

DRINKS
Internet-Draft
Intended status: Informational
Expires: September 9, 2010

S. Channabasappa, Ed.
CableLabs
March 8, 2010

DRINKS Use cases and Protocol Requirements
draft-ietf-drinks-usecases-requirements-01

Abstract

This document captures the use cases and associated requirements for interfaces to provision session establishment data into SIP Service Provider components that aid 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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 9, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1.	Terminology	3
2.	Overview	5
3.	Use Cases and Requirements	10
3.1.	Registry Provisioning	10
3.1.1.	Use Cases	10
3.1.2.	Requirements	15
3.2.	Distribution of data into local data repositories	18
4.	Security Considerations	19
5.	IANA Considerations	20
6.	Acknowledgments	21
7.	References	22
7.1.	Normative References	22
7.2.	Informative References	22
	Author's Address	23

1. Terminology

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](#)].

This document reuses terms from [[RFC3261](#)] (e.g., SIP) and [[RFC5486](#)] (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.

SED Record: A SED Record contains much of the session establishment data or a 'redirect' to another registry where the session establishment data can be discovered. SED Records types supported are NAPTRs, CNAME, DNAME, and NS Records.

Channabasappa, Ed.

Expires September 9, 2010

[Page 3]

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

Data Recipient: SP or SSP that receives or consumes SED and related information.

Data Recipient Group: A group of Data Recipients that receive the same set (or subset) of SED and related information.

[2.](#) Overview

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 complete the call. See [[RFC5486](#)] for more details.

The specification of the format and protocols to configure 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. For scalability reasons SED is rarely exchanged directly between the intended parties. Instead, it is exchanged via intermediate 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.

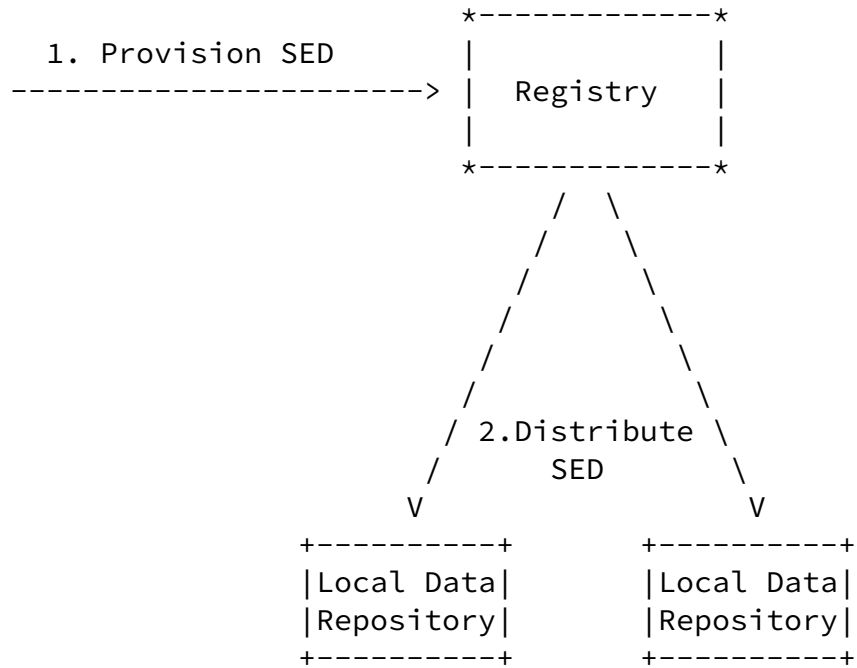
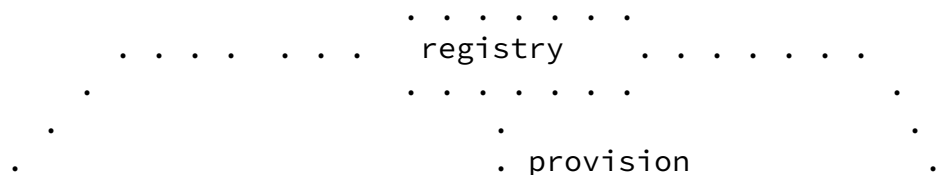


Figure 1: General Diagram

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.



- o Aggregation of public Identifiers: The initial input 'key' to a SED lookup is a public identifier. Since many public identifiers will share similar (or identical) destinations, and hence return similar (or identical) SED, provisioning the same set of SED for millions of public identifiers is inefficient, especially in cases where the SED needs to be modified. Therefore, an aggregation mechanism to 'group' public identifiers is proposed. This aggregation is called a 'destination group'.

- o Aggregation of SSPs: It is expected that SSPs may want to expose different sets of SED, depending on the receiving SSP. This exposure may not always be unique, in which case an aggregation makes it efficient. Such an aggregation is proposed, and termed 'Data Receptient Group'.

- o Aggregation of SED records: Finally, it is anticipated that a complete set of routing data will 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 at this level is proposed, and called 'Routing Group'.

The above aggregations are illustrated in Figure 3.

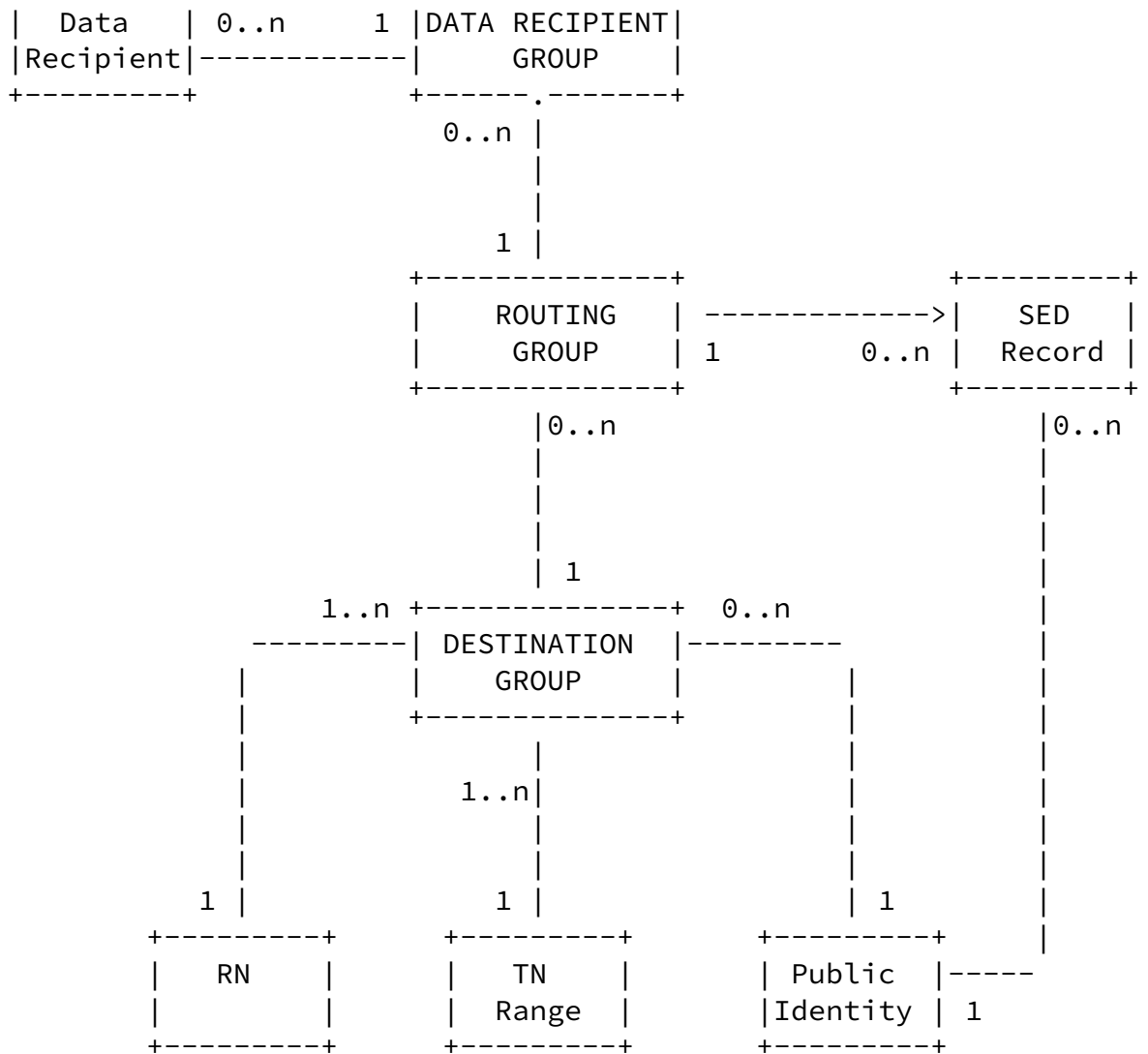


Figure 3: Data Model Diagram

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

This section presents the use cases and associated requirements.

[3.1.](#) Registry Provisioning

Registry is the authoritative source for session establishment data (SED). The registry needs to be provisioned with this data to perform its function. This data includes: destination groups, routing groups and data recipient groups. It can also include RNs and TN Ranges. The following sub-sections illustrate the use cases and the requirements, respectively.

[3.1.1.](#) Use Cases

The use cases are divided into the following categories - process, routing, identity, administration, and number portability.

[3.1.1.1.](#) Category: Process

UC PROCESS #1 Near-real-time provisioning: The registry is provisioned with data that is not accompanied by an effective date or time. In such cases, the registry will validate the data and make it effective in near real-time.

UC PROCESS #2 Deferred provisioning with effective date/time: The registry is provisioned with data that is accompanied by an effective date and time. In scenarios such as this, the registry will validate the data and wait until the effective date and time to make it effective. TBD: What happens if near-real time data overrides data parked for later incorporation?

UC PROCESS #3 Batch provisioning: The registry is provisioned via an

asynchronous provisioning process. For instance, an SSP has commissioned a new registry and wishes to download a very large number of telephone numbers. Rather than stream individual entities, one at a time, the SSP's back-office system prefers to perform the operation as a set of one or more batches (e.g., via an external data file), instead of the near-real-time provisioning interface.

Channabasappa, Ed.

Expires September 9, 2010

[Page 10]

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

[3.1.1.2](#). Category: Routing

UC ROUTING #1 Intra-network SED: SSP wishes to provision their intra-network Session Establishment Data (SED) such that it enables current and future network services to identify and route real-time sessions. For example, in the case of VoIP calls it allows one SoftSwitch (calling) to discover another (called). The SSP provisions IP addressing information pertaining to each SoftSwitch, which is provisioned to the registry but only distributed to a specific local data repository. This SED may differ from the SED that is distributed to other local data repositories.

UC ROUTING #2 Support for destination groups: An SSP may wish to control the flow of traffic into their network (ingress) based on groupings of Public Identities. Associating each group of Public Identities with a specific set of ingress SBEs or points-of-interconnect. The SSP, for example, sub-divides the country into four regions: North-East, South-East, Mid-West, and West-Coast. For each region they establish points-of-interconnect with peers and provision the associated SED hostnames or IP addresses of the SBEs used for ingress traffic. Against each region they provision the served Public Identities into groups- termed Destination Groups - and associate those destination groups with the appropriate points of ingres.

UC ROUTING #3 Modifying destination groups: A set of public identities are assigned a different Destination Group which effectively changes their routing information. This may be due to a network re-arrangement, a Signaling path Border Element being split into two, or a need to do maintenance, two carriers merging, or other considerations. This scenario can also include an effective date and time.

UC ROUTING #4 Indirect Peering to Selected Destinations: The SSP transit provider wishes to provide transit peering points for a set of destinations. But that set of destinations does not align with the destination groups that already exist. The SSP wishes to

Channabasappa, Ed.

Expires September 9, 2010

[Page 11]

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

establish its own destination groups for the destinations that it provides transit to. (Editor's note: This use case needs more work.)

UC ROUTING #5 Inter-network SED (direct and selective peering): In this case the SSP is the actual carrier-of-record; the entity serving the end-user. The SSP wishes to communicate different SED data to some of its peers that wish to route to its destinations. So the SSP has implemented direct points-of-interconnect with each peer and therefore would like address-resolution to result in different answers depending on which peer is asking.

UC ROUTING #6 Selecting egress points: An SSP has a peering relationship with a peer, and when sending messages to that peer's point of interconnection, the originating SSP wishes to use one or more points of egress. These points of egress may vary for an given peer. This capability is supported by allowing an originating SSP to provision SED for identities terminating to other SSPs where the originating SSP is itself the data recipient. The provisioning SSP may make use of

multiple data recipient identities if it requires different sets of egress points be used for calls originating from different parts of its network. Routing from egress points to ingress points of the terminating SSP may be accomplished by static routing from the egress points or by the egress points using data provisioned to the Registry by the terminating SSP.

UC ROUTING #7 SSP prefers to provision LUF and LRF data in the registry: SSP prefers the registry to have access to LUF and LRF information. In this case the originating SSP does not have to rely on mechanisms such as DNS (e.g., [[RFC3263](#)]) for routing information since a registry query will return the terminating SBE.

UC ROUTING #8 Provision an authoritative name server (not actual route): 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: Identity

UC ID #1 Deletion of public identity: 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. This can also trigger delete operations to keep the local data repositories up-to-date.

UC ID #2 Global TN destinations: The SSP wishes to add or remove one or multiple fully qualified TN destinations in a single provisioning request.

UC ID #3 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 #4 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 #5 LUF-only provisioning: SSP wants to provision the registry for LUF lookup only and prefers LRF to be accomplished via non-registry mechanisms. In this case the registry lookup will return a domain name and the originating SSP will rely on mechanisms such as ([RFC3263](#)) to obtain routing

information. This routing information is managed by the (terminating) SSP, via DNS mechanisms.

3.1.1.4. Category: Administration

UC ADMIN #1 Moving an SSP from one data recipient group to another: An SSP would like to re-assign the destination groups it shares with a peer and move the peer SSP from one Data Recipient Group to another. This results in the moved peer seeing a new and different set of routing data.

UC ADMIN #2 Separation of responsibility: An SSP's operational practices can separate 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 ADMIN #3 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.

[3.1.1.5.](#) Category: Number Portability

UC NP #1 The SSP does not wish to provision individual TNs, but instead, for ease of management, wishes to provision Routing Numbers (e.g., as in some number portability implementations). Each RN effectively represents a set of individual TNs, and that set of TNs is assumed to change 'automatically' as TNs are ported in and ported out. Note that this approach requires a query to resolve a TN to an RN prior to using the provisioned data to route.

[3.1.2.](#) Requirements

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.

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

- 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.

[3.2.](#) Distribution of data into local data repositories

This section targets use cases concerned with the distribution of SED to local data repositories. This is considered out-of-scope for this version of the document.

[4.](#) Security Considerations

Session establishment data allows for the routing of SIP sessions 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.

Channabasappa, Ed.

Expires September 9, 2010

[Page 19]

Internet-Draft

ietf-drinks-usecases-reqs

March 2010

[5.](#) IANA Considerations

This document does not register any values in IANA registries.

[6.](#) Acknowledgments

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 is primarily the result of feedback from David

Schwartz (Xconnect) and Jean-Francois Mule (CableLabs), with input from other participants listed above.

Channabasappa, Ed. Expires September 9, 2010 [Page 21]

Internet-Draft ietf-drinks-usecases-reqs March 2010

[7.](#) References

[7.1.](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

7.2. Informative References

- [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.

- [RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", [RFC 3263](#), June 2002.

- [RFC5486] Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology", [RFC 5486](#), March 2009.

Author's Address

Sumanth Channabasappa
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: sumanth@cablelabs.com

