.au DOMAIN ADMINISTRATION LTD

ccNSO Tech Day

.au Registry Transformation Project

Barcelona, Spain

22 October 2018

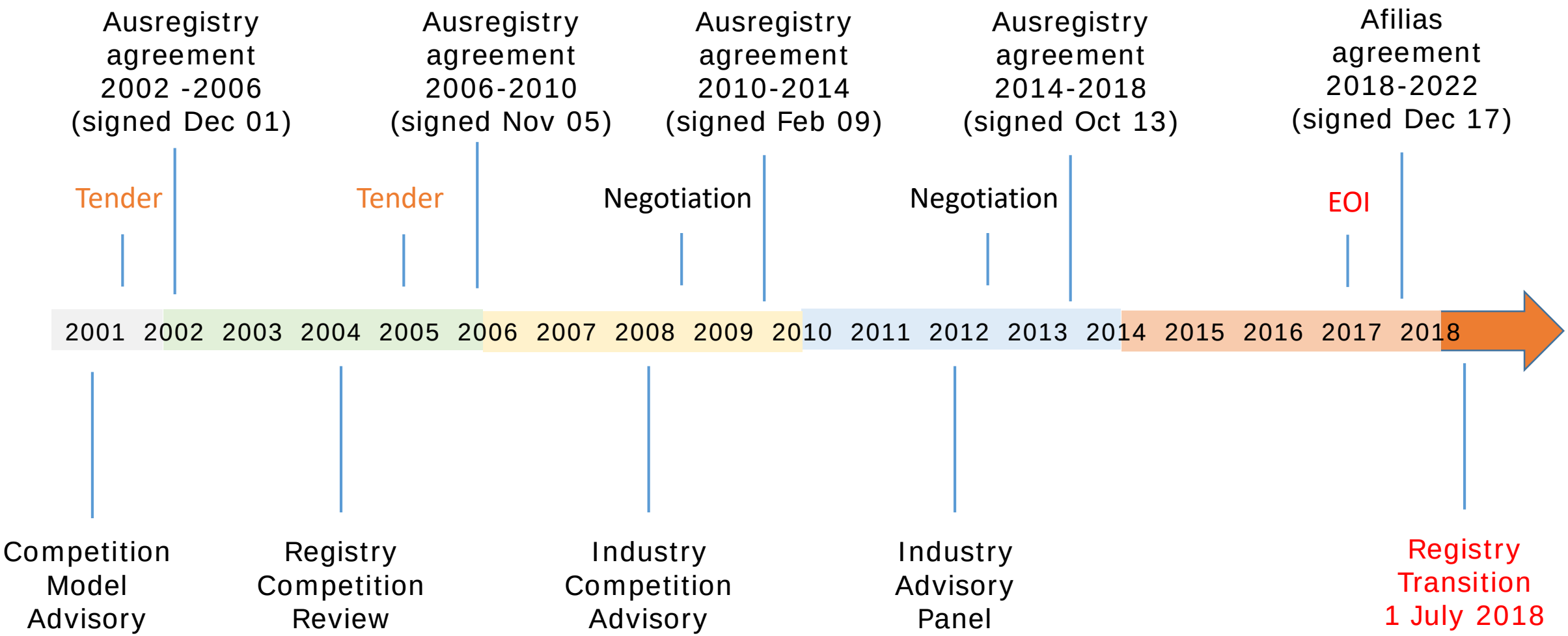
Contents

- Background
- Transition
- Outcomes
- Lessons Learnt

.au DOMAIN ADMINISTRATION LTD

Background

Background - Timeline



Registry Transformation Project Goals

a) Clear and effective separation between policy and operations

b) Maintain and further enhance trust with the Australian Government and the Australian community

c) Maintain operational stability and utility of the .au ccTLD

d) Becoming a world leader in managing security, confidentiality, integrity and availability of .au registry data

e) Supporting longer term goal to be an Emergency Back-end Registry Operator (EBERO) for other gTLDs or ccTLDs

f) Supporting a data science and data analytics capability in relation to the registry data

Second level domains

- .com.au - 2.8m names - main commercial name space in Australia
- .net.au - 260,000 names – originally for network providers
- .org.au – 70,000 names – for non-commercial organizations
- .id.au – 12,000 names – for individuals
- .asn.au – 3,400 – incorporated and un-incorporated associations
- .edu.au (.vic.edu.au etc) – 17,000 – educational institutions
- .gov.au (.nsw.gov.au, .vic.gov.au etc) – 5,000 – Government entities
- .qld.au, .vic.au etc – 220 - neighbourhood community orgs
- Linux.conf - 1 – technical conference
- **Total** - 3.1m names

Expression of Interest process

- The Request for Expressions of Interest (**REOI**) was the initial scoping exercise to:
  - define parameters of the subsequent restricted tender process
  - assess potential suppliers and options
- Call for Expression of Interest – 29 May 2017
- Expression of Interest closed – 26 June 2017
- Received 15 responses –mixture of ccTLD, gTLD operators, and software development proposals

Request for Tender process

- Draft Technical Specification published for comment – 26 August 2017
  - Summary of changes to Technical Specification published 21 September 2017
- Request for Tender (RFT) issued – 1 September 2017
- RFT closed – 3 October 2017
- 9 complete responses
- Short list of 3 – asked for best and final offers, and negotiated contracts with all 3
- Afilias selected in Dec 2017

Relevant international standards

- ISO 31000 – Risk management
- ISO 27000 – Information Security Management Systems
- ISO 22301 – Business Continuity Management Systems
- ISO 20000 – Service Management
- ITIL Service Operation – 2011 edition

Relevant Australian Security standards

- Australian Signals Directorate – Essential Eight
  - Application Whitelisting
  - Patch applications
  - Configure Microsoft Office macro stings
  - User application hardening
  - Restrict Administrative privileges
  - Patch Operating Systems
  - Multi-factor authentication
  - Daily backups
- Australian Gov't Information Security Manual (ISM) – Protected level

.au DOMAIN ADMINISTRATION LTD

Transition between Registry Operators

Transition Approach

- 6 month process – a lot to do:
  - Software Development – customized data fields and EPP extensions
  - Data Migration – 3.1 million domains, and numerous host and contact records
  - Infrastructure build – registry platform, disaster recovery site, DNS nodes in each Australian capital city (8)
- Close coordination with registrars – monthly briefings

Transition Approach

- Focussed on International and Australian best practice standards with respect to the transition of a major IT service provider
- Particular focus on risk management (ISO 31000) and security (ISO 27001)
- Ernst & Young engaged as independent risk assurance auditor and provided reports to the auDA Board on the state of risk management

Software development

- Test environments for registrars delivered in March (Phase 1) and April (Phase 2) 2018
- First test environment included all the core operations to create, update, renew and cancel domain names
- Second test environment included more specialized commands – support for resellers, policy deletes, registrant-to-registrant transfers
- Extensive testing from Feb 2018 to June 2018
  - Afilias testing team
  - auDA testing team
  - Registrar testing

Data Migration

- Gained access to the data from the previous registry operator in March 2018
  - Monthly drops of registry data – Mar, Apr, May
  - Weekly drops of registry data – June
- Had read access to the .au second level zones
- Migrated each drop of data into a test platform and generated zonefiles to compare with the existing operator's generated zonefile , and also created a publicly accessible WHOIS service in May 2028 using the data that registrars could check for errors
- Identified data gaps from the existing provider and also constantly adjusted the migration scripts to address migration errors

Infrastructure Rollout

- Registry Data had to stay in Australia
- Test environments were built in Australia as well as production environment
- Before any registry data was allowed to be used in any environment it needed to go through a security audit and penetration testing
- Full DR testing was also completed prior to transition
- Began operating Afilias DNS nameservers at top level in Jan 2018, and copies of the zone also operated at the second level (unlisted in .au). Progressively added nameservers in each capital city over Jan to Jun 2018 period.

DNS transition

- Ran new nameservers with copies of the zone file months before transition
- In the week before transition – new nameservers were added to the .au zone file, and the previous registry operator nameservers were removed
- DNSSEC signatures for the new registry were published in the zone weeks before transition
- On transition day Afilias took over publishing and signing the zonefile – all the new DNS nameservers were already operating before the transition weekend

Independent audits

- Multiple independent reviews of security prior to transition
  - Ernst & Young - risk assurance – weekly review
  - Pivot Point Security – appointed by Afilias for penetration testing
  - Foresight IT Consulting – appointed by the Aust. Government to do an independent review of security processes for transition
  - Australian Government security agencies (ASD, ASIO, ACSC) did their own separate review of security
  - Regular meetings with the auDA Board's Security and Risk Committee

Crisis Management

- Crisis management plan developed with input from Afilias, auDA, and Australian Government security agencies
- Multiple crisis scenario exercises run with the participation of Afilias, auDA, and Australian Government security agencies, with auDA Board observers

Registry cut-over on 30 June / 1 July

- Announced a 48 hour planned outage
  - Target was completion in 24 hours with a 24 hour buffer
- Final copy of the registry data from the previous operator was delivered ahead of schedule on 30 June
- Data migration completed smoothly
- Completed transition within 24 hours
- Most Registrars immediately commenced operations on 1 July with little disruption
- auDA uses a network of 20 probes covering Australian cities as well as key locations globally - measuring uptime and performance

.au DOMAIN ADMINISTRATION LTD

Outcomes

Key outcomes

- Lower registry fee – 10% drop in wholesale prices for registrars
- Registry Data to remain in Australia
- DNS services in all Australian capital cities
  - Perth, Adelaide, Melbourne, Hobart, Canberra, Sydney, Brisbane, Darwin
- Pro-active security monitoring – daily inspection of names
- Extensive data collection for advanced data analytics to move to proactive compliance management and development of business information for registrars
- Focus on improved security and performance

.au DOMAIN ADMINISTRATION LTD

Lessons Learnt

Lessons for next time

- EPP testing was very thorough but would have benefited from being able to test EPP commands through to a test WHOIS display
- Earlier you get access to the registry data the better - would have preferred access 6 months before transition
- Differences in how the registry operators publish host data in the DNS – Neustar took a narrow publishing approach and Afilias a wide publishing approach - resulted in some old host records being published that were used by some resolvers when the authoritative servers failed – focus of testing was on the domain name data rather than some of the host address data

Lessons for next time

- IT service providers – resellers to registrars – used purpose built tools (e.g. authInfo retrieval) by the previous registry that weren‘t picked up in the testing process, and needed to be improved after transition – need to engage resellers as part of the planning for testing
- DNS nameservers gave geographic diversity around Australia – but strange routing from ISPs particularly for IPv6 resulted in queries going to physical locations at long distances from the source of the queries