DRINKS	S. Channabasappa, Ed.	
Internet-Draft	CableLabs	
Intended status: Informational	May 3, 2010	
Expires: November 4, 2010		

TOC

DRINKS Use cases and Protocol Requirements
draft-ietf-drinks-usecases-requirements-02

Abstract

This document captures the use cases and associated requirements for interfaces that provision session establishment data into SIP Service Provider components, to assist with session routing. Specifically, the current version of this document focuses on the provisioning of one such element, termed the registry.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
This Internet-Draft will expire on November 4, 2010.

Copyright Notice

Table of Contents

---

1. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).
This document reuses terms from [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) (e.g., SIP) and [RFC5486] (Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," March 2009.) (e.g., LUF, LRF). In addition, this document specifies the following additional terms.

> **Registry:** The authoritative source for provisioned session establishment data (SED) and related information.
>
> **Local Data Repository:** The data store component of an addressing server that provides resolution responses.
>
> **Destination Group:** A set of public identities that are grouped together to facilitate session setup and routing.
>
> **Public Identity:** A generic term that refers to a telephone number (TN), an email address, or other identity as deemed appropriate,

such as a globally routable URI of a user address (e.g., mailto:john.doe@example.net).

Routing Group: A grouping of SED records.

Authoritative SSP or Entity This refers to the carrier-of-record, for a public identity or TN Range.

Non-authoritative SSP or Entity This refers to the transit provider for a public identity or TN Range.

---

2. Overview

TOC

The SPEERMINT WG specifies Session Establishment Data, or SED, as the data used to route a call to the next hop associated with the called domain's ingress point. More specifically, the SED is the set of parameters that the outgoing signalling path border elements (SBEs) need to establish a session. See [RFC5486] (Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," March 2009.) for more details.

The specification of the format and protocols to provision SED is a task taken up by the DRINKS WG. The use cases and requirements that have been proposed in this regard are compiled in this document.

SED is typically created by the terminating SSP and consumed by the originating SSP. To avoid a multitude of bilateral exchanges, SED is usually shared via intermediary systems - termed Registries within this document. Such registries receive SED via provisioning transactions from other SSPs, and then distribute the received data into Local Data Repositories. These local data repositories are used for call routing by outgoing SBEs. This is depicted in Figure 1 (General Diagram).

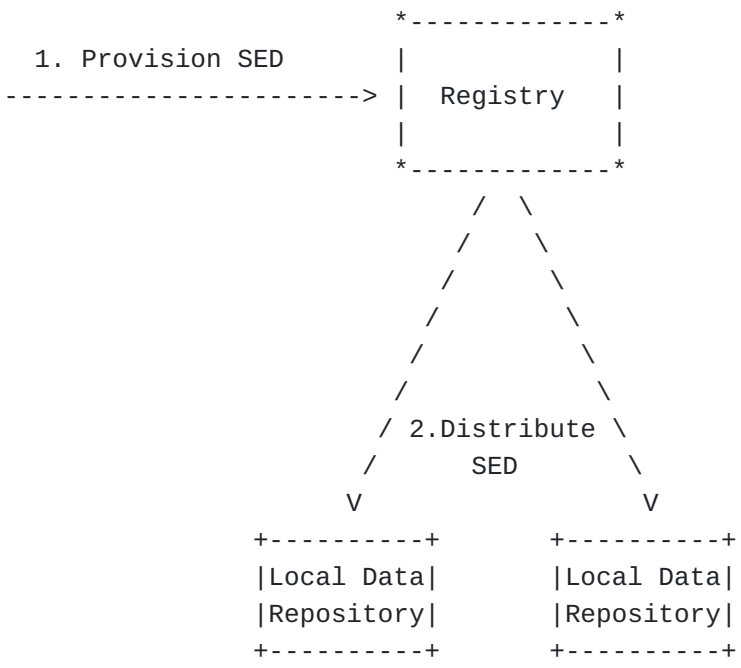

Figure 1: General Diagram

In this version of the document, we primarily address the use cases and requirements for provisioning registries. Future revisions may include data distribution. The resulting provisioning protocol can be used to provision data into a registry, or between registries. This is depicted in Figure 2 (Functional Overview).

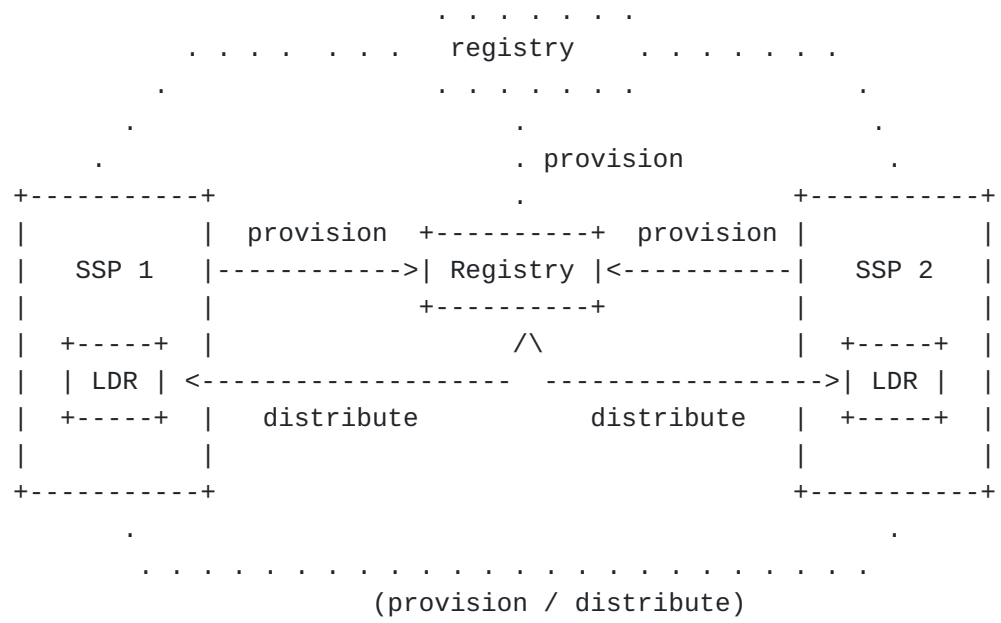

Figure 2: Functional Overview

The following is a summary of the proposed responsibilities for Registries and Local Data Repositories:

- *Registries are the authoritative source for provisioned session establishment data (SED) and related information.

- *Local Data Repositories are the data store component of an addressing server that provides resolution responses.

- *Registries are responsible for distributing SED and related information to the local data repositories.

In addition, this document proposes the following aggregation groups

with regards to SED (refer to the use cases in Section 3.1.1.3 (Category: Data Aggregations) for the rationale):

*Aggregation of public Identifiers into a destination group.

*Aggregation of SED records into a Routing Group.

The above aggregations are illustrated in Figure 3 (Data Model Diagram).

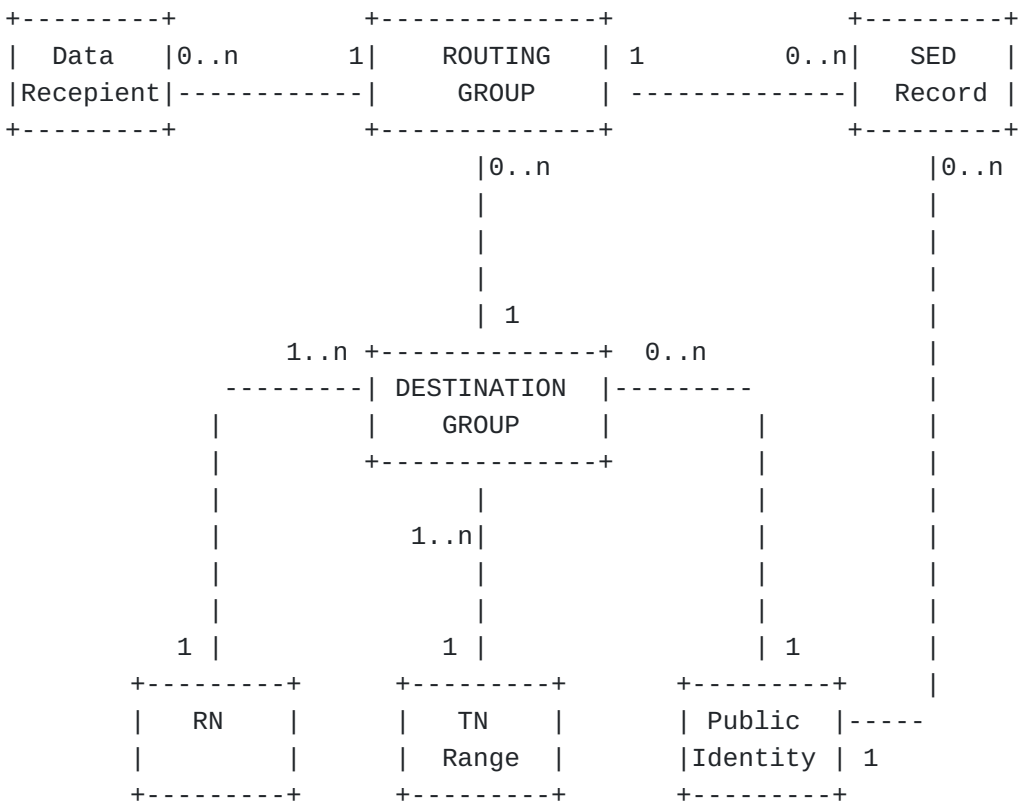

Figure 3: Data Model Diagram

Additional clarifications follow:

- A routing group is associated with zero or more SED Records; NAPTRs and other SED record types associated with routes are not user or TN-specific. For example the user portion of a NAPTR regular expression will be "\1".

- A routing group is associated with zero or more peering organizations to control visibility or access privileges to that routing group and the destination groups they expose.

- A data recipient group contains zero or more data recipients to facilitate the allocation of access privileges to routing groups.

---

3. Use Cases and Requirements

TOC

This section presents the use cases and associated requirements.

3.1. Registry Provisioning

TOC

This Section documents use cases related to the provisioning of the registry. Any request to provision, modify or delete data is subject to authorization. However, the act of authorization is considered out of scope within this document.

3.1.1. Use Cases

TOC

The use cases are divided into the following categories - different provisioning options, options for provisioning SED data, administration, and number portability.

3.1.1.1. Category: Provisioning Options

TOC

UC PROCESS #1 Real-time provisioning: once a registry is established events may occur that necessitate SSPs to add, modify or delete data in the registry, in real-time, to maintain accuracy of the data. Examples of such events can be found in

other use cases within this document (e.g., identity related use cases).

UC PROCESS #2 Non-real-time or bulk provisioning: There are cases when a registry needs to be provisioned with bulk data sets, via an offline mechanism, as opposed to real-time provisioning requests. Examples include: when a new registry is established or when data is being restored from a backup.

3.1.1.2. Category: SED options

TOC

UC SED DATA #1 Inter-network SED: An SSP provisons SED records for a specific end-user, so that other SSPs can use this SED data to establish sessions intended with this end-user. The provisioning SSP can either be the carrier-of-record (direct peering), or a transit provider (indirect peering).

UC SED DATA #2 Intra-network SED: An SSP provisons SED records for a specific end-user, for use within the SSP's networks. This will allow internal signaling elements to establish sessions intended for this end-user. The provisioned SED is only distributed to specific local data repositories, and will probably differ from the SED provisioned for use by signaling elements from other SSPs.

UC SED DATA #3 Selective peering: While an SSP may provision the same SED records for all other SSPs, an SSP may also wish to provision different SED records for different SSPs (e.g., if they have different peering agreements).

UC SED DATA #4 LUF-only data: An SSP can choose to provison LUF-only data in the registry. A querying SSP that receives LUF-only data may need to rely on other mechanisms (e.g., [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) for domain-name based LUF) to obtain LRF information.

UC SED DATA #5 LUF and LRF data: An SSP can provison LUF- and LRF-data in the registry. In such cases, the querying SSP does not have to rely on mechanisms such as DNS (e.g., [RFC3263]

(Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.)) for routing information.

UC SED DATA #6 Target Domain as a resolvable Domain Name, administrative domain name, or both: The target domain pertaining to a public identity or TN Range can either be a DNS-resolvable domain name (i.e., via [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.)) or an administrative domain. An SSP may also wish to provision both sets of data, and the response is based on a default choice or the querying entity.

UC SED DATA #7 Target Domain as an administrative domain: The target domain for a public identity or TN Range can be an administrative domain. In such cases the resolution may be out of scope for this document.

UC SED DATA #8

UC SED DATA #9 EDITOR's NOTE: This use case seems to be a special case of LUF-only provisioning. Thoughts?

Provision an authoritative name server: An SSP maintains a Tier 2 name server that contains the NAPTR records that constitute the terminal step in the LUF. The SSP needs to provision an registry to direct queries for the SSPs numbers to the Tier 2. Usually queries to the registry should return NS records, but, in cases where the Tier 2 uses a different domain suffix from that used in the registry, CNAME and NS records may be employed instead.

3.1.1.3. Category: Data Aggregations

TOC

UC DATA #1 Aggregation of public Identifiers: The input key to a SED lookup is a public identifier. Since several public identifiers will potentially share similar (or identical) destinations, and hence similar (or identical) SED records, provisioning the same set of SED for millions of public identifiers is inefficient. Therefore, an aggregation mechanism to 'group' public identifiers is proposed. This aggregation is

termed as a 'destination group' in the proposed data model.

UC DATA #2 Aggregation of SED records: A complete set of session establishment data may consist of more than just one SED record. To be able to create and use the same set of SED records multiple times (without creating duplicates) an aggregation mechanism is required. This is termed as a 'Routing Group' in the data model.

3.1.1.4. Category: Administration

TOC

UC ADMIN #1 New authoritative additions: An SSP provisions a public identity or TN Range, as its authoritative entity (i.e., carrier-of-record).

UC ADMIN #2 New non-authoritative additions: An SSP provisions a public identity or TN Range, as a non-authoritative (i.e., transit) entity.

UC ADMIN #3 Authoritative modifications to existing entries: An SSP indicates that it is the authoritative entity for an existing public identity or TN Range. If the public identity or TN Range was previously associated with a different authoritative entity then there are two possible outcomes: a) the previous authoritative entity is disassociated, or, b) the previous authoritative entity is relegated to non-authoritative status. The choice may be dependent on the deployment scenario, and is out of scope for this document.

UC ADMIN #4 Non-authoritative modifications to existing entries: An SSP indicates that it is a transit provider for an existing public identity or TN Range. In such cases, this SSP is associated with the public identity or TN Range, in non-authoritative status.

UC ADMIN #5 Authoritative disassociation from existing entries: An SSP disassociates itself from a public identity or TN Range that it is authoritative for. If there are no other (non-authoritative) SSPs associated with this public identity or TN Range, then the public identity may be deleted.

UC ADMIN #6

Non-authoritative disassociation from existing entries: A SSP disassociates itself from a public identity or TN Range that it is linked with, as a non-authoritative entity. If there are no other authoritative or non-authoritative entities associated with this public identity or TN Range, the public identity may be deleted.

UC ADMIN #7 Deletion of existing public identity or TN Range: A public identity (or a TN range) is taken out of service because it is no longer valid. The Registry receives a delete operation and removes the public identity from its database.

UC ADMIN #8 EDITOR's Note: We may need to normalize the language here to use specified terms.

Time-To-Live (TTL): For performance reasons, in favor of localized lookups, a query entity may decide to cache the answers and selectively query the resolution server when either the TTL expires or as a result of another out of band trigger. Therefore, the publishing entity should be able to *optionally* specify the TTL for a given route record. If the provisioning server doesn't support TTL option, it will result in a failure and a well-known error should be returned in the response.

3.1.1.5. Category: Number Portability

TOC

UC NP #1 EDITOR's NOTE: We need to reconcile these two paragraphs.

Routing Numbers: The SSP does not wish to provision individual TNs, but instead, for ease of management, wishes to provision Routing Numbers. Each RN represents a set of individual TNs, and that set of TNs is assumed to change 'automatically' as TNs are ported-in or ported-out. Note that this approach requires a query to resolve a TN to an RN prior to using the provisioned data to route.

The SSP wishes to provide in query response to public identities an associated routing number or RN. This is the case when a set of public identities is no longer associated with original SSP but have been ported to a recipient SSP who provides access to

these identities via a switch on the SS7 network identified by the RN. In this case a destination group containing all numbers that should be routed to this RN needs to be created and the route group associated with this DG needs to contain the RN

UC NP #2 Authoritative release: A release command associated with one or more public identities (or TN Ranges) is received from an authoritative entity indicating his relinquishing of authoritative "ownership" over the respective identities.

EDITOR's NOTE: Can't this be achieved by an authoritative disassociation?

UC NP #3 Authoritative lock error: An existing public identity (or a TN range) is added indicating authoritative ownership by the provisioning entity. However, there may be cases where an explicit release is required. If so, and a release has not been provided, this will result in an error response.

3.1.1.6. Category: PLEASE REVIEW AND SEE IF THESE NEED TO BE ADDED

TOC

UC ID #1 Global TN destinations: The SSP wishes to add or remove one or multiple fully qualified TN destinations in a single provisioning request.

UC ID #2 TN range destinations: The SSP wishes to add or remove one or multiple TN range destinations in a single provisioning request. TN ranges support number ranges that need not be 'blocks'. In other words the TN range 'start' can be any number and the TN range 'end' can be any number that is greater than the TN range 'start'.

UC ID #3 Non-TN destinations: An SSP chooses to peer their messaging service with another SSPs picture/video mail service. Allowing a user to send and receive pictures and/or video messages to a mobile user's handset, for example. The important aspect of this use case is that it goes beyond simply mapping TNs to IP addresses/hostnames that describe points-of-interconnect

between peering network SSP's. Rather, for each user the SSP provisions the subscriber's email address (i.e. jane.doe@example.com). This mapping allows the mobile multimedia messaging service center (MMSC) to use the subscriber email address as the lookup key and route messages accordingly.

UC ID #4 Separation of responsibility: An SSP's operational practices can seperate the responsibility of provisioning the routing information, and the associated identities, to different entities. For example, a network engineer can establish a physical interconnect with a peering SSP's network and provision the associated domain name, host, and IP addressing information. Separately, for each new service subscription, the SSP's back office system provisions the associated public identities.

UC ID #5 Peering offer/acceptance: An SSP offers to allow terminations from another SSP by adding that SSP to a Data Recipient Group it controls. This causes notification of the offered SSP. An SSP receiving a peering offer should be able to accept or decline the offer. If the offer is rejected the registry should not provision corresponding SED to the rejecting SSP. It is expected that this capability will apply mainly in the transit case where non-authoritative parties (in the sense of not being the terminating SSP for an identity) wish to offer the ability to reach the identity and originating SSPs may wish to restrict the routes that are provisioned to their local data repositories.

3.1.2. Requirements

TOC

EDITOR's NOTE: !!!!!THIS NEEDS TO BE REVISED AFTER WE SIGN-OFF ON THE USE CASES!!!!!

The following data requirements apply:

DREQ1: The registry provisioning data model MUST support the following entities: public identities, destination groups, routing groups and data recipient groups.

DREQ2: The registry provisioning data model MUST support the grouping and aggregation of public identities within destination groups.

DREQ3:
The registry provisioning data model SHOULD support the grouping and aggregation of TN Ranges within destination groups.

DREQ4: The registry provisioning data model SHOULD support the grouping and aggregation of RNs within destination groups.

The following functional requirements apply:

FREQ1: The registry provisioning interface MUST support the creation and deletion of: public identities, destination groups, routing groups and data recipient groups.

FREQ2: The registry provisioning interface MUST support near-real-time, non-real-time and deferred provisioning operations.

FREQ3: The registry provisioning interface MUST support the following types of modifications:
- reassignment of one or more public identities from one destination group to another;

- reassignment of one data recipient from one destination group to another;

- association and disassociation of a "Default Routing Group" with a Data Recipient; and,

- identification of a destination group as a "Carrier of Record" (COR) destination group or a "Transit" destination group.

FREQ4: When an entity with a different client identifier than that of the carrier of record for a public identity in a destination group adds a new SSP to a destination recipient group associated with that destination group, the registry provisioning interface MUST: a) notify the new SSP of the updated routing information (which constitutes a peering offer) b) not provision the SED to the new SSP's LDR unless the new SSP signals acceptance.

FREQ5: The registry provisioning interface MUST separate the provisioning of the routing information from the associated identities.

FREQ6: The registry provisioning protocol MUST define a discrete set of response codes for each supported protocol operation. Each response code MUST definitively indicate whether the operation succeeded or failed. If the operation failed, the response code MUST indicate the reason for the failure.

FREQ7:

The registry provisioning interface MUST allow an SSP to define multiple sub-identities that can be used in data recipient groups

FREQ8: The registry provisioning interface MUST define the concurrency rules, locking rules, and race conditions that underlie the implementation of that protocol operation and that result from the coexistence of protocol operations that can operate on multiple objects in a single operation and bulk file operations that may process for an extended period of time.

FREQ9: The registry provisioning interface MUST support the ability for a Data Recipient to optionally define a Routing Group as their Default Routing Group, such that if the Data Recipient performs a resolution request and the lookup key being resolved is not found in the Destination Groups visible to that Data Recipient then the SED Records associated with the Default Routing Group shall be returned in the resolution response.

FREQ10: The registry provisioning interface MUST support the ability for the owner of a Routing Group to optionally define Source Based Routing Criteria to be associated with their Routing Group(s). The Source Based Routing Criteria will include the ability to specify zero or more of the following in association with a given Routing Group: Resolution Client IP Address(es) or Domain Names, Calling Party URI(s). The result will be that the resolution server would evaluate the characteristics of the Source, compare them against Source Based Routing Criteria associated with the Routing Groups visible to that Data Recipient, and return any SED Records associated with the matching Routing Groups.

FREQ11: The registry provisioning interface MUST track, via a client identifier, the entity provisioning each data object (e.g. Destination Group or Routing Group). This client identifier will identify the entity that is responsible for that data object from a protocol interface perspective. This client identifier SHOULD be tied to the session authentication credentials that the client uses to connect into to the registry.
The registry provisioning interface MUST incorporate a data recipient identifier that identifies the organization responsible for each data object from a business perspective. This organization identifier may or may not ultimately refer to the same organization that the client Identifier refers to. The separation of the data recipient identifier from the client identifier will allow for the separation of the two entities, when the need arises.

> Exactly one client identifier MUST be allowed to provision objects under a given data recipient identifier. But a client identifier MUST be allowed to provision objects under multiple data recipient identifiers.
>
> Objects provisioned under one "Protocol Client Identifier" MUST NOT be alterable by a provisioning session established by another "Protocol Client Identifier".

FREQ12: The registry provisioning protocol MUST allow an SSP to provision LUF-only or LUF+LRF data in the registry via a single provisioning interface and data model.

---

4. Security Considerations

TOC

Session establishment data allows for the routing of SIP sesions within, and between, SIP Service Providers. Access to this data can compromise the routing of sessions and expose a SIP Service Provider to attacks such as service hijacking and denial of service. The data can be compromised by vulnerable functional components and interfaces identified within the use cases.

---

5. IANA Considerations

TOC

This document does not register any values in IANA registries.

---

6. Acknowledgments

TOC

This document is a result of various discussions held by the DRINKS requirements design team, which is comprised of the following individuals, in alphabetical order: Deborah A Guyton (Telcordia), Gregory Schumacher (Sprint), Jean-Francois Mule (CableLabs), Kenneth Cartwright (TNS, Inc.), Manjul Maharishi (TNS, Inc.), Penn Pfautz (AT&T Corp), Ray Bellis (Nominet), the co-chairs (Richard Shockey, Nuestar; and Alexander Mayrhofer, enum.at GmbH), and the editors of this document.

This specific version of the document is a result of contributions from, primarily, David Schwartz (XConnect), Kenneth Cartwright (TNS, Inc.) and Syed Ali (Neustar, Inc.). Other participants who reviewed and

provided comments include: Alexander Mayrhofer (enum.at GmbH), Jean-Francois Mule (CableLabs), Manjul Maharishi (TNS, Inc.), and other participants on the DRINKS mailing list.

7. References

TOC

7.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

7.2. Informative References

TOC

[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002 (TXT).
[RFC3263]	Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," RFC 3263, June 2002 (TXT).
[RFC5486]	Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," RFC 5486, March 2009 (TXT).

Author's Address

TOC

	Sumanth Channabasappa
	CableLabs
	858 Coal Creek Circle
	Louisville, CO 80027
	USA
Email:	sumanth@cablelabs.com