

Applicant input specification for pre-delegation testing

Version: 1.1

05 March 2013

1 Introduction

This document contains specifications for the input data required for the pre-delegation tests that the applicants shall provide to the PDT Provider.

The purpose of the pre-delegation testing is to verify that the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described in the gTLD Applicant Guidebook (AGB) and that applicant can operate the gTLD in a stable and secure manner. Each applicant will be required to complete pre-delegation testing as a prerequisite to delegation into the root zone.

The test elements cover both the DNS server operational infrastructure and registry system operations. The tests are based on the AGB, in specific Module 5 (*Transition to Delegation*) and specification 2, 4, 6 and 10, and are described in detail in the document: Pre-delegation testing, Master Test Plan.

1.1 Methodology

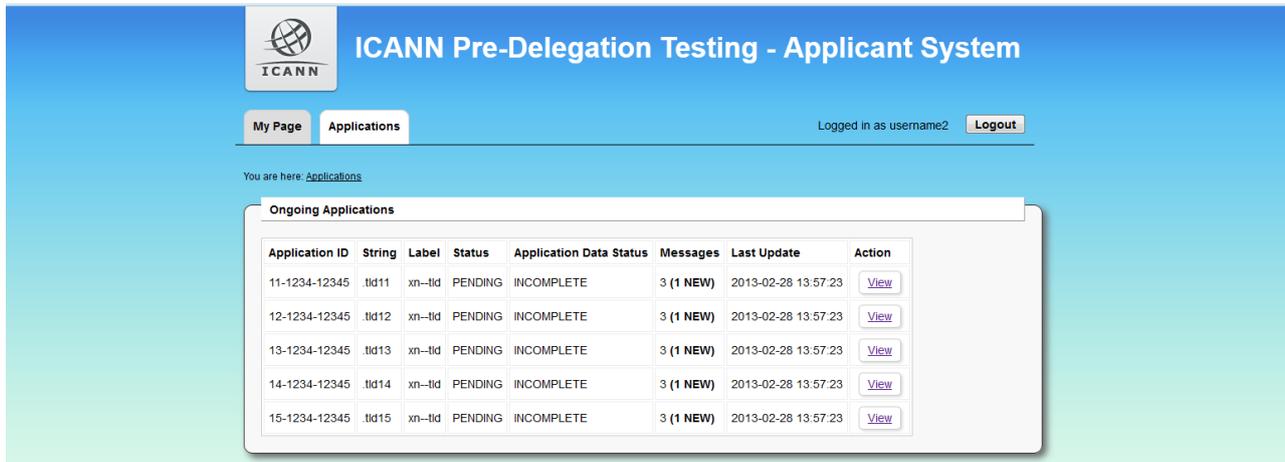
The tests are documented according to the standard IEEE 829-2008, as described in the Master Test Plan. The standard allows for different types of tests, e.g. unit, system, and acceptance tests. This test environment will focus on acceptance testing. Multiple areas have however been identified within the system requirements:

- DNS
- Whois
- EPP
- IDN
- Data Escrow
- Documentation

Each test area is further described in its own Level Test Plan and one or more Level Test Case documents, which will be published by ICANN.

1.2 Data entry into the PDT Applicant System

All input data to the tests shall be provided by the applicant via the PDT Applicant System, available as a web application at <https://pdt.iis.se/>. Login credentials will be given to the applicant once the testing has been scheduled by ICANN.



The screenshot displays the ICANN Pre-Delegation Testing - Applicant System interface. The header includes the ICANN logo and the title "ICANN Pre-Delegation Testing - Applicant System". Below the header, there are navigation tabs for "My Page" and "Applications", and a user status indicator "Logged in as username2" with a "Logout" button. The main content area shows a breadcrumb "You are here: Applications" and a section titled "Ongoing Applications" containing a table with the following data:

Application ID	String	Label	Status	Application Data Status	Messages	Last Update	Action
11-1234-12345	.ltd11	xn--ltd	PENDING	INCOMPLETE	3 (1 NEW)	2013-02-28 13:57:23	View
12-1234-12345	.ltd12	xn--ltd	PENDING	INCOMPLETE	3 (1 NEW)	2013-02-28 13:57:23	View
13-1234-12345	.ltd13	xn--ltd	PENDING	INCOMPLETE	3 (1 NEW)	2013-02-28 13:57:23	View
14-1234-12345	.ltd14	xn--ltd	PENDING	INCOMPLETE	3 (1 NEW)	2013-02-28 13:57:23	View
15-1234-12345	.ltd15	xn--ltd	PENDING	INCOMPLETE	3 (1 NEW)	2013-02-28 13:57:23	View

The Applicant System is further described in a separate User guide, which will be published by ICANN.

2 DNS test

2.1 Introduction

The PDT Provider will verify applicant's DNS infrastructure over both UDP and TCP, and that DNSSEC is supported including life cycle management of Zone and Key signing keys.

All tests will be carried out for both IPv4 and IPv6. In case applicant is utilizing anycast cluster(s) each individual node will be evaluated.

For the DNS tests, applicant should supply the following information to the PDT Provider:

[REQUIRED]

- FQDN of all authoritative name servers
- IPv4 and IPv6 addresses for same
- Delegation Signer (DS) information

[FOR EACH ANYCAST CLUSTER, IF ANY]

- FQDN and IPv4/v6 address for authoritative name server
- Name of the anycast provider (optional)
- An ID for each location that is unique within the cluster
- Either FQDN or IPv4/v6 address of each location
- Optionally port number, description for each location

If FQDN is given for a location, a DNS query for SRV record may be used to look up destination address and port, with service set to '_domain' and protocol to '_tcp' or '_udp'. Like so:

```
_domain._udp.proxy.example.com. IN SRV.
```

If the SRV lookup fails, A or AAAA address for the FQDN will be used.

If public unicast addresses of the anycast locations cannot be provided, applicant must provide a DNS proxy for all the unicast locations in the anycast network.

2.2 Expected input

The applicant shall provide the input data for the DNS test in a single XML file according to the XML schemas provided by the PDT provider.

2.2.1 XML schemas

There are two different XML schemas of which the applicant can choose from. These are the W3C XML Schema (XSD) and the RELAX NG (RNG).

- ptdns.rng
- ptdns.xsd

2.3 Example of input

For your convenience an example XML file containing input data for the DNS test is provided.

3 Whois test

The PDT Provider will verify that Whois data is accessible over IPv4 and IPv6, both via TCP port 43 and via a web interface. If applicant states that searching in Whois data is supported, this functionality will also be evaluated.

For the Whois tests, applicant should supply the following information to the PDT Provider:

[REQUIRED]

- An existing domain name which has Whois data
- An existing registrar which has Whois data
- The domain name of an existing name server which has Whois data
- IPv4 or IPv6 address of an existing name server which has Whois data

[OPTIONAL]

- Credentials, e.g. username and password, if required for accessing the Whois search service as a logged in user

3.1 Expected input

The applicant shall provide the input data for the Whois test in a single XML file according to the XML schemas provided by the PDT provider.

3.1.1 XML schemas

There are two different XML schemas of which the applicant can choose from. These are the W3C XML Schema (XSD) and the RELAX NG (RNG).

- pdtwhois.rng
- pdtwhois.xsd

3.2 Example of input

For your convenience, an example XML file containing input data for the Whois test is provided.

4 EPP test

The PDT Provider will verify that applicant's EPP Service conforms to appropriate RFCs, including EPP extensions for DNSSEC. Changes and updates in zone data must be visible in applicant's zone file and Whois service within 60 minutes. If applicant states support for EPP over IPv6, the PDT Provider will verify this too.

For the EPP tests, applicant should supply the following information to the PDT Provider:

[REQUIRED SETUP INFORMATION]

- Information about the EPP server: IPv4 address+port, server certificate and optionally IPv6 address+port
- Credentials required to access the EPP service
- URI and Schema Location for Domain, Contact and Host objects
- URI and Schema Location for the SecDns extension (DNSSEC)
- URI and Schema Location for other extensions, if applicable

[FOR THE TESTS]

- FQDN for at least two name servers
- Three not registered domain names, ready to be created
- One registered domain name ready to be renewed
- Two registered domain names ready for transfer
- One domain name that can be deleted
- A new Contact object, to be created
- Contact and Host objects to be updated
- Contact and Host objects to be deleted

4.1 Expected input

The applicant shall provide the input data for the EPP test in a single XML file according to the XML schemas provided by the PDT provider.

While EPP allows for a large number of extensions to each object, the applicant should only submit values for those extensions that are mandatory for their registration system.

4.1.1 XML schemas

There are two different XML schemas of which the applicant can choose from. These are the W3C XML Schema (XSD) and the RELAX NG (RNG).

- pdtepp.rng
- pdtepp.xsd

4.2 Example of input

For your convenience, an example XML file containing input data for the EPP test is provided.

5 IDN test

5.1 Introduction

The pre-delegation testing of a new gTLD's IDN support requires access to two sets of documents. The first is the full listing of available codepoints in the form of one or more tables formatted according to RFC 4290 or RFC 3743. If there is any reason why these formats cannot be used, a detailed explanation must be included. In all cases, the tables must be machine parsable .TXT files with the codepoint keying each row being immediately identifiable.

The second component of the documentation is a complete statement of the policies that determine how the tabulated codepoints may be strung together to form registerable labels, and the way in which indicated variant relationships between codepoints are managed. This may take the form of comments placed in the tables themselves or as separate texts. This material should also be submitted in .TXT files in a format that readily permits the copying and pasting of text out of it.

5.2 Expected input

The applicant shall provide .TXT files as specified above.

6 Data Escrow test

The PDT Provider will verify that the data escrow deposit conforms to the relevant IETF draft or RFC document. This includes, among other things, file formats, file names and methods for encryption and signing of the escrow file(s).

For the Data Escrow tests, applicant should supply the following information to the PDT Provider:

[REQUIRED]

- A Data Escrow profile in W3C XML schema format
- One full deposit, encrypted
- A signature file, containing the signature of above
- Applicant's public key in OpenPGP format

[OPTIONAL]

- A differential deposit, encrypted
- A signature file, containing the signature of above

6.1 Expected input

Both the full deposit and the differential deposit may be split over several files. In this case each data file shall be individually signed and accompanied by a corresponding signature file.

The deposit shall be supplied in files formatted according to the rules in <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow> (refer to latest version) or corresponding RFC as well as RFC 4880.

7 Self-certification documentation test

7.1 Introduction

This section contains the specification for the self-certification data that the applicant shall provide as part of the pre-delegation test.

The documentation tests are divided into the following groups:

- Self-certification of DNS, Whois and EPP
- DNSSEC Practice Statement
- Data Escrow

7.2 Expected input

The applicant shall provide the following input data for the different groups of self-certification documentation tests:

Documentation Test	Input data
Self-certification	A single PDF/A file following the template provided by the PDT Provider
DNSSEC Practice Statement	A single PDF/A file containing the DNSSEC Practice Statement
Data Escrow	One or more PDF/A files containing the escrow provider agreement with all appendices

7.2.1 Templates and examples

The self-certification template is provided as an HTML file.

Documentation Test	Templates
Self-certification	File Self-certification document1_v1.1.html

8 Appendix 1:

The following files are attached to this document:

- Self-certification document1_v1.1.html
- ptdns.rng
- ptdns.xml
- ptdns.xsd
- pdtepp.rng
- pdtepp.xml
- pdtepp.xsd
- pdtwhois.rng
- pdtwhois.xml
- pdtwhois.xsd