Instructions for PDT testing

Version: 1.5 Update 1
16 May 2013

1 Introduction

This document contains information that the applicants need to prepare for the pre-delegation tests. All applicants are urged to carefully read this document.

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 System

All input data to the tests shall be provided by the applicant via the PDT 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 PDT System is further described in a separate User guide, which will be published by ICANN.

2 PDT Test Nodes

The PDT Service Provider will verify applicant's infrastructure (whois, EPP and DNS) from the PDT Test Nodes. The applicant must make sure that firewalls and access lists are open for the following IP addresses (both IPv4 and IPv6). The applicant's infrastructure must be available for testing during the whole test period.

Please make sure that you look at the latest version of this document so that you have the current set of IP addresses of the PDT Test Nodes.

2.1 IP addresses

PDT Test Node	IPv4	IPv6	Hostname
North America	74.63.16.34	2620:171:f0::34	node-pao.pdt.iis.se
	74.63.17.34	2620:171:f1::34	node-iad.pdt.iis.se
Latin America and Caribbean	74.63.19.34	2620:171:f3::34	node-gru.pdt.iis.se
	74.63.18.34	2620:171:f2::34	node-eze.pdt.iis.se
	200.1.120.31	2001:1398:3:120::31	node-scl.pdt.iis.se
Asia/ Australia/ Pacific	203.178.137.9	2001:200:0:180a::502	node-nrt.pdt.iis.se
	74.63.20.34	2620:171:f4::34	node-sgw.pdt.iis.se
	103.6.87.155	2403:2500:4000::afd	node-mma.pdt.iis.se
Africa	74.63.22.34	2620:171:f6::34	node-cai.pdt.iis.se
	197.96.55.76	2c0f:fc00:a000:1100::4	node-jnb.pdt.iis.se
	74.63.23.34	2620:171:f7::34	node-cpt.pdt.iis.se
Europe	74.63.25.34	2620:171:f9::34	node-ams.pdt.iis.se
	74.63.24.34	2620:171:f8::34	node-fra.pdt.iis.se
	77.72.225.37	2a01:3f0:0:4c::37	node-sth1.pdt.iis.se
	212.247.172.243	2a00:800:752:10::6a:3	node-sth2.pdt.iis.se

3 DNS test

3.1 Introduction

The PDT Service 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 Service 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
- An ID for the cluster that is unique within the delegation
- 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.

3.2 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 Service Provider.

3.2.1 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).

- pdtdns.rng
- pdtdns.xsd

3.3 Example of input

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

4 Whois test

The PDT Service 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 Service Provider:

[REQUIRED]

- An existing domain name for this TLD, 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

4.1 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 Service Provider.

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).

- pdtwhois.rng
- pdtwhois.xsd

4.2 Example of input

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

5 EPP test

The PDT Service Provider will verify that applicant's EPP Service conforms to appropriate RFCs, including EPP extensions for DNSSEC. For Create, the new object has to be visible in zone file and Whois within 24 hours. For changes, the 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 Service Provider will verify this too.

If your EPP server requires a client certificate for a client to be able to login, make sure you include the pkcs12 file and password in the Client/KeyPair part of the XML.

For the EPP tests, applicant should supply the following information to the PDT Service 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 registered domain name ready to be updated
- 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

5.1 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 Service 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.

5.1.1 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

5.2 Example of input

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

5.3 Submitting EPP extensions

If applicant's EPP server needs extra data not found in the standard object definitions, corresponding EPP extensions have to be specified as part of the input data.

Below you will find working XML example code to input three different EPP extensions and their associated data. Together with each example, the Extensions part of the resulting EPP command that will be sent to applicant's server during testing is shown.

5.3.1 A normal extension with two Name:Value fields

```
<Extension>
   <URI>urn:se:iis:xml:epp:iis-1.2</URI>
   <SL>urn:se:iis:xml:epp:iis-1.2 iis-1.2-xsd</SL>
   <Field>
      <Name>orgno</Name>
      <Value>[SE]551112-3282</Value>
   </Field>
   <Field>
      <Name>vatno</Name>
      <Value>SE551112328201</Value>
   </Field>
</Extension>
```

Resulting EPP fragment

```
<extension>
   <ex01:create xmlns:ex01="urn:se:iis:xml:epp:iis-1.2"
    xsi:schemaLocation="urn:se:iis:xml:epp:iis-1.2 iis-1.2-xsd">
      <ex01:orgno>[SE]551112-3282</ex01:orgno>
      <ex01:vatno>SE551112328201</ex01:vatno>
   </ex01:create>
</extension>
```

5.3.2 An IDN extension with a single text node

```
<Extension>
   <ExtName>language</ExtName>
   <URI>urn:ietf:params:xml:ns:idn-1.0</URI>
   <SL>urn:ietf:params:xml:ns:idn-1.0 idn-1.0.xsd</SL>
   <ExtValue>ger</ExtValue>
</Extension>
```

Resulting EPP fragment

```
<extension>
   <ex01:language xmlns:ex01="urn:ietf:params:xml:ns:idn-1.0"
    xsi:schemaLocation="urn:ietf:params:xml:ns:idn-1.0 idn-1.0.xsd">ger</ex01:language>
</extension>
```

5.3.3 An IDN extension with a single Name:Value field

```
<Extension>
   <URI>urn:ar:params:xml:ns:idn-1.0</URI>
   <SL></SL>
   <Field>
      <Name>languageTag</Name>
      <Value>ar</Value>
   </Field>
</Extension>
```

Resulting EPP fragment

```
<extension>
   <ex01:create xmlns:ex01="urn:ar:params:xml:ns:idn-1.0" xsi:schemaLocation="">
      <ex01:languageTag>ar</ex01:languageTag>
   </ex01:create>
</extension>
```

6 IDN test

6.1 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.

6.2 Expected input

The applicant shall provide .TXT files as specified above.

The applicant shall also submit a complete example of an EPP Domain Create command for a valid, unregistered, IDN label. The successful registration of this example (EPP result code 1000 or 1001) during the PDT process is a requirement for further IDN testing.

7 Data Escrow test

The PDT Service 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 Service Provider:

[REQUIRED]

- An encrypted full deposit in binary OpenPGP format (.ryde)
- The signature of above in binary OpenPGP format (.sig)
- Applicant's public key in OpenPGP format (.pub)

[OPTIONAL]

- An encrypted differential deposit in binary OpenPGP format (.ryde)
- The signature of above in binary OpenPGP format (.sig)

7.1 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.

Encryption shall be done using the PDT Service Provider's public test key, pdtescrow.pub.

8 Self-certification documentation test

8.1 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

8.2 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 adhering to the chapter structure of the template provided by the PDT Service Provider
DNSSEC Practice Statement	A single PDF/A file containing the DNSSEC Practice Statement
Data Escrow	A single PDF/A file containing the escrow provider agreement with all appendices

8.2.1 Templates and examples

For the self-certification documentation, an instruction and a template are provided.

Documentation Test	Files
Self-certification	Self-certification instruction.pdf
Self-certification	Self-certification template.txt

9 Appendix 1:

The following files are attachments to this document:

- Self-certification instruction.pdf
- Self-certification instruction.txt
- pdtdns.rnc
- pdtdns.rng
- pdtdns.xml
- pdtdns.xsd
- pdtepp.rnc
- pdtepp.rng
- pdtepp.xml
- pdtepp.xsd
- pdtwhois.rnc
- pdtwhois.rng
- pdtwhois.xml
- pdtwhois.xsd