuant to agreements with the Registry Operator. The Registry Operator may cooperate with other Registry Operators, carriers, or ISPs to host secondary 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.

The Registry Operator should note that geographical and carrier dispersion of nameservers is considered essential for reliability (see RFC2182).

2.3.2 Zone File Maintenance

The Registry Operators will use the Registry Database as the authoritative source for creation of zone file information. Registry Database updates must be reflected in the zone file(s) within five (5) minutes of completion.

2.3.3 Provision of Zone Files to auDA and Zone Transfers

(a) a copy of the zone file(s) must be made available to auDA on request;

(b) the Registry Operator must ensure that all DNS software used is capable of performing TSIG signed zone transfers. All zone transfers, full or incremental, between primary and secondary nameservers are to be TSIG signed. The TSIG key should be rotated every six months at a minimum. If dynamic updates are to be used for updating the primary nameserver they are not to be sent to the live primary name server but rather a system of a ‘hidden’ primary that is only accessible to the Registry Operator should be used. All live nameservers must be configured to reject dynamic update requests. All dynamic updating should also employ TSIG based signing.

2.3.4 DNS Service Performance and Availability

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

(a) **Overall Service availability**: 100% per calendar month;

(b) **Service Availability Per Registry Operator nameserver:** At least 99.95% per calendar month;

(c) **Processing time - nameserver resolution**: At least 95% to be processed in less than 1.5 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 nameserver Planned outages**: Nil.

2.4 WHOIS Service

At auDA's discretion for the purposes of enabling auDA to provide a central public WHOIS service, the Registry Operator must provide auDA with a full data set containing the objects associated with each 2LD 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 0 and a WHOIS document type definition that will be developed by auDA in parallel with the Tender.

2.4.1 Registry-provided Public WHOIS

The Registry Operator must provide a reliable public WHOIS service for the 2LD(s) under its management. The WHOIS service must be fully compliant with RFC954 and must conform to auDA's stated policies with regard to each 2LD. In particular, auDA will specify:

(c) the information which may be provided as a result of a WHOIS enquiry. This may vary between 2LDs;

(d) 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;

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

Registry Operators should develop their WHOIS service in such a way that these factors are taken into consideration.

2.4.2 WHOIS Data Set

The following information is to be potentially available from the Registry Database as a result of a WHOIS enquiry. Fields within this set may be restricted by auDA policy for some 2LDs:

(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, e-mail address, voice telephone number, and (where available) fax number of the domain name Registrant;

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

(h) the name, postal address, e-mail 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.) Registry Operators must be able to demonstrate that integrity will be maintained between the WHOIS files (if any) and the Registry Database.

2.2.3 WHOIS Enquiries

The public WHOIS service to be provided by Registry Operators is to be oriented towards providing information about specific domain names or constrained sets of domain names. Bulk access to WHOIS information will be managed by auDA.

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) a string of five or more contiguous characters to be matched at the beginning of the domain;

(c) the name of the Registrant;

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

Where a key results in multiple matches, a short list containing the matched items (domain names or Registrant names) is to be returned to the user. Only when a user has identified a single domain name or a single Registrant is the full WHOIS information to be returned.

Repeated public WHOIS enquiries from individual hosts are to be limited to a specific number in a given time period (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.

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

```
Domain Name: auda.org.au
Last Modified: Never Updated
Registrar ID: R00001-AR
Registrar Name: auDA
Status: OK

Registrant: .au Domain Administration Ltd
Registrant ID: OTHER 079 009 340
Registrant ROID: C0059419-AR
Registrant Contact Name: Chris Disspain
Registrant Email: ceo@auda.org.au
```

```
Tech ID: C0059421-AR
Tech Name: Chris Disspain
Tech Email: ceo@auda.org.au

Name Server: warrane.connect.com.au
Name Server IP: 192.189.54.33
Name Server: yarrina.connect.com.au
Name Server IP: 192.189.54.17
Name Server: ns1.iinet.net.au
Name Server IP: 203.14.168.3
Name Server: ns2.iinet.net.au
Name Server IP: 203.59.24.3
Name Server: ns1.auda.org.au
Name Server IP: 203.202.88.210
```

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 99.5% per calendar month;

(b) **Processing time**: At least 98% of enquiries serviced within 1.5 seconds;

(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 8 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 18 hours per calendar month; 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 100 in any 24-hour period. Blacklist period: 24 hours.

2.5 Legacy Data

Registry Operators 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 CSV format. 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.

2.6 Functional Specification Response

Tenderers must respond to the Functional Specification by indicating how they intend to meet the minimum requirements of the Specification. In particular, Tenderers should indicate how they intend to:

(a) implement the Registry Database as per the Specification, including providing details of the proposed hardware and network configuration;

(b) implement the Registry Access Protocol as per the Specification;

(c) provide a Public WHOIS service as per the Specification, including providing details of the proposed hardware and network configuration;

(d) provide an authoritative nameserver service as per the Specification, including providing details of the proposed hardware and network configuration;

(e) provide details on how the namesever service and/or the WHOIS service will remain in sync with the registry database and in the timeframes as set out in the specifications

(f) meet the Performance Specifications and Service Levels for the Registry Database, WHOIS and nameserver services as set out in the Specification.

3.0 SECURITY ARCHITECTURE

This section of the tender specification relates to security aspects of the proposed 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 Tender that proposed Registry Systems be developed in accordance with the following Australian Security Standards:

(a) Information Technology Code of practice for information security management (AS/NZS ISO/IEC 17799:2001, previously AS/NZS 4444.1:1999);

(b) Information Security Management, Part 2: Specification for information security management systems (AS/NZS 7799.2:2000, previously AS/NZS 4444.2:2000).

The above security standards are generic and not all areas addressed are relevant to the Tender. Tenderers should aim to provide a secure computing environment for reliable and continuous operation of the proposed Registry System. Data integrity is to be emphasized. Tenderers 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 run-time environments. It is recognised that Tenderers have a wide range of options when considering solutions for the proposed Registry System. Solutions may range from a single server to a cluster of servers for all Registries. Servers may be based on a variety of platforms (e.g. Unix, NT etc.). Tenderers may propose new purpose built systems, or may elect to incorporate the Registry System into existing environments. Application software may be entirely web based or may function as part web based and part client/server via a local area network.

With this variety of options, Tenderers should respond to security issues which are appropriate to their solutions. Where an item does not apply, Tenderers should respond with 'Not applicable'.

3.1 Security Policy

A clear statement is required from senior management of the Tenderer's commitment to and support of information security.

If an existing Information Security Policy Document is available, it should be included in the supporting documentation accompanying the Tender.

Details are also required of the Tenderer's on-going review of the security policy in response to changes affecting risk assessment, security incidents and technological change.

3.2 Security

This section relates to the management of information security within an organisation. Tenderers are requested to provide details of the management structure established to implement an information security policy within the organisation and the involvement of staff and users throughout the organisation. Commitment to the information security policy at a senior management level is considered essential.

Responses are required to the following items:

(a) State the name, ranking and other responsibilities of the Information Security Manager within the organisation;

(b) State the policy for allocating responsibility for information assets within the organisation and the authorisation process for information processing facilities;

(c) State the level of reliance the organisation places on external information security advice and list the level of use of external security advisors over the past two years;

(d) List membership of security groups and industry forums;

(e) Provide details of the most recent security audit undertaken by the organisation (internal or external);

(f) Provide details of third party contracts which will impact on the current Tender;

(g) Provide details of outsourcing arrangements which may impact on the Tender.

(h) Provide details of any industry association events or training that staff within the organisation have attended that is specific to the domain name industry.

3.3 Asset Classification and Control

This section relates to the identification and protection of information assets within the proposed Registry System. Individuals within the Tenderer's organisation should be assigned responsibility for information assets and be accountable for those assets and their use.

In this Tender, information assets include databases, data files, system documentation, user manuals, training material, operating instructions and procedures, archived material, application and system software, development tools and utilities. Physical assets include computers, peripherals, communications equipment, magnetic media, other technical equipment, furniture and accommodation. Service assets include computer and other equipment maintenance, and general utilities, e.g. heating, lighting, power, air-conditioning.

Responses are required to the following items:

(a) Provide an itemised list of information assets in the proposed Registry System;

(b) Describe the facilities within the organisation used to maintain an appropriate inventory of information assets;

(c) Provide details of the classification of information within the proposed Registry System, and how this will be used to protect data from illegal use or copying;

(d) Describe the handling procedures for the destruction of information in each classification type.

3.4 Personnel Security

This section deals with security aspects of staffing within an organisation which are specifically designed to reduce the risks of human error, theft, fraud and misuse of facilities and information. Security responsibilities apply to all staff within an organisation, permanent, part-time, contract and service staff.

Responses are required to the following items:

(a) Provide examples of job specifications within the organisation detailing the information security policy as applied to individual positions;

(b) Describe the validation checks performed during the staff selection process to ensure an applicant's details (academic, professional, employment history) are complete and accurate;

(c) Describe or provide examples of confidentially and/or non-disclosure agreements employees are required to sign as part of the terms and conditions of employment;

(d) Describe the levels of training to be provided to staff and users of the proposed Registry System in the area of information security;

(e) Describe the procedures to be incorporated into the proposed Registry System for reporting, registering, investigating and resolving security incidents;

(f) Describe procedures for reporting software malfunctions in the proposed Registry System.

3.5 Physical and Environmental Security

This section relates to physical aspects of security, namely, secure areas to house information systems, protection of equipment, provision of a secure power supply and cabling infrastructure, and a clear desk policy to prevent unauthorised access to information.

3.5.1 Secure Area

The proposed Registry System must be located within Australia in a commercial carrier-class, secure data centre with adequate protection from unauthorised access, damage to equipment and interruption of the Registry service. It is a requirement of the Tender that the site be equipped with 24-hour manned security systems. If shared with other organisations (eg tele-housing facilities) the registry system must be housed in a fully enclosed, separated, designated section that is only accessible to authorised personnel.

Responses are required to the following items:

(a) State in which city or cities the proposed Registry System will be located;

(b) Describe the physical environment which will be used to house the Registry System and staff required to operate it;

(c) Describe security features of the proposed environment and methods for controlling access to the facility;

(d) Provide a risk assessment for the site at which the required 24-hour manned security systems will be located;

(e) Describe security access controls to restrict access to the site to authorised personnel only;

(f) Provide details of fire protection facilities incorporated into the security system;

(g) Describe procedures for processing restricted access for third party personnel (e.g. maintenance engineers).

3.5.2 Equipment Security

Equipment within the secure area should be protected to prevent loss, damage or disruption of the Registry service.

Responses are required to the following items:

(a) Provide a layout diagram of equipment associated with the proposed Registry System showing security boundaries;

(b) Provide the maintenance schedule for equipment in the proposed Registry and details of procedures to be followed when equipment is shipped off-site for maintenance;

(c) Describe controls to minimize the risks of theft, fire, explosives, smoke, water damage, dust, vibration, chemical effects, electricity supply interference, electromagnetic radiation;

(d) Describe measures taken to ensure that the site has a reliable power supply, including details of uninterruptible power supplies and back-up power generators.

3.5.3 Cabling Security

It is a requirement of this Tender that power and telecommunication lines be secured from interception and damage.

Responses are required to the following items:

(a) Describe the method of access of power and telecommunication cables;

(b) Provide network wiring diagrams showing all network connections in the proposed Registry System;

(c) Describe procedures to be adopted to ensure that unauthorised devices are not attached to cables.

3.5.4 Disposal of Equipment

Disposal or re-use of equipment from the Registry System should be subjected to special checks to ensure that all information has been erased from the equipment.

Responses are required to the following items:

(a) Describe the procedures to be followed in the disposal or re-use of equipment from the Registry System;

(b) Describe the methods to be adopted for erasing information from magnetic storage devices;

(c) Describe procedures for destroying damaged storage devices to ensure no data can be copied from the devices.

3.6 Communications and Operational Management

This section considers factors affecting the correct and secure operation of the proposed Registry System.

3.6.1 Operational Procedures

All operational procedures must be fully documented with any changes subjected to formal management review and approval. Operational procedures are required for all information processing tasks, error handling, interaction with maintenance and support specialists, system input and output requests, and restart and recovery procedures in the event of system failure.

Responses are required to the following items:

(a) Provide examples of operational procedures developed by your organisation;

(b) Describe systems developed for operational change control in the above examples;

(c) Describe systems developed for recording and managing incidents (system failures, loss of service, etc.) which occur in the above examples;

(d) Describe controls implemented in the above examples to minimize the effect of accidental or deliberate system misuse;

(e) Describe controls which will be employed for managing external contractors and/or services.

3.6.2 System Planning and Acceptance

This section deals with the issues of system and capacity planning prior to the development of a system and acceptance testing undertaken prior to commissioning a system.

Responses are required to the following items:

(a) Describe your organisation's experience with system and capacity planning with a scope similar to that of the proposed Registry System;

(b) Describe your organisation's experience with acceptance testing in the following areas:

(i) Performance and computer capacity;

(ii) Error recovery, re-start and contingency planning;

(iii) Testing of routine operational procedures;

(iv) Testing of security controls;

(v) Testing of manual procedures;

(vi) Testing of business continuity plans;

(vii) Testing user training.

3.6.3 Protection against Malicious Software

Computers systems are vulnerable to the introduction of malicious software, e.g. computer viruses, logic bombs. Facilities are required to prevent and detect such occurrences.

Responses are required to the following items:

(a) Describe software and procedures to be incorporated in the proposed Registry System to provide protection against malicious software;

(b) Describe controls to be used which prohibit the use of unauthorised software;

(c) Describe procedures for reviewing information and software on computers running the proposed Registry System;

(d) Describe facilities for checking electronic mail or Internet downloads for viruses.

3.6.4 Housekeeping

This section deals with the routine housekeeping activities required to maintain a well organised computer system.

Responses are required to the following items:

(a) Describe procedures for performing back-up and recovery operations of the proposed Registry System;

(b) Describe testing procedures to ensure the back-up and recovery procedures are performing correctly;

(c) Describe procedures for checking that all essential data is included in the back-up and recovery process;

(d) Describe the information recorded in the fault logs maintained in the proposed Registry System;

(e) Describe procedures for reviewing the fault logs and recording the resolution of fault conditions.

3.6.5 Network Management

This section relates to security management of networks and information passing through public networks.

If applicable responses are required to the following items:

(a) Describe your organisation’s approach to network operations in the proposed Registry System;

(b) Describe procedures and controls to be incorporated in the proposed Registry System to maintain the availability of network services and connected computers;

(c) Describe facilities designed to ensure the security of data in networks and to protect connected services from unauthorised users.

3.6.6 Media Handling and Security

This section deals with the protection of documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorised access.

Responses are required to the following items:

(a) Describe procedures and controls in the proposed Registry System to ensure that data is totally erased from computer media no longer required;

(b) Describe procedures and controls in the proposed Registry System to ensure that the copying of system data to removable media is controlled and appropriate audit trails maintained;

(c) Provide details of operational procedures to ensure that information copied to secondary media is stored securely;

(d) Provide details of operational procedures to ensure printed information is handled and disposed of securely;

(e) Describe procedures and controls in the proposed Registry System to ensure that all communication facilities (e.g. e-mail, voice mail, post and fax) are subject to audit;

(f) Describe procedures and controls in the proposed Registry System to ensure that system documentation is secure and accessed only by authorised users.

3.6.7 Exchanges of Information and Software

This section deals with the exchange of information or software between organisations. Such exchange arrangements are subject to formal agreements which define what information is to be transferred and the level of security and controls required in the transfer

Responses are required to the following items:

(a) Describe the level of authentication and authorisation for information exchanges in the proposed Registry System; these should include but not limited to:

   a. Validating registrar digital certificate
   b. Validating registrar source IP address
   c. Validating EPP credentials
   d. Cross referencing these three details with each other

(b) Provide details of the level of encryption of information exchanges in the proposed Registry System.

3.7 Access Control

This section relates to the control of access to information in the proposed Registry System.

3.7.1 Access Control Policy

The proposed Registry System requires relatively high levels of controls over the ability of individuals to access or change information in the system. In general, staff performing system and software development tasks will have different access rights from staff controlling the operation of the production system. It is envisaged that the development environment will be different from the production environment. These may take the form of different directories on one computer, or different computer systems. For example, web based software may be uploaded from the development environment to the production environment.

Responses are required to the following items:

(a) Describe the software development and support environment for the proposed Registry System;

(b) Describe the production environment for the proposed Registry System;

(c) Describe the procedures and controls for assigning access rights to staff (note that a hard rule based system is preferred in which access to a task is forbidden unless specifically assigned).

3.7.2 User Access Management

This section aims at preventing unauthorised access to the proposed Registry System. A formal user registration system is required which specifies a user’s access rights to the system.

Responses are required to the following items:

(a) Describe the procedures and controls in the proposed Registry System for registering users in order to access system facilities;

(b) Describe the mechanism which controls user access to various classes of facilities in the Registry System;

(c) Describe procedures and controls for the assignment of user access privileges to various system facilities, e.g. operating system, databases, application software modules;

(d) Describe procedures and controls for assigning and managing user passwords in the proposed Registry System;

(e) Describe other technologies which are recommended for incorporation in the proposed Registry System (e.g. finger prints, smart cards, etc).

3.7.3 User Responsibilities

This section defines the responsibilities of users accessing the proposed Registry System. The co-operation of authorised users is essential for effective security.

Responses are required to the following items:

(a) Describe procedures and controls in the proposed Registry System to allow users to change passwords (a minimum of six characters is recommended);

(b) Describe procedures and controls in the proposed Registry System for terminating user sessions after a workstation has been inactive for a set elapsed time (e.g. 2 minutes).

3.7.4 Network Access Control

This section relates to the protection of internal and external network services. The proposed Registry System is fundamental to the day-to-day operation of the Internet in Australia and its design must incorporate high levels of internal and external network security to ensure that the Internet operates correctly.

Responses are required to the following items:

(a) The proposed Registry System will be accessed by local users (staff of the successful Tenderer) and via the Internet (Registry Access Protocol, WHOIS and nameserver requests). Provide details of appropriate network controls for both areas;

(b) Provide details of facilities for user authentication for external connections in the proposed Registry System;

(c) Provide details of facilities for network connection control in the proposed Registry System, restricting access to electronic mail, file transfers and interactive access;

(d) Provide details of facilities for restricting access to normal Internet browser services in the proposed Registry System.

3.7.5 Operating System Access Control

This section relates to security facilities at the operating system level used to restrict access to computer and operating system resources. Facilities are required to identify users when they log-in to the system, including an identification of remote computers or terminals being used. Users are authenticated by passwords or other mechanisms and appropriate audit logs are used to record both successful and failed log-ins.

Responses are required to the following items:

(a) Describe facilities to be incorporated in the proposed Registry System to identify user computers or terminals during log-in procedures;

(b) Describe the log-in procedure for users at computers or terminals attached to the proposed Registry System;

(c) Describe the methods adopted for user identification and authentication in the proposed Registry System;

(d) Describe the password management system to be incorporated in the proposed Registry System;

(e) Describe facilities in the proposed Registry System for logging off users who have been in-active for a set period of time (e.g. 2-5 minutes).

3.7.6 Application Access Control

This section relates to the prevention of unauthorised access to information in the proposed Registry System. Security facilities are used to restrict access to modules within the application software.

Responses are required to the following items:

(a) Provide details of facilities in the proposed Registry System which restrict user access to system documentation according to their access requirements;

(b) Provide details of facilities in the proposed Registry System which controls the access rights of users, e.g. read, write, delete, execute.

3.7.7 Monitoring System Access and Use

The proposed Registry System should be monitored to detect unauthorised activities. Audit logs recording exceptions and other security sensitive events should be generated and retained for agreed periods to assist in future investigations and access-control monitoring.

Responses are required to the following items:

(a) Describe facilities in the proposed Registry System for event logging and provide details of the information contained in event logs;

(b) Provide details of facilities in the proposed Registry System for monitoring the use of system modules, e.g. authorising user log-ins, use of supervisor facilities, system start/stop, unauthorised access attempts;

(c) Describe facilities to be incorporated in the proposed Registry System for analysing or searching event log information, e.g. log-ins by user “X”;

(d) Describe facilities in the proposed Registry System for clock synchronization, e.g. to Universal Coordinated Time or local time.

3.7.8 Mobile Computing and Teleworking

This section relates to the use of mobile computing and teleworking facilities with the proposed Registry System. This section is particularly relevant to systems which are completely web based. Organisations should provide details of any use to be made of mobile equipment or teleworking in the proposed Registry System, and special security controls for users of these devices.

Responses are required to the following items:

(a) Describe facilities for access controls, cryptographic methods, back-ups and virus protection for mobile computer users and teleworkers accessing the proposed Registry System;

(b) Provide details of the environment in which mobile computers and teleworking equipment will be operating when users are interacting with the proposed Registry System, for either or both development or production;

(c) Describe facilities to prevent unauthorised access the proposed Registry System by illegal users of mobile computers or teleworking equipment;

(d) Describe the type of work to be undertaken on the proposed Registry System by mobile computer users or teleworkers.

3.8 System Development and Maintenance

This section defines the security levels required in the development and maintenance of the proposed Registry System.

3.8.1 Security Requirements of Systems

The proposed Registry System is fundamental to the day-to-day operation of the Internet in Australia and its design must incorporate high levels of security to ensure that the system operates correctly.

3.8.2 Security in Application Systems

Individual program modules within the proposed Registry System must be designed to prevent loss, modification or misuse of information. Appropriate controls, audit trails and activity logs must be incorporated in the system, and facilities included to validate input data, internal processing and output data.

Responses are required to the following items:

(a) Describe the level of input data validation to be incorporated in the proposed Registry System;

(b) Describe the use to be made of message authentication techniques in the proposed Registry System;

(c) Describe the level of output data validation to be incorporated in the proposed Registry System.

3.8.3 Cryptographic Controls

Cryptographic controls protect the confidentially, authenticity and integrity of information. In the proposed Registry System, cryptographic controls are required when transferring Registry data to other sites but are not necessarily required for in-house database operations.

Responses are required to the following items:

(a) Describe the cryptographic controls to be used with the proposed Registry System;

(b) Describe procedures and controls for managing cryptographic controls and protecting cryptographic keys;

(c) Describe facilities to be provided in the proposed Registry System for registering and processing digital signatures.

3.8.4 Security of System Files

This section relates to the maintenance of a secure operational environment by controlling access to system software and information files.

Responses are required to the following items:

(a) Describe procedures and controls for updating operational program libraries upon receipt of appropriate management authorisation;

(b) Describe procedures and controls for ensuring that software is not implemented on an operational system without appropriate testing and user acceptance;

(c) Describe the contents of the audit log maintained for recording changes to the operating environment;

(d) Describe procedures and controls for retaining old versions of software modules for contingency purposes;

(e) Describe procedures and controls for generating or maintaining test data used for testing software changes;

(f) Describe procedures and controls for maintaining program source libraries.

3.8.5 Security in Development and Support Processes

This section relates to the maintenance of the security of application software and information in the proposed Registry System. Project and support environments should be strictly controlled.

Responses are required to the following items:

(a) Describe the change control procedures that will apply during design, implementation and support of the proposed Registry System;

(b) Describe the system of authorisation or approval of changes to the proposed Registry System;

(c) Describe the level of integration between the change control procedures and corresponding changes to system documentation;

(d) Describe the version control system for software releases in the proposed Registry System;

(e) Describe the information contained in the audit trail of changes that are introduced into the proposed Registry System;

(f) Describe the procedure for ensuring that changes to the proposed Registry System are introduced at the correct time without disturbing the normal operation of the Registry;

(g) Describe the environment for testing changes to the Registry System prior to their release to the production environment;

(h) Describe the procedures established to test the valid operation of developed application software in a changed operating system environment;

(i) Describe procedures and controls to identify covert channels, trojan code or logic bombs included in application software by careless or disgruntled employees;

(j) Describe procedures and controls for testing and accepting software modules developed by external organisations.

3.9 Business Continuity Management

This section deals with the security aspects of business continuity management which itself is discussed in detail in Section 4 of this document. Business continuity management involves the analysis of the consequences of disasters, security failures and loss of service, and the formulation of plans to allow business activities to be restored within an accepted time frame.

Responses are required to the following items:

(a) Provide details of your organisation's experience in developing and implementing business continuity plans;

(b) State how many existing sites are running with established business continuity plans.

3.10 Compliance

Tenderers should note that the design, operation, use and management of the proposed Registry System will be subject to statutory, regulatory and contractual security requirements which may vary from country to country, particularly for information created in one country that is transmitted to another country.

Responses in the form of 'accept' or 'do not accept' are required to the following items:

(a) The successful Tenderer will be required to document all statutory and regulatory requirements of the proposed Registry System, together with specific controls and individual responsibilities to meet these requirements;

(b) The successful Tenderer will be licensed to provide Registry services to auDA. Intellectual property rights of the information contained in the Registry will be vested in auDA;

(c) The successful Tenderer must ensure that appropriate procedures are implemented to ensure that copyright is not infringed;

(d) The successful Tenderer will retain copyright in computer software developed specifically for the proposed Registry System;

(e) The successful Tenderer will be required to maintain a list of proprietary software used in the proposed Registry System and perform any necessary checks and audits to ensure that only authorised software is used in the Registry;

(f) Tenderers should include a copy of their software copyright compliance policy as part of the tender documentation.

4.0 BUSINESS CONTINUITY PLAN

This section of the tender specification relates to the on-going operation of the proposed 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 successful Tenderer will be required to develop and implement a full business continuity plan for the proposed 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 proposed 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 proposed Registry System are considered to be at two levels: production and maintenance. The production items include the real-time components of the proposed 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 proposed Registry System by the end of the next day – e.g. 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 proposed 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 (e.g. bombs, sabotage, viruses, activation of sprinkler systems) or due to industrial disputes (e.g. power strikes). While the variations are numerous, disasters can be categorized as loss of information, loss of access or loss of personnel.

The aim of business continuity planning is to minimize 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 minimize 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 proposed 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 proposed 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 proposed Registry System, in particular:

- Loss of power (e.g. failure or prolonged strike);
- Loss of environmental controls (e.g. air-conditioning);
- Breaches of security (e.g. physical, electronic – virus or hack attack);
- Loss of internal/external communications;
- System failure (e.g. computer or disk malfunction);
- Internet communication failure or interruption;
- Degraded performance;
- File corruption or lost files;
- Unreliable or incorrect results.

(iv) Determination of critical resource requirements for disaster recovery;

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

(vi) Cost/benefit analysis for the various recovery alternatives;

(vii) Staffing requirements for the various recovery alternatives;

(viii) 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 (e.g. 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 proposed 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, e.g. 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 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 periodically 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.

Using the above as a guide, Tenderers should respond with an overview of a business continuity plan appropriate for their proposed Registry System, specifying very clearly the level of disaster recovery incorporated into the plan. Tenderers may also propose alternate business continuity plans.

5.0 DATA ESCROW REQUIREMENTS

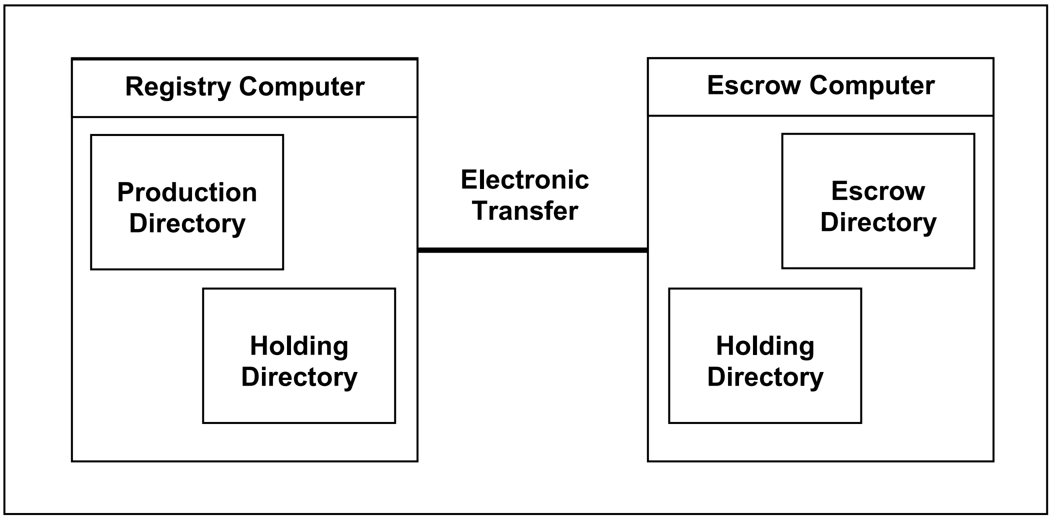
This section of the specification defines the data escrow requirements of the proposed Registry System. Data escrow requires the transfer of data from the proposed Registry System to auDA, and to be accessible by auDA under strictly limited circumstances and ensuring full protection of copyright and intellectual property.

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 proposed 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 purpose of the escrow process is to allow auDA to replicate the original Registry environment if necessary. 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.

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 proposed Registry System.

The Registry Operator is to be responsible for the maintenance of paper records (e.g. 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 is obliged to establish a new Registry.

At Registry rollover, there must be a seamless transition between an incumbent Registry Operator and the designate Registry Operator. The Registry Operator is required to co-operate 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 format and provided with appropriate scripts to facilitate the loading of this data in to an Oracle database or as Oracle native dump.

5.4 Data Escrow Proposal

Using the above as a guide, Tenderers should respond with an overview of a data escrow plan appropriate for their proposed Registry.

Tenderers will be required to develop or supply the software required for the data escrow process. Tenderers must also develop or supply any special software that is required in the Escrow Computer during data escrow operations. The data escrow facilities should allow transfer of files to and from the data escrow computer.

6.0 DOMAIN NAME EXPIRY AND DELETION

This section of the tender specification relates to the expiry and deletion of domain names in the proposed 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. 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 Tender 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 will be defined by auDA at the time of contract.

It is also a requirement of the Tender that the proposed 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 proposed Registry.

A dispute resolution process has been established by auDA to determine ownership of domain names which are shown to be held in bad faith. Registry Operators 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.

Tenderers are requested to acknowledge the above and describe the facilities to be incorporated in the proposed Registry to control these undesirable practices.

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 proposed Registry, or as noted made available to auDA on request. The monthly report must be presented to auDA within the first seven days of the following month. The following information is required form 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 .au Domain Names currently in the Registry System at the end of the given month.

vi) Report the total number of .au Domain Names, by zone currently in the Registry System at the end of the given month.

vii) 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 the facility to auDA to generate reports on the number of blacklisted hosts.

iv) Report on suspicious WHOIS activity as required.

(c) Service Level Performance

i) Provide a report stating the actual service availability performance for the Registry System, the Name Servers and the WHOIS service.

ii) Provide the average processing time for each EPP transaction type for the Registry System.

iii) Provide the average update frequency for the Name Servers

iv) Provide the planned outage time for the Registry System and WhoIs service

v) Provide the extended planned outage time for the Registry System and WhoIs service

vi) Provide the planned outage notification time for the Registry System and WhoIs service

vii) Provide the facility to 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

(d) Database

i) Provide the ability for auDA to generate a report detailing the number of Database transactions for a given period.

ii) Provide the ability for auDA to generate a report detailing the average daily transaction rate for a given month.

iii) Provide the ability for auDA to generate a report detailing the Registry Database size.

(e) 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 Name Servers for a given month for Domains. This will include all Name Servers operated by the Registry.

(f) Name Severs

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

- Successful Queries
- Rreferrals
- Non existent Domains (nxdomain)
- Non existent record set (nxrrset)
- Failures
- Look-ups resulting in recursion

(g) Average Registry Response Time

Provide a report that details the average response times recorded in the Registry System for:

- WhoIs
- Name Servers
- Transform
- Queries

(h) Hardware, Software and Network Security Issues

Should any hardware, software, network or security issues be encountered during the month the Registry Operator will provide auDA with a report of the steps taken to resolve the issues and ensure that the issues do not reoccur.

In circumstances where a security breach occurs, auDA will be provided with a report detailing the nature, extent of the breach and action taken, at the earliest available opportunity.

(i) 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.

8.0 REGISTRAR SUPPORT SERVICES

This section of the specification describes the Registrar support services to be provided as part of the proposed 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) E-mail 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:

   i. Technical information and downloads
   ii. Accreditation information
   iii. Accounts management
   iv. Statistics

(f) Provision of a test and evaluation environment to enable the testing of new software;

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

Tenderers are requested to comment on the above and describe any additional Registrar support services to be incorporated in the proposed service.

APPENDIX A: DEFINITION OF TERMS

Service Availability. Service availability is defined as the time, in minutes, that the Registry is responding to its users. Service is unavailable 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. Downtime to allow for regular maintenance.

Planned Outage Duration. The 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. In some cases such as software upgrades and platform replacements an extended maintenance timeframe is required.

Extended Planned Outage Duration. The 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. Processing Time refers to 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. This is delay 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. Cross-Network Nameserver Performance is the measured round-trip time and packet loss from arbitrary locations on the Internet to the Registry.

APPENDIX B: SERVER POLICY DOCUMENT

Server Policy

AusRegistry Pty Ltd

Last Update:

08/03/2005

Table of Contents

1 Introduction 1
2 General Protocol Restrictions 2
2.1 Language 2
2.2 Passwords 2
2.3 AuthInfo 2
2.4 Authentication 2
2.5 Timeouts 2
2.6 Invalid Requests 3
2.7 Maximum Connections 3
3 Domains: 4
3.1 Creation 4
3.2 Period 4
3.3 Reserved Domains 4
3.4 Minimum Contact objects required 5
3.5 Minimum Name Servers 5
3.6 Extension Policy 5
3.7 Correction to .au only EPP Extensions 5
3.8 Legacy MX Only Domains Policy 5
4 Host Policy 6
4.1 Valid Hosts 6
4.1.1 Hosts for Zones Hosted by this Registry 6
4.1.2 TLD.CC Host Create/Update Permission Tables 6
4.1.3 State Level .gov and .edu.au Host Create Permission Tables 7
5 Contacts: 8
6 Transfer Policy 9
6.1 clientTransferProhibited Status 9
6.2 Contacts after a Transfer of Domain 9
6.3 Registrant Transfers 9
6.4 Transfers During or After Expiry Date. 9
7 Renew Policy 10
8 Delete Policy 11
8.1 Domain deleted within three days of creation 11
8.2 Domain deleted after three days of creation 11
8.3 Domain Expires (See Renew Policy) 11
8.4 Disputed Domain Delete 11
9 Polling Messages 12
9.1 Transfer 12
9.2 Balance 12
10 Daily Statistic Messages Sent To Registrar 13
10.1 Domains Transferred In: 13
10.2 Transfers Cancelled: 13
10.3 Domains Transferred Out: 13
10.4 Domains Created: 13
10.5 Domains Cancelled: 13

10.6 Domains Expired: 13
10.7 Domains Deleted: 13
10.8 Domains Renewed: 13
11 WhoIs 14
11.1 Policy 14

Table of Tables

Table 1 6
Table 2 6
Table 3 7
Table 4 7

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 ccTLD's that we manage and on AusRegistry's own recommendations.

GENERAL PROTOCOL RESTRICTIONS

Language

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

Passwords

Login 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
- Is NOT based on a dictionary word.

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); and
> c) no dictionary words."

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

Authentication

All the following MUST be met for successful authentication:

- Source IP address MUST be a nominated IP
- 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
- MUST match the registrar name in the common name of the certificate being presented.

This means:

- Your Certificate is only valid from your nominated IP addresses
- Your Credentials are only valid from your nominated IP addresses
- No-one else can use your certificate and credentials should they get hold of them, unless they are able to use your IP addresses 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.

Invalid Requests

The AusRegistry EPP server will close the socket if it receives a datagram header indicating that the EPP packet (command) contains more than 5000 characters. This would usually indicate an invalid request.

Maximum Connections

Registrars are limited to a maximum of twenty connections at one time to the EPP system.

DOMAINS:

Creation

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

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

Access restrictions prohibit registrars from actually registering certain domains. They will be rejected and give out a parameter value policy error. Special rules apply for the other ccTLD's in our registry:

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). 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. No domain will have its expiry date extended beyond the specified time frame of the date of renewal or creation.

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 appropriate zone file. Any time an update to a domain is done that results in it having less than the required number of name servers, the domain will be removed from the zone. The exception is when a domain has expired. As a domain in pendingDelete is automatically removed from the DNS, no updates to the hosting records will affect that status.

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 www.auda.org.au for more information regarding the policy.

Correction to .au only EPP Extensions

To make any corrections to registrant details, the Admin interface has a Modify Registrant option under the Domains menu. Fill in the appropriate details and submit the change request, it will be placed in a queue and manually processed.

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 2LD 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. We are not responsible for any outages due to NS and MX records not set up at the client end.

HOST POLICY

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 Hosted by this Registry

- 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.
- Only sponsors of parent domains can update hosts or create child host records with IP addresses.

TLD.CC Host Create/Update Permission Tables

Table 1

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

Table 2

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

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

State Level .gov and .edu.au Host Create Permission Tables

Table 3

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

Table 4

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

Where state can be: .act, .nsw, .nt, .qld, .sa, .tas, .vic or .wa.
Where 2LD can be: .edu or .gov.

CONTACTS:

- Unused contacts should be flushed from the database periodically

TRANSFER POLICY

clientTransferProhibited Status

auDA policy prohibits the use of the clientTransferProhibited status on a domain. 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

If a contact linked with a transferred domain is not linked with any other domain sponsored by any other registrar other than the gaining registrar, then the contact will be transferred across automatically and the gaining registrar of the transferred domain will also sponsor the contacts.

If a contact linked with a transferred domain is linked with any other domain sponsored by any other registrar other than the gaining registrar, then the contact will not be transferred across to the gaining registrar of the transferred domain.

With the second instance, the gaining registrar of the transferred domain has the following options:

- Request a transfer of contact from the current sponsoring registrar to you. This is done in the same way that domain transfers are done. You 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. A reminder that 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 you will then be the sponsoring registrar of the contact and 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 you cannot modify.

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

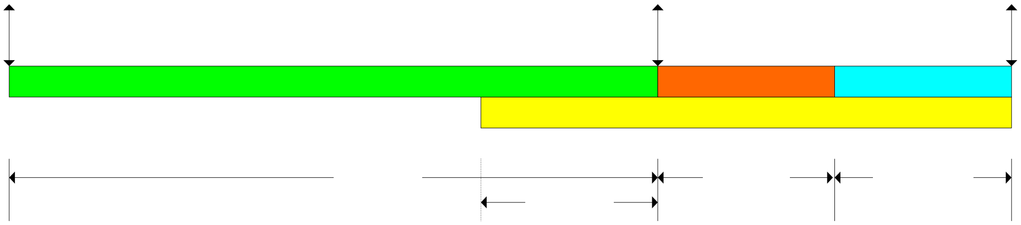
Registrant Transfers

To transfer a domain to a new registrant the Modify Registrant option under the Domains menu will allow you to submit a change request. Fill in the appropriate details and submit them. The change request will be manually accepted from our management interface when we check the queue. 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.

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. If a domain has already expired at the time a transfer request is applied to it, it will be removed from the DNS and the expiry process will be enacted.

RENEW POLICY



- At 00:00:00UTC, (10:00:00AEST / 11:00AEST Daylight Saving) the AusRegistry database runs a job once a day that sets the status of all expiring domains to ‘Pending Delete’. This job takes about ten minutes to run.
- DNS information is taken away once the domain expires.
- Domain renewals exactly add two years to the expiry date.
- Domain renewals can happen within 90 days before the expiry day, or 14 days after, however, domain renewals cannot happen while the database is running the job that sets the status of all expiring domains to ‘Pending Delete’.
- After the 14 days is up, a randomly chosen number between 0 and 7 days is added to the actual deletion date.
- Renewals are non-refundable transactions.

Begin
Date

DELETE POLICY

Domain deleted within three days of creation

- No pending delete.
- Instant drop from DNS
- Refunded creation fee
- Irreversible

Domain deleted after three days of creation

- Pending delete for three days.
- Instant drop from DNS
- No refund.
- Can be manually undeleted (via an email to Registrar Support).

Domain Expires (See Renew Policy)

- Pending delete for 14 days + random 0-7 days
- Instant drop from DNS upon expiry
- Can be renewed or transferred until deleted (no longer provisioned)

Disputed Domain Delete

- Pending delete for 14-21 days
- Instant drop from DNS
- Can be manually undeleted (via an email to Registrar Support)

POLLING MESSAGES

Transfer

“Registrar” <registrar roid> “has “

“approved”
“cancelled”
“rejected”
“requested”

“the transfer of“

“contact”
“domain”

<object roid>

Balance

Zero balance:	“Alert: Very low credit balance:” <balance>
10% of standard balance:	“Warning: Low credit balance:” <balance>
else	“Notice: Credit balance:“ <balance>

DAILY STATISTIC MESSAGES SENT TO REGISTRAR

Domains Transferred In:

Number of completed registrar to registrar domain transfers, where the subject registrar is the gaining registrar (In).

Transfers Cancelled:

Number of registrar to registrar domain transfers that were requested, but cancelled.

Domains Transferred Out:

Number of completed registrar to registrar domain transfers, where the subject registrar is the losing registrar (Out).

Domains Created:

Number of domains created by a registrar.

Domains Cancelled:

Number of domains deleted within three days of creation.

Domains Expired:

Number of domains that were deleted 14-21 days after the expiry date.

Domains Deleted:

Number of domains deleted more than three days after creation and before expiry date.

Domains Renewed:

Number of domains owned by a registrar which have been renewed.

WHOIS

Policy

- IP addresses get 20 WhoIs lookups per hour.
- Blacklist lasts till the end of the day on which the limit was exceeded.
- **Limit of 100 lookups in a single day.**