

Technical Requirements for TelHosting Providers

June 2008



Contents

1.	INTRODUCTION	1
2.	ADDITIONAL DEFINED TERMS	1
3.	NAMING	2
4.	DNS PROTOCOL REQUIREMENTS.....	2
5.	NAME SERVER PERFORMANCE CRITERIA	3
5.1	DNS Service Availability	3
5.2	Throughput, packet loss and round-trip times	3
5.3	TTL Values and Propagation Times	4
6.	TELHOSTING PROVIDERS AND DNS OPERATIONAL REQUIREMENTS.....	5
7.	API COMPLIANCE	7
8.	USER-LEVEL FUNCTIONAL REQUIREMENTS	7
9.	TECHNICAL TELHOSTING PROVIDER FUNCTIONAL REQUIREMENTS.....	8
9.1	Zone Content Provisioning Features.....	8
9.2	TelHosting Provider NAPTR Support Notes.....	8
9.3	XML Import/Export.....	9
9.4	Provisioning Performance Requirements	9
10.	ADDRESS RECORDS.....	10
	Appendix A.....	1
	Contact Support in .tel	1
1.	Introduction.....	A-1
1.1	Specifications.....	A-1
1.2	Document Structure	A-1
2.	Enumservice Support in .tel.....	A-2
2.1	IETF Standards Track Enumservices.....	A-2
2.2	Non-IETF Enumservices	A-3
3.	Additional Adopted Contact Specifications.....	A-4
3.1	VoIP and IM Enumservices	A-4
3.2	Auxiliary Descriptive Enumservices	A-4
3.3	Protected Contacts	A-7
4.	Client Processing of Contacts	A-10
4.1	Telnic-funded client support.....	A-10
5.	Auto-Provisioning Support using Contacts	A-14
	Appendix B.....	16
	TXT Support in .tel.....	16
1.	Introduction.....	B-1
1.1	Generic data in TXT Records	B-1
1.2	Structured Data within TXT Records	B-1
2.	.TEL TXT Record Format	B-3
2.1	Parsing.....	B-3
3.	Special Strings in TXT records in .tel.....	B-5
3.1	Keyword types	B-5
3.2	System Message Types	B-7
3.3	Full Examples	B-7

1. INTRODUCTION

The Sponsoring Organisation has identified the role of a provider of TelHosting services (a “**TelHosting Provider**”) as an important entity within the system for the .tel TLD. TelHosting Providers will provide DNS service for delegations in the .tel TLD.

The .tel TLD is a sponsored TLD. Therefore the Sponsoring Organisation will be the sole authority for accreditation of TelHosting Providers. This document defines the technical specifications and requirements for accreditation, including minimum specifications in a number of areas relating to the domain name system: protocol compliance; performance metrics; name server configuration and operation; and adherence to the Sponsoring Organisation’s policies and TelHosting Provider functional requirements.

Any references in this document to the TelHosting Provider’s name server infrastructure apply to the name servers supplied by the TelHosting Provider for hosting zones for the .tel TLD. They are not intended to apply to any other name servers or zones maintained or hosted by the TelHosting Provider.

2. ADDITIONAL DEFINED TERMS

In this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” are to be interpreted as described in RFC 2119. These interpretations are as follows:

MUST; REQUIRED; SHALL the definition is an absolute requirement of the specification.

MUST NOT; SHALL NOT the definition is an absolute prohibition of the specification.

SHOULD; RECOMMENDED there may exist valid reasons in particular circumstance to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT; NOT RECOMMENDED there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY; OPTIONAL an item is truly optional. One TelHosting Provider may choose to include the item because a particular marketplace requires it or because it feels that it enhances its service offering while another TelHosting Provider may omit the same item.

3. NAMING

The naming standards policies for domain names in the .tel TLD (“Domain Names”) are described in a separate Acceptable Use Policy, which is posted on the Registry’s web site, and TelHosting Providers **MUST NOT** permit the use of Domain Names which conflict with those policies.

Delegations in the .tel TLD **MUST** only be served by name servers operated by accredited TelHosting Providers. The names of these servers **MUST** be subdomains of dns.nic.tel. The apex for the names under dns.nic.tel assigned for a TelHosting Provider’s name servers will be determined by the Sponsoring Organisation.

The Sponsoring Organisation’s naming standards policies may change from time to time. TelHosting Providers **MUST** ensure their systems follow the current policy and ensure any changes to the Sponsoring Organisation’s policies are incorporated in a timely manner. TelHosting Providers **MUST** commit to ensuring any changes to the Sponsoring Organisation’s policies are implemented no later than 135 days after any policy changes have been approved by the Sponsoring Organisation and posted to the Registry’s web site.

4. DNS PROTOCOL REQUIREMENTS

All name servers used in .tel **MUST** be operated in compliance with the DNS protocol specifications defined in the following Requests for Comments (RFCs): 1034, 1035, 1101, 1996, 2181, 2182, 2308, 2671, 3263, 3401, 3402, 3403, 3404, 3405, 3597 and 3671. TelHosting Providers **MUST** ensure the name servers hosting .tel TLD zones comply with all these RFCs and any subsequent RFCs which update or supersede them.

Name servers in .tel **SHOULD** implement:

Incremental Zone transfer, IXFR, defined in RFC 1995;

NOTIFY as documented in RFC 1996; and

Dynamic DNS, which is defined in RFC 2136.

These protocol features enhance performance and improve interoperability. A TelHosting Provider’s name servers **SHOULD** also offer TSIG and SIG(0) for authentication of the IXFR, NOTIFY and Dynamic DNS transactions. RFCs 2845 and 2931 define these two protocol specifications respectively. TelHosting Providers **SHOULD** comply with these DNS protocols.

The Sponsoring Organisation does not offer Internationalised Domain Names (IDNs) or Secure DNS (DNSSEC) for the time being. These may be introduced at some point however. Therefore TelHosting Providers **MAY** support the core standards for Internationalised Domain Names. These are documented in RFCs 3490, 3491 and 3492 along with any Standards Track RFCs which update or supersede these specifications. Similarly, TelHosting Providers **MAY** support the core DNSSEC specifications which are defined in RFCs 4033, 4034 and 4035 as well as those Standards Track RFCs which update or supersede these specifications. Although it would be prudent for TelHosting Providers to ensure their systems and procedures have been designed to facilitate the introduction of IDNs and

DNSSEC, the Sponsoring Organisation does not currently insist on this as an accreditation requirement.

The Sponsoring Organisation's DNS protocol requirements may change as a result of new protocol developments such as DNS-related Standards Track RFCs produced by the IETF or other relevant standards-making organisations. TelHosting Providers MUST commit to ensuring any changes to the Sponsoring Organisation's DNS protocol requirements are implemented no later than 135 days after these changes have been approved by the Sponsoring Organisation and posted on the Registry's web site.

5. NAME SERVER PERFORMANCE CRITERIA

5.1 DNS Service Availability. DNS service availability refers to the ability of a TelHosting Provider's name servers to resolve a DNS query from an Internet user. TelHosting Providers SHOULD provide a minimum service availability of 99.999% measured in monthly time frames. In other words, delegations in .tel SHOULD NOT be unresolvable for longer than a cumulative total of 25 seconds in any 30 day period.

At any time at which it is available, each name server serving Delegated Zones operated by an accredited TelHosting Provider MUST be able to handle a load of queries for DNS data that is three times the measured daily peak (averaged over the monthly time frame) of such requests on the most loaded name server. In this context the term "name server" applies to a cluster of name servers using a common IP address or some form of load balancer: the cluster is treated as a single DNS server.

5.2 Throughput, packet loss and round-trip times. TelHosting Providers MUST provide DNS service for .tel TLD delegations that meets or exceeds the specifications defined by ICANN's Cross-Network Name Server Performance Requirements (CNNP) for .tel, as described in Appendix 7, Section 7 of the Registry Agreement.

The current required performance specification for Cross-Network Name Server Performance is a measured round-trip time (RTT) of less than 300 ms and measured packet loss of fewer than 10%. CNNP measurements will be carried out by the Sponsoring Organisation at its discretion and at times of its choosing, in the following manner:

- (a) The measurements will be conducted by sending strings of DNS request packets from each of four measuring locations to each of the name servers and observing the responses from the TelHosting Provider's name servers. (These strings of requests and responses are referred to as a "CNNP Test".) The locations for conducting these tests will be chosen by the Sponsoring Organisation and are expected to be major Internet exchange points in Europe, Asia and North America.
- (b) Each string of request packets will consist of 100 UDP packets at 10-second intervals requesting NAPTR records for arbitrarily selected second-level domains in .tel, preselected to ensure that the names exist and are hosted on the TelHosting Provider's DNS infrastructure. The packet loss (i.e. the percentage of response packets not received) and the average RTT for response packets received will be noted.

To meet the packet loss and RTT requirements for a particular CNNP Test, all three of the following MUST be true:

- (a) The RTT and packet loss from each measurement location to at least one name server MUST NOT exceed the required values.
- (b) The RTT to each of 75% of the name servers from at least one of the measurement locations MUST NOT exceed the required value.
- (c) The packet loss to each of the name servers from at least one of the measurement locations MUST NOT exceed the required value.

Any failing CNNP Test result obtained during an identified Core Internet Service Failure shall not be considered.

To ensure a properly diverse testing sample, the Sponsoring Organisation MAY conduct the CNNP Tests at varying times (i.e. at different times of day, as well as on different days of the week). The CNNP performance requirement will be deemed not to have been met if the name servers persistently fail the CNNP Tests with no less than three consecutive failed CNNP Tests to be considered to have persistently failed.

In the event of a failure of the CNNP Tests prior to accreditation, the Sponsoring Organisation will give the TelHosting Provider written notice of the failures (with backup data) and the TelHosting Provider will have sixty days to cure the failure.

If, following the TelHosting Provider's opportunity to cure, the TelHosting Provider's DNS infrastructure continues to fail CNNP Tests and the TelHosting Provider fails to resolve the problem within thirty days after written notice of the continuing failures, the TelHosting Provider's accreditation will not be accepted.

Sixty days before the commencement of testing under this provision, the Sponsoring Organisation will provide TelHosting Providers with the opportunity to evaluate the testing tools and procedures to be used. In the event that a TelHosting Provider does not approve of such tools and procedures, the Sponsoring Organisation will work directly with the TelHosting Provider to make necessary modifications. If mutual agreement is not possible, the Sponsoring Organisation's decision will be final and binding on both parties.

The Sponsoring Organisation MAY conduct CNNP Tests under this procedure at any time after the initial accreditation had been granted, such as to investigate a complaint. In the event of an accredited TelHosting Provider failing these tests, the Sponsoring Organisation will consider this failure and may apply sanctions which include, but are not limited to, withdrawal of accreditation.

5.3 TTL Values and Propagation Times. The Sponsoring Organisation MAY from time to time issue recommendations or policies on Time To Live (TTL) values and zone propagation times in .tel. A TelHosting Provider MUST ensure its systems comply with these requirements. Systematic failure to meet these obligations without good reason may result in action (such as loss of accreditation) being taken against the TelHosting Provider by the Sponsoring Organisation.

In the absence of superseding recommendations or policies, the following requirements apply:

- (a) The expire value in a .tel zone's SOA record SHOULD NOT be less than 30 days (2592000 seconds).
- (b) The refresh interval in a .tel zone's SOA record SHOULD NOT exceed 8 hours (28800 seconds).
- (c) The retry interval in a .tel zone's SOA record SHOULD NOT exceed 1 hour (3600 seconds).
- (d) The time-to-live (TTL) value for a .tel zone's NS records SHOULD NOT be less than 1 day (86400 seconds).
- (e) The default TTL value for negative caching in a .tel zone's SOA record SHOULD NOT exceed 15 minutes (900 seconds).
- (f) The default TTL value for all NAPTR records in a .tel zone record SHOULD NOT exceed 15 minutes (900 seconds).
- (g) All resource records of the same name, class and type in a .tel zone SHOULD have the same TTL.
- (h) Updates to a .tel zone SHOULD be propagated from the TelHosting Provider's provisioning system or master name server to all of the zone's name servers within 15 minutes (900 seconds) or the zone's refresh interval, whichever is the lower.
- (i) The maximum time for updates to a .tel zone to be propagated from the TelHosting Provider's provisioning system to all of the zone's name servers MUST NOT exceed 15 minutes (900 seconds) or the zone's refresh interval, whichever is the higher.
- (j) The average time for updates to a .tel zone to be propagated from the TelHosting Provider's provisioning system to all of the zone's name servers SHOULD NOT exceed 30 minutes (1800 seconds) or half the zone's refresh interval, whichever is the lower.

The Sponsoring Organisation's DNS performance requirements may change as a result of new IETF protocol developments or contractual obligations imposed by ICANN and any other relevant standards-making organisations. TelHosting Providers MUST commit to ensuring any changes to the Sponsoring Organisation's DNS performance requirements are implemented no later than 135 days after these changes have been approved by the Sponsoring Organisation and posted on the Registry's web site.

6. TELHOSTING PROVIDERS AND DNS OPERATIONAL REQUIREMENTS

TelHosting Providers MUST ensure that name servers hosting zones for .tel TLD delegations do not query other name servers, except when such queries are essential to providing DNS service for those zones. In other words, a TelHosting Provider's name servers MUST offer authoritative-only DNS service for delegated .tel zones. These authoritative-only name servers MUST NOT offer recursive service or fetch glue. They MUST NOT initiate DNS

queries, other than SOA refresh/retry checks, zone transfers and NOTIFY messages where these are necessary for proper operation of a .tel TLD delegation.

Name servers for .tel TLD delegations SHOULD provide NOTIFY, dynamic update and incremental zone transfer capabilities as documented in RFCs 1996, 2136 and 1995 respectively. They SHOULD also offer TSIG and SIG(0) for authentication of these transactions. RFCs 2845 and 2931 define these two protocol specifications.

Zone transfers for all .tel TLD delegations SHOULD be restricted to authorised name servers: the TelHosting Provider's slave servers or to approved audit and escrow systems.

A TelHosting Provider's name servers for .tel MUST NOT support "alternate roots".

All name servers in the .tel TLD MUST support DNS queries using TCP as well as UDP.

A TelHosting Provider's name servers SHOULD be operated in accordance with the recommendations of RFC 2812 and RFC 2870 as far as these can reasonably be applied. This means TelHosting Providers SHOULD make reasonable efforts to avoid single points of failure in their DNS infrastructure: for example by placing name servers in different physical locations in different networks and using different hardware, operating systems and DNS server software. The TelHosting Provider's name servers SHOULD be configured and managed in line with the advice given in RFC 2870, with particular reference to the guidance on physical, network and systems security.

TelHosting Providers SHOULD implement effective monitoring of their DNS systems and provide a reasonable problem escalation and resolution process. A TelHosting Provider's monitoring procedures SHOULD check for obvious DNS service problems such as lameness, unreachable or unresponsive servers and zone synchronisation inconsistencies. A TelHosting Provider MUST take appropriate corrective action whenever such problems are identified. TelHosting Providers SHOULD provide adequate customer service and fault reporting mechanisms.

Appropriate logging, audit trails and change management procedures SHOULD be in place for management of the TelHosting Provider's name servers and provisioning systems. TelHosting Providers MUST deploy relevant patches and security fixes to their name servers and provisioning platforms in a timely manner. TelHosting Providers SHOULD monitor DNS loads and traffic patterns for capacity planning, server placement and traffic analysis. TelHosting Providers MUST take reasonable precautions to defend against denial of service attacks, malware and other security violations.

Where reasonably practical to do so, TelHosting Providers SHOULD offer at least one name server in each RRset for a .tel TLD delegation that has IPv6 capability and can be reached over IPv6 from the Internet: i.e. at least one name server for every .tel TLD zone should have a valid IPv6 address in a prefix which is routed on the Internet, not a link-local IPv6 address.

TelHosting Providers SHOULD provide support for the Sponsoring Organisation-supplied toolkits and provisioning software to allow end users to manipulate their Domain Name data. TelHosting Providers choosing to operate other software for such provision MUST ensure it provides similar functionality to and can interwork with those Sponsoring Organisation-supplied components.

TelHosting Providers MUST facilitate the transfer of DNS service between TelHosting Providers when reasonably requested by end users.

The Sponsoring Organisation's TelHosting Provider and DNS operational requirements may change from time to time. TelHosting Providers MUST commit to ensuring any changes to the Sponsoring Organisation's operational requirements are implemented no later than 135 days after these changes have been approved by the Sponsoring Organisation and posted on the Registry's web site.

7. API COMPLIANCE

TelHosting Providers MUST support the APIs defined in the Sponsoring Organisation's "API Schemas for TelHosting Provider Provisioning System" published on the Registry's web site.

TelHosting Providers MUST pass any API conformance tests defined by the Sponsoring Organisation. These tests may be updated from time to time and a TelHosting Provider MUST ensure its systems comply with updated conformance tests within 135 days of these being endorsed by the Sponsoring Organisation and posted on the Registry's web site.

8. USER-LEVEL FUNCTIONAL REQUIREMENTS

TelHosting Providers MUST provide the following minimum set of features to users of the .tel TLD system. These include, but are not limited to:

- (a) The ability for a user to change or restore his or her password or other authentication token for accessing the TelHosting Provider system.
- (b) The ability of users to update and manipulate the contact data the TelHosting Provider publishes for them in their .tel TLD zones.
- (c) The ability for Domain Name holders to populate protected contacts for their choice of selected readers, as specified in Appendix A "Contact Support in .tel" document.
- (d) Support for profile switching, through any combination of web-based activity and switching requests issued by the user from a hand-held or other device.
- (e) The capability to import and export a user's TelHosting Provider data in full to facilitate TelHosting Provider transfers and promote competition.
- (f) A Domain Name holder must be able to populate and update textual data as defined in Appendix B "TXT Support in .tel" document into his or her Domain Name's zone. Where that data consists of structured keywords, the TelHosting Provider SHOULD notify the Sponsoring Organisation's search system within 1 hour (3600 seconds) of such an update.
- (g) Adequate backup and archive arrangements.

- (h) A restore/undo capability to permit Domain Name holders to revert to previous versions of their Domain Name zone, friends list, profiles and keywords.

The TelHosting Providers MUST employ reasonable security measures to protect Domain Name holders and their Domain Name delegations. These include but are not limited to: access controls for updates; checkpointing and roll back/forward of zone contents; warnings when using unwise constructs such as inappropriate TTLs, unaccredited services, unverifiable certificates, etc.; alerts when updates fail to propagate within the accepted constraints; and syntactic and semantic sanity checks on zone contents.

9. TECHNICAL TELHOSTING PROVIDER FUNCTIONAL REQUIREMENTS

Domain Name holders MUST be offered access to systems that allow them to provision their delegated zones appropriately. Such systems MUST meet the criteria of Section 3 of the Acceptable Use Policy and provide the following features.

9.1 Zone Content Provisioning Features.

- (a) Automatic Provisioning of the Sponsoring Organisation-defined Address Record in the apex of the registered Domain Name, and a Sponsoring Organisation-defined CNAME Record for the www label within the Domain Name. The value of the Address Record and the CNAME Record MUST be exactly as specified and published by the Sponsoring Organisation. No other Address Record or CNAME Record (or values) will be permitted in delegated zones. Therefore user-specified provisioning of such records MUST NOT be supported;
- (b) TXT records, as specified in Appendix B “TXT Support in .tel” document;
- (c) Full support for E2U NAPTR Records, as specified in Appendix A “Contact Support in .tel”;
- (d) D2U/D2T/D2S NAPTR records as defined in RFC 3263;
- (e) SRV records (specifically in _sip._udp and _sip._tcp subdomains);
- (f) MX records;
- (g) ZS (“TXT-like”) records when these are processed by the IETF;
- (h) In-zone subdomains and the Resource Records within those subdomains, where these are referred to by non-terminal NAPTRs, or when required for protected contact use as defined in Appendix A “Contact Support in .tel” ; and
- (i) Profiles of zone content, allowing sets of pre-provisioned zone data to be selected and published en bloc.

9.2 TelHosting Provider NAPTR Support Notes.

- (a) A TelHosting Provider's provisioning system **MUST** offer full support for NAPTR Records with Enumservices as listed in Appendix A "Contact Support in .tel". Other Enumservices **MAY** be supported by the TelHosting Provider.
- (b) A TelHosting Provider's provisioning system **MUST** allow Domain Name holders to create NAPTR Records for protected contacts and couple these to the person or organisation to which the Domain Name holder chooses to make that protected contact data available as described in Appendix A "Contact Support in .tel".
- (c) A TelHosting Provider's provisioning system **SHOULD** populate a provisioning system contact within each Domain Name's zone it supports, as described in Appendix A "Contact Support in .tel".

9.3 XML Import/Export. A TelHosting Provider's systems **MUST** allow Domain Name holders to import and export domain contents and metadata, including any protected contacts, readers and groups, and profile provisioning data in an XML format.

9.4 Provisioning Performance Requirements. As well as supporting the above features, a TelHosting Provider **MUST** deliver a service with acceptable performance. The provisioning service **MUST** be responsive to the needs of Domain Name holders. TelHosting Providers **MUST NOT** exceed the maximum response and processing times specified below for the majority of requests using either an API SOAP interface or web-based system. The maximum response time for an API call **MUST NOT** exceed 500ms.

A TelHosting Provider **MUST** meet the performance requirements on the minimum, maximum and average times between requests that cause changes to a .tel TLD delegated zone being processed in the provisioning system itself and those changes being reflected in the Delegated Zone's name servers. These are specified in Section 5.3 of this document.

The following service levels apply to the operation of TelHosting services.

- (a) Performance

To load and render the registrant log-in page.

1. Load time for 3KB of pure HTML:
 - (i) The average load time for 3KB of pure HTML:
500 ms (averaged per 24 hour day).
 - (ii) The time below which 95% of all pure HTML pages of 3KB will be delivered:
1.5 seconds averaged per 24 hour day.
2. Average wait time for log-in response (measured from HTTP request dispatch until HTML response is fully received):

1.5 seconds (averaged per 24 hour day) for users with 20 or fewer domains.

To process other registrant actions.

3. Average wait time for single data manipulation action (measured from HTTP request dispatch until response screen HTML is fully received):

1.75 seconds (averaged per 24 hour day).

(b) Availability

Uptime for NSP Provisioning Service:

99.8% over a rolling one year period with no single outage greater than 4 hours duration. This excludes scheduled outages.

10. ADDRESS RECORDS

A TelHosting Provider's systems and provisioning tools **MUST NOT** allow the insertion of user-defined Address Records into .tel TLD delegated zones. A TelHosting Provider **MUST** allow for Address Records approved by the Sponsoring Organisation to be added to a delegated .tel TLD zone.

Appendix A

Contact Support in .tel

1. INTRODUCTION

To ensure that .tel domain name registrants are provided with a good service, the Sponsoring Organisation specifies the minimum level of support in provisioning (and in presentation and use of contacts) that will be populated in .tel domains. Programs that provision or operate on this data will be expected to provide these features.

Technically, communications contacts are stored within domains in the DNS using Naming Authority Pointer (NAPTR) resource records. Systems used to support or query the .tel TLD will need to help the user in provisioning and interpreting the communications contacts. This document lists the main features to be supported by these systems.

1.1 Specifications

The specification for NAPTRs is included in the IETF document set RFC 3401, RFC 3402, RFC 3403. These documents cover the “Distributed Delegation Discovery Service” (DDDS), with RFC 3403 in particular covering the overall syntax and use of NAPTR resource records. The variant of DDDS on which the .tel service is based is described in RFC 3761 - this specifies the “E2U” DDDS Application. More clarification and interpretation of these standards is given in draft-ietf-enum-experiences-07.txt.

This document covers the aspects not considered in these specifications and should be considered along with them. In particular, this document lists the services people can expect to use to populate their .tel domain names, and the extra elements and services that will be supported in .tel-compliant programs.

In the following text, presence of “MUST” indicates an element that it is mandatory to implement, while “SHOULD” indicates an element that must be supported unless there is an overwhelming reason not to do this in a particular context, and “MAY” indicates an element for which implementation and/or use is optional.

1.2 Document Structure

This document lists the Enumservices to be supported in Section 2. This is followed in Section 3 by descriptions of the additional “non-Standards Track IETF” Enumservices that have been adopted for use in the .tel TLD as a convenience to users. Section 4 covers the expected behaviour of client programs (either stand-alone or proxy web based) on receiving contacts using these Enumservices.

2. ENUMSERVICE SUPPORT IN .TEL

Any TelHosting Provider's Provisioning System, Web Proxies, and client programs designed to operate with .tel MUST recognise the following Enumservices. Provisioning Systems SHOULD allow provisioning of all of these, with the exception of those mentioned in Sections 2.1.1 and 2.2, where support MUST be provided. In the case of clients, these are of course dependent on the local availability of features capable of supporting the specified communications methods. However, these SHOULD (at least) recognise the following listed Enumservices and not treat their presence as an error.

Proxy web clients SHOULD support these services, and provide clickable links (as further described in Section 3, and the "Web-based Contact Handling" table). Whether or not a computer on which a browser (requesting the web proxy results) operates has external programs that support these services will of course vary, and so the result of clicking on these links will be computer-dependent.

2.1 IETF Standards Track Enumservices

These are those listed on the IANA Number Registry's web site, at least including the following:

- sip
- h323
- voice:tel
- sms:tel
- ems:tel
- mms:tel
- sms:mailto
- ems:mailto
- mms:mailto
- email:mailto
- web:http, web:https
- ft:ftp
- fax:tel

Enumservices are listed on the IANA web site. See <<http://www.iana.org/assignments/enum-services>>.

2.1.1 Non-Terminal NAPTR Support

As a core element of the DDDS standards and thus the "E2U" application on which .tel is based, non-terminal NAPTRs (NTNs) are mandatory to implement. The .tel TLD supports provisioning and use of sub-domains to partition the information published by domain owners. For this reason, it also makes extensive use of non-terminal NAPTRs to "point" to these sub-domains. All clients (stand alone or web based) and all provisioning systems MUST implement support for non-terminal NAPTRs both internally and within the user interface they present to users.

2.2 Non-IETF Enumservices

These are the additional Enumservices that have been adopted for use in the .tel TLD. These are detailed in the next Section, but are summarised here.

2.2.1 Voice Over IP and Instant Messaging Enumservices

The following Enumservices indicate that this contact can be used to start a communications session including voice/video and Instant messaging with a user of typical services (such as AIM, Skype, and so on). The sub-type identifies the URI scheme of the system.

- x-voice:<system>
- x-im:system>

2.2.2 Protected Content Enumservice

As one element of support for protected contacts, both provisioning and client systems MUST support encrypted NAPTRs, as specified in Section 3.3 of this document and in the document “IANA Registration for Encrypted Enum”, available at <http://www.ietf.org/internet-drafts/draft-timms-encrypt-naptr-00.txt>, (or its successors).

- x-crypto:data:<csid>

2.2.3 Auxiliary/Descriptive Enumservices

These auxiliary Descriptive Enumservices are “purely descriptive” Enumservices, used to label a containing NAPTR with textual information that can be presented to a querying user. They cannot exist alone in a NAPTR, but must be used with one of the Enumservices listed in the Sections above.

Descriptive Enumservices fall into two classes: Location Indicator Hints and Descriptive Labels. As the name implies, the Location Indicator Hint class is intended as hints to the location of a user, or that this URL involves a Premium Rate Service (and so, if contactable, use of this URL may cost the caller more than a normal call). Examples of this class are:

- x-mobile
- x-home
- x-work
- x-main
- x-transit
- x-prs

The Descriptive Label class is more flexible, and is intended merely for presentation to the user. The general syntax for this Enumservice is listed here. The <text> tokens indicate one or more strings that fulfil the limitations of an Enumservice type or sub-type (see RFC 3761) – the main limitation being that each text is a maximum of 32 characters in length, and includes only characters in the Alphabetic or Numeric sets, or the hyphen character (“-”).

- “x-lbl:” text *[":" text]

3. ADDITIONAL ADOPTED CONTACT SPECIFICATIONS

This Section describes the Enumservices (other than those meeting current IETF standards track specifications) that have been adopted for use in the .tel TLD. It gives further details and specification for those Enumservices listed in Section 2.2, and in particular the Enumservice(s) in Sections 2.2.2 and 2.2.3.

Note that unless indicated these specifications have not been condoned by or introduced to the IETF at this time. The IETF Enumservice registration process is in the process of change, and registrations for these elements will be re-considered once the new IETF Enumservice registration process is complete.

3.1 VoIP and IM Enumservices

These Enumservices imply that this contact is used for common VoIP/IM services (such as google or skype). By selecting this contact, the user would expect an appropriate program to run and to initiate contact with the person who has an account with this service. The sub-type indicates the particular service within which the associated URI exists; this holds the service-specific URL scheme (e.g. gtalk, ymsgr).

In these Enumservices, x-voice is used for all real time communication sessions other than Instant Messaging. Thus it indicates that a video and/or a voice session could be started by using the associated URI in the NAPTR holding this Enumservice. Conversely, x-im is used to start an Instant Messaging chat session with the user listed in the URI. Also note that most existing services allow the user to switch between video/voice and IM chats in mid-session, so that the Enumservice indicates merely the kind of session to start.

The URI generated from the enclosing NAPTR will be the one appropriate for the VoIP/IM service, so will be of the form skype:jamesbrown, gtalk:awebuser, or msnim:alive1.

- x-voice:aim
- x-voice:skype
- x-voice:gtalk
- x-im:aim
- x-im:icq
- x-im:ymsgr
- x-im:msnim
- x-im:xmpp

In addition, “legacy” Enumservices that have been used in other public contexts are still supported by the client programs and web proxies, and are treated as if they were the replacements shown:

+ x-skype:callto => x-voice:skype

3.2 Auxiliary Descriptive Enumservices

This class of Enumservices does NOT indicate the abstract Application or protocol to be used to process the URI contained in its NAPTR. Instead, it adds further descriptive information on the service this NAPTR represents.

An Auxiliary Enumservice is independent of the application and of the URI generated by the NAPTR that contains it.

The NAPTR holding an auxiliary Enumservice **MUST** contain at least one “active” Enumservice that indicates the treatment of the NAPTR’s generated URI; a NAPTR cannot include only Auxiliary Enumservices.

As mentioned above, there are two classes of such Enumservices, Descriptive Labels and Location Indicator Hints. These are described next, with examples of NAPTR services fields containing these Enumservices following those descriptions.

3.2.1 Descriptive Labels

This is an Experimental Enumservice. As such, the type starts with the facet “X-”. This is also an auxiliary Enumservice.

The Enumservice is called “Label”, and the Type is “X-LBL”.

The subtype(s) is/are a set of text blocks, each of which is between 1 and 32 characters long, and can contain only ALPHA, DIGIT, or ‘-’ characters.

As this is an Auxiliary Enumservice, there is no intended service implied by its presence. The Intended action for this Enumservice is for the sub-type labels to be presented to the end user (and/or interpreted by a suitable client program acting on his/her behalf).

It is suggested that any ‘-’ character (other than that in the initial “X-” facet) **MAY** be replaced by Linear White Space Character(s) or other token separator character(s) when the text is presented.

If there is more than one subtype present within this Enumservice, the text these contain **SHOULD** be processed in a left-to-right order. Thus “+x-lbl:Foo:Bar” could be presented:

```
Foo
Bar
```

If there is more than one such Enumservice, the text these contain should be handled in a left-to-right order. Thus “+x-lbl:one+x-lbl:two:bar” could be presented:

```
one
two
bar
```

Note that it is recommended that the length of labels should be limited where possible. There is a finite limit to the overall length of the services field within a NAPTR (254 octets). However, there are circumstances in which the length of this field should be restricted where possible. For example, in a protected NAPTR, the service field is encrypted along with the rest of the NAPTR. As the total length of the protected content is limited, the maximum length of the REGEXP field will depend on the Services field and any labels that contains.

3.2.2 Location Indicator Hints

Members of this group are Experimental Enumservices. As such, in each case the type starts with the facet “X-”. They are also Auxiliary Enumservices. There is no intended “active” service implied by the presence of one or more of this set of Enumservices.

The set of these services consists of:

- x-mobile
- x-work
- x-main
- x-home
- x-transit
- x-prs

The intended action for these Enumservices is that they can be interpreted by a suitable client to indicate that this NAPTR is associated with a means of communication available when the publishing user is mobile, when that user is at work, as the main contact, when that user is at home, when that user is in transit, or that this contact will involve a premium rate call.

The client program may choose to select an appropriate indication when presenting this contact to a user. These indicators differ from the Label Enumservices (described above) in that the text need not be presented literally. Instead the client may interpret the hint and either act on this or present the contact with its own choice of indication. Thus x-mobile might be presented to the user with a specific Icon variant, or with the label “Handyphone number:”, or other appropriate indications.

3.2.3 Auxiliary Enumservice Examples

- E2U+voice:tel+x-work
- E2U+email:mailto+x-home
- E2U+voice:tel+x-prs
- E2U+web:http+x-lbl:my-blog
- E2U+email:mailto+x-lbl:work-mail
- E2U+voice:tel+x-lbl:my-company:london-office:secretary
- E2U+voice:tel+x-lbl:voicemail
- E2U+voice:tel+x-lbl:away
- E2U+sms:tel+x-lbl:home:dect-phone
- E2U+web:http+x-lbl:my-profile
- E2U+x-voice:skype+x-lbl:Desk-PC
- E2U+x-im:aim+x-lbl:my-aim-account

Full examples:

IN	NAPTR	10	49	“u”	“E2U+voice:tel+x-lbl:paris-hilton-line+x-prs” !“^.*\$!tel:+44904999999!”
IN	NAPTR	10	50	“u”	“E2U+web:http+x-lbl:my-yahoo-profile” !“^.*\$!http://members.yahoo.com/interests?.oc=t&.kw=myuserid&.sb=1!”
IN	NAPTR	10	51	“u”	“E2U+web:http+x-lbl:my-yahoo-status” !“^.*\$!http://opi.yahoo.com/online?u=myuserid&m=g&t=2!”

```
IN NAPTR 10 52 "u" "E2U+sip+x-work+x-lbl:my-video-phone"
!^.*$!sip:myuserid@example.net!"
IN NAPTR 10 53 "u" "E2U+email:mailto+x-main+x-lbl:primary"
!^.*$!mailto:myworkuserid@example.com!"
```

Notes:

- It is recommended that the length of labels should be limited where possible. For example, in a protected NAPTR, the service field is encrypted along with the rest of the NAPTR. As the total length of the protected content is limited, the maximum length of the REGEXP field will depend on the Services field and any labels that contains.

3.3 Protected Contacts

3.3.1 Definitions

- Protected Contact

A protected contact is a contact that is encrypted so that it can only be read and used by a chosen person. The contact (held in a NAPTR) is published in DNS according to the document “IANA Registration for Encrypted Enum”, available at <http://www.ietf.org/internet-drafts/draft-timms-encrypt-naptr-00.txt>, (or its successors).

- Reader

Readers are people for whom a domain owner has agreed to publish protected private contacts in dedicated sub-domains.

- Publisher

Publishers are domain owners who populate dedicated sub-domains with their choice of protected contacts for individual readers. Each reader is assigned his/her own dedicated sub-domain within the owner’s domain into which protected contacts for that individual will be stored.

- Publisher Store

A list, maintained in the Sponsoring Organisation (SO) Systems, containing the domain names of publishers who have accepted this individual as a reader, together with the dedicated sub-domains into which those publishers have chosen to store protected contacts for this reader. It is used internally by the SO system web proxy, by remote client programs and (for .tel domain owners) by the registrant’s TelHosting Provider’s Provisioning System.

- Reader Store

A list, maintained in the Provisioning System operated by the domain owner's TelHosting Provider, containing the individuals that this publisher has accepted as readers, together with the DNS domain in which those individual reader's public keys are stored. It is used internally by the TelHosting Provider's systems and by remote client programs acting for the registrant.

3.3.2 Telnic support for Protected Contacts

Telnic has funded development of all of the components need for protected contacts. From a developer or user's perspective, this infrastructure includes client programs for various devices and computers, a web proxy client, the Sponsoring Organisation web site and service, and the TelHosting software used by accredited TelHosting Providers. All of these systems working together support publication and reading of protected contacts, and initiation of relationships between readers and publishers.

As mentioned, the protected contacts are published in DNS as specified in the document "IANA Registration for Encrypted Enum", available at <http://www.ietf.org/internet-drafts/draft-timms-encrypt-naptr-00.txt>, or its successors. All Telnic systems are designed to use the cyphersuite value '8210' from this specification. This means that these system use 1024-bit RSA encryption, with PKCS#1.5 padding and no additional cryptographic hash to protect contacts. By definition, protected contacts encrypted for a reader will be processed using his or her 1024 bit RSA Public key. To decrypt those NAPTRs, the reader will have to use the associated RSA private key.

It is assumed that the reader's Public key is published in a dedicated domain within DNS. It is also assumed that the domain owner stores protected contacts for a given reader in a dedicated sub-domain known to them both. For the scheme to work, the publisher needs to know the domain in which the reader's Public key is stored, before protected contacts can be published for that individual. Likewise, the reader needs to know the dedicated sub-domain into which these protected contacts will be published by a domain owner, in order to find the protected contacts to be decoded and read by the user. Passing this needed information between reader and publisher implies a message exchange. This is similar to the "friending" process common to existing social networks.

- SO Member System

The Sponsoring Organisation (SO) systems have been designed to facilitate the process. Individuals (regardless of whether or not they own .tel domains) can register with the SO member system. When an individual registers, this SO member system will create an account for him or her. This account includes credentials for the member to log into the system's web site, and other credentials to be used by client programs acting for him or her to connect to the system's web services). The system will also create a Public/private key pair, and will publish the Public key in a dedicated domain under its management for that member.

- SO Messaging Sub-system

The SO member system also includes a messaging sub-system by which individual members can send “friend requests” to participating .tel domain owners, and by which those domain owners can send “friend responses” back. This messaging sub-system is accessible to all members. These messages can be sent and received via the SO web site (specifically the web proxy client pages), via the client programs running on the member’s mobile devices or PC, and via the web pages of the TelHosting system operated by the domain owner’s TelHosting Provider.

Using these systems, the individual member can send and receive the “friending” messages needed to initiate a new reader and publisher relationship without having to deal with the detailed mechanisms used to achieve protected contacts. As a result, arranging this relationship is very similar to the usual “friending” process found on social networking sites. The components have already been designed to handle the complexity for the SO members.

4. CLIENT PROCESSING OF CONTACTS

This Section covers the way that stand alone or web-mediated client programs are expected to handle Contacts that they retrieve from .tel domains. By implication, TelHosting Providing systems are expected to provide a user interface by which a domain owner can provision the contacts (as shown in the following tables, with the Service and NAPTR URI fields being populated within appropriate NAPTR records).

Whilst the descriptions that follow are exemplary of the client programs and web servers already developed, it is expected that independent client programs will behave in the same way. When they present contacts to their users, selecting one of these contacts SHOULD initiate an external program designed to support the selected URI and start an appropriate communications session.

4.1 Telnic-funded client support

Telnic has funded development of a number of different client applications to ensure that anyone with network access can use .tel domains. The current list of Telnic-funded stand alone client programs is:

- Plug-in program for Microsoft Outlook, integrated with Outlook address book.
- Program for the Blackberry that integrates with the Blackberry Address Book.
- Client program for Microsoft Mobile cell phones

Web server mediated clients have also been developed for Telnic. In particular, a proxy web server has been developed that receives web requests for registered .tel domains, queries those domains in DNS, and presents a list of the available contacts. This is integrated as part of the Sponsoring Organisation systems and is operated by the Sponsoring Organisation as a service to the .tel community.

In the table of examples shown next, the client is expected to process NAPTRs that include Enumservices as shown, and with the URL generated from the REGEXP field in the form shown in the NAPTR URI column.

The Outlook plug-in program is designed with an open architecture. This means that whilst it will initially have support for voice:tel (telephone calls), IM and video calls using Skype, MSN, AIM, and Yahoo! services, web links (using HTTP or HTTPS URLs) and (of course) email, support for other communications sessions can be easily added.

The Blackberry and other cell phone based client programs are limited only by the communications support included in the cell phones themselves. Thus, the initial supported feature set for the Blackberry client includes support for email, web links, telephone calls, and (for recent versions of the Blackberry Operating System), SMS.

4.1.1 Client-based handling of Contacts

In the following table, the SERVICE and NAPTR URI columns show the expected Enumservice and generated URI values from received NAPTRs. The Launch URI column shows the URI value that is recognised by external programs, and the Supported Clients

column lists the service-specific programs that have been tested and shown to operate with these URIs. Other methods of running external programs are covered at the end of this Section.

Macintosh (Mac OSX) Contact Handling

Service	NAPTR URI	Launch URI	Supported Clients
x-im:aim	aim:freddy	aim:goim?screenname=freddy	iChat AOL Messenger Adium
x-voice:sip, voice:sip, sip	sip:freddy@sip.com	n/a - AppleScript	EyeBeam, X-Lite
voice:tel	tel:+441794833000	n/a - Bluetooth dialler	Bluetooth phone
		n/a - AppleScript	EyeBeam, X-Lite
		Skype:+441794833000?call	Skype
x-im:skype	skype:freddy	Skype:freddy?chat	Skype
x-voice:skype	skype:freddy	skype:freddy?call	Skype
email:mailto, sms:mailto	mailto:freddy@foo.com	mailto:freddy@foo.com	(System)
ft:ftp	ftp://ftp.foo.com/	ftp://ftp.foo.com/	(System)
web:http,	http://www.foo.com/	http://www.foo.com/	(System)
web:https	https://www.foo.com/	https://www.foo.com/	(System)
sms:tel, ems:tel, mms:tel	tel:+447794833000	n/a - Bluetooth SMS sender	Bluetooth phone

Windows Contact Handling

Service	NAPTR URI	Launch URI	Supported Clients
x-im:aim	aim:freddy	aim:goim?screenname=freddy	AOL Messenger
x-im:ymsgr	ymsgr:freddy	Ymsgr:sendim?freddy	Yahoo! Messenger
x-im:msnim	msnim:freddy	Msnim:freddy	MSN Messenger
x-voice:sip, voice:sip, sip	sip:freddy@sip.com	n/a - cmd - dial=freddy@sip.com	X-Lite
voice:tel	tel:+441794833000	n/a - Bluetooth dialer	Bluetooth phone
		n/a - cmd - dial=00441794833000	X-Lite
		Skype:+441794833000?call	Skype
x-im:skype	skype:freddy	Skype:freddy?chat	Skype
x-voice:skype	skype:freddy	Skype:freddy?call	Skype
email:mailto,	mailto:freddy@foo.com	mailto:freddy@foo.com	(System)

sms:mailto			
ft:ftp	ftp://ftp.foo.com/	ftp://ftp.foo.com/	(System)
web:http,	http://www.foo.com/	http://www.foo.com/	
web:https	https://www.foo.com/	https://www.foo.com/	(System)
sms:tel, ems:tel, mms:tel	tel:+447794833000	n/a - Bluetooth SMS sender	Bluetooth phone

Web-based Contact Handling

Service	NAPTR URI	Launch URI/Link Generated	Supported Clients
x-im:aim	aim:freddy	aim:goim?screenname=freddy	AOL Messenger
x-voice:aim	aim:freddy	- none -	- none -
x-im:ymsg	ymsg:freddy	Ymsg:sendim?freddy	Yahoo! Messenger
x-voice:ymsg	ymsg:freddy	- none -	- none -
x-im:msnim	msnim:freddy	Msnim:chat?contact?freddy	MSN Messenger
x-voice:msnim	msnim:freddy	Msnim:chat?voice?freddy	MSN Messenger
x-voice:sip, voice:sip, sip	sip:freddy@sip.com	sip:freddy@sip.com	
voice:tel	tel:+441794833000	callto:+441794833000	Skype
x-im:skype	skype:freddy	Skype:freddy?chat	Skype
x-voice:skype	skype:freddy	Skype:freddy?call	Skype
email:mailto, sms:mailto	mailto:freddy@foo.com	mailto:freddy@foo.com	(System)
ft:ftp	ftp://ftp.foo.com/	ftp://ftp.foo.com/	(System)
web:http,	http://www.foo.com/	http://www.foo.com/	
web:https	https://www.foo.com/	https://www.foo.com/	(System)
sms:tel, ems:tel, mms:tel	tel:+447794833000	- none -	- none -

Contact handling - other methods

In the tables above, where the Launch URI column shows n/a, this indicates that other methods of starting a communication session can be used. For example, it is possible to send commands to an external bluetooth connected cell phone to trigger it to dial a telephone number. Also, where there are Client programs that support these services, but they do not respond to a system call using a Launch URI (i.e. the program has not registered itself as a URI handler with the operating system), then other methods may be used (for example, on a Macintosh, using an Applescript to start the external program). Similarly, Windows allows “command line” instructions, and this can be used to run programs on that platform; these are shown in the tables above as “cmd – x”.

In addition, a number of services have web-based solutions. For example, Gmail, Hotmail and Yahoo! Mail can be accessed via web browsers, and so could be used to send email

messages to recipients, with the following “Launch URLs”. If so configured, the client program could convert the contact’s URL (mailto:freddy@foo.com” in these examples) into the following launch URLs, and pass these to the local web browser:

http://mail.google.com/mail/?view=cm&fs=1&tf=1&to=freddy@foo.com&fs=1	Gmail
http://hotmail.msn.com/secure/start?action=compose&to=freddy@foo.com	Hotmail
http://search.yahoo.com/search?p=%21mail+freddy@foo.com	Yahoo! Mail

5. AUTO-PROVISIONING SUPPORT USING CONTACTS

This Section outlines the process by which .tel client software acting for a domain owner may automatically configure TelHosting settings based on the domain contents. The motivating factor behind this feature is that users may not be comfortable provisioning TelHost system connection information into a freshly installed .tel client program, particularly if this involves typing in long and complicated SOAP URLs to run TelHost-related actions.

Instead, it would be convenient for a domain owner to type in just the domain name he or she owns, and to have the settings (except for the TelHost account password, of course) configured automatically by the client program.

To this end, the Telnic-funded client programs (and TelHosting software) will look at contacts within two reserved sub-domains within a .tel domain name. These sub-domains are ‘_soap._nsp’ and ‘_web._nsp’. The contacts expected in these sub-domains are shown below, and will allow the client programs to find the soap end point and the (human readable) web pages respectively. In this example, the TelHosting system hosts the example.tel’s zone, and will provision these contacts as shown:

```
$ORIGIN example.tel.  
  
.      IN SOA ...  
  
.      IN NS ...  
  
_soap._nsp  
  
      IN NAPTR 10 50 “u” “e2u+web:https+x-lbl:1-3”  
          “!^.*$!https://exampletelhost.com:8254/action!” .  
  
      IN NAPTR 10 51 “u” “e2u+web:https+x-lbl:1-1”  
          “!^.*$!https://exampletelhost.com:8253/action!” .  
  
_web._nsp  
  
      IN NAPTR 10 50 “u” “e2u+web:https”  
          “!^.*$!https://www.exampletelhost.com/login!” .
```

In all cases, the TelHosting Provider is advised that the sub-domain that the clients will expect is “_soap._nsp” for the web service end point, and “_web._nsp” for the ‘human readable’ web pages.

The client programs will look for contacts in these sub-domains when they are given the .tel domain name. If these are not found (or the contacts within them are not usable) then the client program will inform the end user that auto-provisioning is not available, and ask for the settings to be entered manually.

Note that the ORDER/PRIORITY reflects the TelHosting Provider’s preference. The client may well have its own preference, based on the API version supported. Thus when a client

program finds an appropriate contact, the client program looks for an x-lbl auxiliary Enumservice, and if detected will match the x-lbl content (if present) against its own capabilities.

Appendix B

TXT Support in .tel

1. INTRODUCTION

This document describes the usage of TXT records within .tel domains.

The TXT resource record type is defined in the main DNS standard (RFC 1035). TXT records can be stored in the DNS and hold a series of strings, each of which is less than or equal to 255 octets in length. Multiple TXT records can exist in a single domain, with all available TXT records being returned in response to a query. The order in which these records are returned is not guaranteed.

TXT records are used in .tel domains to store non-contact related information about the registrant. Generic descriptions or messages can be displayed as well as more structured data such as addresses or the category of business (for corporate registrants). These records can also be used for “system messages” – data intended as a “hint” to the recipient program, and not normally for presentation to the user.

1.1 Generic data in TXT Records

Where a TXT record is returned and the first (or only) string in that record does **not** hold either of the reserved identifier patterns shown below (in Sections 1.2.1 and 1.2.2), it is treated as holding a generic set of data to be displayed to the end user in the normal way. Within .tel, clients (either stand-alone or web proxy mediated) are expected to be able to handle TXT records that have multiple strings, and to present these accordingly to the end user. Similarly, provisioning systems are expected to allow the registrant to populate TXT records into his or her domain, and to allow each of these TXT records to hold multiple strings.

1.2 Structured Data within TXT Records

There are two forms of structured data that are given special processing rules in .tel domains. These are Structured Keywords, and Structured System Messages. In both cases, the initial string holds a specific identifier pattern. This is informally named the “*magic identifier*” and should be used by clients to determine whether the TXT record is one of these special cases, or instead should be treated as a generic TXT record. The second string will hold a version value, expressed as a decimal numeric.

The subsequent strings in the TXT record are interpreted according to the structured message type; in general, these are arranged in pairs, with the first of the pair holding the data type, and the second string in that pair holding the data value. There will be at least one pair of such type and data strings. Beyond this structure, the formal limit is the maximum size of a DNS resource record. In practice, of course, creating a massive TXT record (or set of TXT records) is unwise; the DNS is optimised for relatively short messages, and not all networks react correctly to excessively long DNS messages.

1.2.1 Structured Keywords record

A Structured Keywords record begins with a special value in its first string; this is “.tkw” (short for .tel keywords). Strings after the next (version number) string consist of keyword (type, value) pairs. The types of keywords are listed in Section 3.1.

1.2.2 Structured System Message record

This type of structured data uses the TXT resource record, and has similarities to the Keyword form described above. The difference lies in the intended use of the contained data and the identifier by which this kind of content is indicated. The expectation is that this TXT record is intended to influence the client behaviour, and is NOT intended for presentation to the end user.

A client program receiving a TXT record in which the first string is exactly “.tsm” (short for .tel system message) should interpret the strings following the version in this TXT resource record as a structured System Message according to this specification.

System message types are covered in Section 3.2.

1.2.3 Version matching

When evaluating its capability against that required to understand the received structured record format, the client program will consider the next string in the TXT record after the *magic identifier* – this contains the version value. The client program will be expected to be capable of handling a certain major version of this specification. To compare its capability with that indicated as required in the TXT record, it should examine the version string. This version string should be padded with “0” characters to the right if it has less characters than the client’s internal capability value. Conversely, the client’s internal capability value should be right-padded with “0” characters if it is shorter than the version value in the received structured data record.

Once this is done, the client should treat both its internal capability string and the extended TXT record’s version string as if they were integer values, and compare them numerically. If the client program’s capability is higher or equal to the version value, then this client can be expected to understand the rest of this structured data. If the first digit in the internal capability string is the same as that in the TXT record’s version string, then there is major version compatibility; this means that the client will be able to parse the TXT record content, even if it does not recognise the values of the fields. If the value in the version string is higher than in the client’s capability, then the client cannot make this assumption, and must discard the TXT record.

For this current version of the specification, provisioning systems that populate .tel domains with structured data records must use the value “1” as the version string in these records.

2. .TEL TXT RECORD FORMAT

There is no guarantee of the order in which TXT records will be delivered in a DNS response. Registrants (and the provisioning systems they use) cannot assume the order in which these TXT records will be processed by a client program. However, strings that exist within a TXT record will be processed in a left to right order, and advantage can be taken of this by registrants: the order of strings provisioned within a TXT record can and will be maintained by client programs.

For a generic TXT record, the strings it contains will be presented to the user in the left-to-right sequence in which they appear in the record.

Where the TXT record contains structured keywords, a similar approach is taken. In principle, keywords are independent of one another. By grouping keywords together in a single TXT record, a logical relationship between these keywords is established. For example, a TXT record with an initial keyword type "*postalAddress*" may contain the subsequent keyword types "townCity", "postalCode", and "stateProvince". The value of the postal address keyword type denotes a "label" that can be used to differentiate between different address, e.g. "Home", "Work", "School". The values for the subsequent keywords will normally be displayed to the user in the order in which they appear within the TXT record. This allows a postal address to be presented in the "natural form" as chosen by the registrant, rather than requiring the client program to collate and interpret these values before display.

Only a single structured system message is permitted within a TXT record. However, registrants must take care not to have conflicting system message records within a domain. As the order in which TXT records are delivered is indeterminate, contradictory system messages are unwise (as the eventual interpretation made by a querying client program cannot be determined).

2.1 Parsing

Parsing the structured data records should be performed on a per-TXT record basis. The general form for structured data records is shown here:

```
<magic> <version> <primaryType> <primaryValue> [ <secondaryType>
<secondaryValue> ] ...
magic = ".tkw" / ".tsm" - TXT record contains keywords/system message
version = 1*(0..9) - examples: "1", "11", "20"
```

For structured keywords, the TXT record may contain more than one keyword type/data pair. In the specific case of the *pa* and *bpa* keywords, subsequent keywords are expected in the same TXT record (forming a complete postal address), and will be processed and presented in the order in which these appear in that TXT record.

In the case of system message records, this version of the specification allows only one system message per TXT record. Thus there will be a single pair of type/value strings in such a record.

2.1.1 Lazy Parsing and Presentation of Structured Keywords

When a client receives a record that holds keywords, the record can be parsed by considering the initial keyword type and value, and then taking each subsequent keyword in turn. The

types of these subsequent keywords can be discarded, and their keyword values can be simply concatenated (with a suitable separator between each of the strings). The result can then be presented to the user with no further interpretation; in the majority of cases, the initial keyword type will give the user enough of a semantic “hint” to understand the context and meaning of the record.

3. SPECIAL STRINGS IN TXT RECORDS IN .TEL

3.1 Keyword types

The keyword types and values in the following tables are deliberately loosely defined to allow extension and innovation by the community. The suggested keyword types in this document provide a “core” to which others can be added in the future. Where possible the keyword types should remove the need for structured values. For instance, separating out keyword types for the address components removes the need to parse comma delimited addresses.

The keywords listed here are semantically broken down into two categories: Individual and Corporate. There is no restriction on mixing the types when provisioning, but it makes sense to logically differentiate between the two when implementing separate interfaces for White and Yellow pages or when presenting these records to a user who has asked for information on a queried domain.

As an example of the difference in usage between the corporate keywords and individual keywords: Individuals will have the opportunity to populate the “organisation” field with the name of their employer – should they wish to do this.

So “Adam Smith”, employee of Telnic, would put “Telnic Limited” in the “Organisation” field. Conversely, Telnic would populate the field “Business Name” with “Telnic Limited” and leave “Organisation” blank.

3.1.1 Character Sets and Language preferences

The keyword types listed below are all in the US-ASCII range. Short-hand equivalents to the keyword types are shown inside parentheses and in italics within the following tables. Where possible, it is recommended that these short-hand forms be used in the keyword type strings when provisioning keywords within a TXT record. To limit the potential for misrepresentation, it is also recommended that these type values be provisioned into the TXT record, (regardless of the language preference of the registrant or potential readers), rather than creating new language-specific keyword types. Client programs receiving these TXT records should be able to convert the types into a “local” equivalent for presentation, and provisioning systems should be able to map local keyword type names into these “canonical forms”.

It is assumed that the contents of the keyword value strings are in the Universal Character Set, and are encoded in UTF-8. Registrants should be aware that potential readers of these keywords may not share the same language or cultural preferences.

This is especially important when provisioning corporate keywords such as Business Area and Business Sub-Area. If the registrant wants a multi-lingual audience to know that it is involved in shoe repairs, then the language specific value “Cobbler” may not be appropriate for the *bsa*.

3.1.2 Individual keywords

These keywords relate to individuals, both commercial and non-commercial. The “short-hand” version is shown in italics.

- salutation (*s*)..... e.g. “Mr”, “Mrs”, etc
- commonName (*cn*)..... e.g. “Adam J. Smith”
- firstName (*fn*)..... e.g. “Adam”
- lastName (*ln*)..... e.g. “Smith”
- nickName (*nn*)..... e.g. “Ade”
- date of Birth (*dob*)..... e.g. “20/03/1966”¹
- gender (*g*) e.g. “Male” or “Female”
- maritalStatus (*ms*)..... e.g. “Married”, “Single”, etc
- postalAddress (*pa*) e.g. “Favourite restaurant” “a1”
“8 Wilfred Street” “tc” “London”
“pc” “SW1E 6PL” “c”, “UK”
- addressLine1 (*a1*)..... e.g. “8 Wilfred Street”
- addressLine2 (*a2*)..... e.g. “Victoria”
- addressLine3 (*a3*)..... e.g. “Westminster”
- townCity (*tc*) e.g. “London”
- stateProvince (*sp*)..... e.g. “Hampshire”
- postalCode (*pc*) e.g. “SW1E 6PL”
- country (*c*)..... e.g. “Scotland”
- latitudeLongitude (*ll*) e.g. “ 52° 11’ 1.55” N / 0° 5’
16.37” W “²
- organization (*o*)..... e.g. “Telnic Limited”
- department (*d*)..... e.g. “IT”
- jobTitle (*jt*)..... e.g. “Chief Rocket Scientist”
- hobbiesInterests (*hi*)..... e.g. “Scuba Diving”

¹ NB: an appropriate date format should be suggested or enforced for effective indexing.

² Note that this value includes the degree character – this character (u+00B0) is represented by two bytes in UTF-8; ‘C2 B0’.

- freeText (*ft*) e.g. “Selfless, innovating, trustworthy, red hair”

3.1.3 Corporate Keywords

These keywords extend those relating to individuals and pertain to businesses and corporate entities. The short-hand version is again shown in italics.

- businessName (*bn*) e.g. “Marie’s Marriage Emporium”
- businessPostalAddress (*bpa*)..... e.g. “London Office” “a1” “8 Wilfred Street” “tc” “London” “pc” “SW1E 6PL” “c” “UK”
- businessArea (*bar*) e.g. “Weddings”
- businessSubArea (*bsa*)..... e.g. “Dresses, Flowers, Venues”
- serviceArea (*sa*) e.g. “Hertfordshire, Essex, Cambridgeshire”

3.2 System Message Types

At present, only one Structured System Message type is defined. This is the system message type “pddx”. This indicates that private data does not exist within the containing .tel domain. The value string will hold either “1” or “0”, indicating respectively that private data is absent, or that there may be private data in this domain.

Clients use this indication as they choose. As an example, the Telnic-developed web proxy client will disable the “friend” UI elements when presenting queried .tel domains that include a TXT record with this system message. The rationale for this choice is that, If there is no private data published in this .tel domain, then there is little point in sending a friend request message to the domain owner.

3.3 Full Examples

Full examples:

IN	TXT	“Fun Contacts” “” “Life outside work”
IN	TXT	“.tkw” “1” “o” “Telnic Limited”
IN	TXT	“.tkw” “1” “s” “Mr” “fn” “James” “fn” “Fenimore” “ln” “Cooper” “jt” “Technical Author” “g” “male” “dob” “15/09/1789”
IN	TXT	“.tkw” “1” “pa” “Where I work”
IN	TXT	“.tkw” “1” “bpa” “Telnic South” “a1” “8 Wilfred Street” “a2” “Victoria” “tc” “London” “pc” “SW1E 6PL” “c” “UK”
IN	TXT	“.tsm” “1” “pddx” “1”