Internet Engineering Task Force (IETF)
Request for Comments: 6461
Category: Informational
ISSN: 2070-1721

S. Channabasappa, Ed.
CableLabs

January 2012

Data for Reachability of Inter-/Intra-NetworK SIP (DRINKS) Use Cases and Protocol Requirements

Abstract

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

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6461.

Copyright Notice

Table of Contents

1. Overview

[RFC5486] (Section 3.3) defines 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 signaling path border elements (SBEs) need to establish a session. However, [RFC5486] does not specify the protocol(s) or format(s) to provision SED. To pave the way to specify such a protocol, this document presents the use cases and associated requirements that have been proposed to provision SED.

SED is typically created by the terminating or next-hop SIP service provider (SSP) and consumed by the originating SSP. To avoid a multitude of bilateral exchanges, SED is often shared via intermediary systems -- termed "registries" within this document. Such registries receive data via provisioning transactions from SSPs, and then distribute the received data into Local Data Repositories (LDRs). These LDRs are used for call routing by outgoing SBEs. This is depicted in Figure 1.

```
                                       *-------------*
                1. Provision SED       |             |
              -----------------------> |  Registry   |
                                       |             |
                                       *-------------*
                                            /  \
                                           /    \
                                          /      \
                                         /        \
                                        /          \
                                       /            \
                                      / 2.Distribute \
                                     /      SED       \
                                    V                  V
                              +----------+       +----------+
                              |Local Data|       |Local Data|
                              |Repository|       |Repository|
                              +----------+       +----------+
```

Figure 1: General Diagram

In this document, we address the use cases and requirements for provisioning registries. Data distribution to local data repositories is out of scope for this document. The resulting provisioning protocol can be used to provision data into a registry or between multiple registries operating in parallel. In Figure 2, the case of multiple registries is depicted with dotted lines.

```
                                  . . . . . . .
                  . . . .  . . .   registry    . . . . . . .
                .                 . . . . . . .              .
              .                        .                      .
             .                         .                       .
            .                          . provision             .
       +-----------+                   .                 +-----------+
       |           |  provision  +----------+  provision |           |
       |   SSP 1   |------------>| Registry |<-----------|   SSP 2   |
       |           |             +----------+            |           |
       |  +-----+  |                   /\                |  +-----+  |
       |  | LDR | <--------------------  ------------------>| LDR |  |
       |  +-----+  |   distribute           distribute   |  +-----+  |
       |           |                                     |           |
       +-----------+                                     +-----------+
              .                                                .
               . . . . . . . . . . . . . . . . . . . . . . . .
                              (provision / distribute)
```

Figure 2: Functional Overview

In addition, this document proposes two aggregation groups, as follows:

o Aggregation of public Identifiers into a destination group.

o Aggregation of SED records into a route group.

The use cases in Section 3.5 provide the rationale. The data model depicted in Figure 3 shows the various entities, aggregations, and the relationships between them.

```
       +---------+            +--------------+               +---------+
       |  Data   |0..n    0..n|     Route    | 1         0..n|   SED   |
       |Recipient|------------|     Group    | --------------|  Record |
       +---------+            +--------------+               +---------+
                                     |0..n                        |0..n
                                     |                            |
                                     |                            |
                                     |                            |
                                     |0..n                        |
                            1 +--------------+  0..1              |
                     ---------| Destination  |---------           |
                    |         |    Group     |         |          |
                    |         +--------------+         |          |
                    |                |                 |          |
                    |               1|                 |          |
                    |                |                 |          |
                    |                |                 |          |
               0..n |           0..n |                 | 0..n     |
               +---------+      +---------+       +----------+    |
               |   RN    |      |   TN    |       | Public   |----
               |         |      |  Range  |       |Identifier| 1
               +---------+      +---------+       +----------+
```

Figure 3: Data Model Diagram

The relationships are as described below:

- A public identifier object can be directly related to zero or more SED Record objects, and a SED Record object can be related to exactly one public identifier object.

- A destination group object can contain zero or more TN (telephone number) Range objects, and a TN Range object can be contained in exactly one destination group object.

- A destination group object can contain zero or more public identifier objects, and a public identifier object can be contained in exactly one destination group object.

- A destination group object can contain zero or more RN (routing number) objects, and an RN object can be contained in exactly one destination group object.

- A route group object can contain zero or more SED Record objects, and a SED Record object can be contained in exactly one route group object.

- A route group object can be associated with zero or more destination group objects, and a destination group object can be associated with zero or more route group objects.

- A data recipient object can be associated with zero or more route group objects, and a route group object can refer to zero or more data recipient objects.

2. 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), [RFC5486] (e.g., SSP, LUF, LRF, SED) and [RFC5067] (carrier-of-record and transit provider). In addition, this document specifies the following additional terms.

Registry: The authoritative source for provisioned session establishment data (SED) and related information. A registry can be part of an SSP or be an independent entity.

Registrar: An entity that provisions and manages data into the registry. An SSP can act as its own registrar or -- additionally or alternatively -- delegate this function to a third party (who acts as its registrar).

Local Data Repository (LDR): The data store component of an addressing server that provides resolution responses.

Public Identifier: A public identifier refers to a telephone number (TN), a SIP address, or other identity as deemed appropriate, such as a globally routable URI of a user address (e.g., sip:john.doe@example.net).

Telephone Number (TN) Range: A numerically contiguous set of telephone numbers.

Telephone Number (TN) Prefix: A preceding portion of the digits common across a series of E.164 numbers. A given TN prefix will include all the valid E.164 numbers that satisfy the expansion rules mandated by the country or the region with which the TNs comply.

Routing Number (RN): A Routing Number. For more information, see [RFC4694].

Destination Group: An aggregation of a set of public identifiers, TN Ranges, or RNs that share common SED, which is exposed to a common set of peers.

Data Recipient: An entity with visibility into a specific set of public identifiers (or TN Ranges or RNs), the destination groups that contain these public identifiers (or TN Ranges and RNs), and a route group’s SED records.

Route Group: An aggregation that contains a related set of SED records and is associated with a set of destination groups. Route groups facilitate the management of SED records for one or more data recipients.

3. Registry Use Cases

This section documents use cases related to the provisioning of the registry. Any request to provision, modify, or delete data is subject to several security considerations (see Section 5). The protocols that implement these use cases (and associated requirements) will need to explicitly identify and address them.

3.1. Category: Provisioning Mechanisms

UC PROV #1 Real-Time Provisioning: Registrars have operational systems that provision public identifiers (or TN Ranges or RNs) in association with their SED. These systems often function in a manner that expects or requires that these provisioning activities be completed immediately, as opposed to an out-of-band or batch provisioning scheme that can occur at a later time. This type of provisioning is referred to as "real-time" or "on-demand" provisioning.

UC PROV #2 Non-Real-Time Bulk Provisioning: Operational systems that provision public identifiers (or TN Ranges or RNs) and associated SED sometimes expect that these provisioning activities be batched up into large sets. These batched requests are then processed using a provisioning mechanism that is out of band and occurs at a later time.

UC PROV #3 Multi-Request Provisioning: Regardless of whether or not a provisioning action is performed in real time, SSPs often perform several provisioning actions on several objects in a single request or transaction. This is done for performance and scalability reasons, and for transactional reasons, such that the set of provisioning actions either fail or succeed atomically, as a complete set.

3.2. Category: Interconnect Schemes

UC INTERCONNECT #1 Inter-SSP SED: SSPs create peering relationships with other SSPs in order to establish interconnects. Establishing these interconnects involves, among other things, communicating and enabling the points of ingress and other SED used to establish sessions.

UC INTERCONNECT #2 Direct and Indirect Peering: Some inter-SSP peering relationships are created to enable the establishment of sessions to the public identifiers for which an SSP is the carrier-of-record. This is referred to as "direct peering". Other inter-SSP peering relationships are created to enable the establishment of sessions to public identifiers for which an SSP is a transit provider. This is referred to as "indirect peering". Some SSPs take into consideration an SSP’s role as a transit or carrier-of-record provider when selecting a route to a public identifier.

UC INTERCONNECT #3 Intra-SSP SED: SSPs support the establishment of sessions between their own public identifiers, not just to other SSPs’ public identifiers. Enabling this involves, among other things, communicating and enabling intra-SSP signaling points and other SED that can differ from inter-SSP signaling points and SED.

UC INTERCONNECT #4 Selective Peering (a.k.a. per-peer policies): SSPs create peering relationships with other SSPs in order to establish interconnects. However, SSP peering relationships often result in different points of ingress or other SED for the same set of public identifiers. This is referred to as "selective peering" and is done on a route group basis.

UC INTERCONNECT #5 Provisioning of a delegated hierarchy: An SSP may decide to maintain its own infrastructure to contain the route records that constitute the terminal step in the LUF. In such cases, the SSP will provision registries to direct queries for the SSP’s public identifiers to its own infrastructure rather than provisioning the route records directly. For example, in the case of DNS-based route records, such a delegated hierarchy would make use of NS and CNAME records, while a flat structure would make use of NAPTR resource records.

3.3. Category: SED Exchange and Discovery Models

UC SED EXCHANGE #1 SED Exchange and Discovery using unified LUF/LRF: When establishing peering relationships, some SSPs may wish to communicate or receive SED (e.g., points of ingress) that constitutes the aggregated result of both LUF and LRF.

UC SED EXCHANGE #2 SED Exchange and Discovery using LUF’s Domain Name: When establishing peering relationships, some SSPs may not wish to communicate or receive points of ingress and other SED using a registry. They only wish to communicate or receive domain names (LUF step only), and then independently resolve those domain names via [RFC3263] to the final points of ingress data (and other SED).

UC SED EXCHANGE #3 SED Exchange and Discovery using LUF’s Administrative Domain Identifier: When establishing peering relationships, some SSPs may not wish to communicate or receive points of ingress and other SED using a registry. They only wish to communicate or receive an administrative domain identifier, which is not necessarily resolvable via DNS. The subsequent process of using that administrative domain identifier to select points of ingress or other SED can be SSP specific and is out of scope for this document.

UC SED EXCHANGE #4 Coexistent SED Exchange and Discovery Models: When supporting multiple peering relationships, some SSPs have the need to concurrently support all three of the SED Exchange and Discovery Models already described in this section (Section 3.3) for the same set of public identifiers.

3.4. Category: SED Record Content

UC SED RECORD #1 SED Record Content: Establishing interconnects between SSPs involves, among other things, communicating points of ingress, the service types (SIP, SIPS, etc.) supported by each point of ingress, and the relative priority of each point of ingress for each service type.

UC SED RECORD #2 Time-To-Live (TTL): For performance reasons, querying SSPs sometimes cache SED that had been previously looked up for a given public identifier. In order to accomplish this, SSPs sometimes specify the TTL associated with a given SED record.

3.5. Category: Separation and Facilitation of Data Management

UC DATA #1 Separation of Provisioning Responsibility: An SSP’s operational practices often separate the responsibility of provisioning the points of ingress and other SED from the responsibility of provisioning public identifiers (or TN Ranges or RNs). 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 subscriber, the SSP’s provisioning systems provision the associated public identifiers.

UC DATA #2 Destination Groups: SSPs often provision identical SED for large numbers of public identifiers (or TN Ranges or RNs). For reasons of efficiency, groups of public identifiers that have the same SED can be aggregated. These aggregations are known as destination groups. The SED is then indirectly associated with destination groups rather than with each individual public identifier (or TN Ranges or RNs).

UC DATA #3 Route Groups: SSPs often provision identical SED for large numbers of public identifiers (or TN Ranges or RNs), and then expose that relationship between a group of SED records and a group of public identifiers (or TN Ranges or RNs) to one or more SSPs. This combined grouping of SED records and destination groups facilitates efficient management of relationships and the list of peers (data recipients) that can look up public identifiers and receive the associated SED. This dual set of SED records and destination groups is termed a "route group".

3.6. Category: Public Identifiers, TN Ranges, and RNs

UC PI #1 Additions and Deletions: SSPs often allocate and de-allocate specific public identifiers to and from end-users. This involves, among other things, activating or deactivating specific public identifiers (TN Ranges or RNs), and directly or indirectly associating them with the appropriate points of ingress and other SED.

UC PI #2 Carrier-of-Record versus Transit Provisioning: Some inter-SSP peering relationships are created to enable the establishment of sessions to the public identifiers (or TN Ranges or RNs) for which an SSP is the carrier-of-record. Other inter-SSP peering relationships are created to enable the establishment of sessions for which an SSP is a transit provider. Some SSPs take into consideration an SSP’s role as a transit or carrier-of-record provider when selecting a route.

UC PI #3 Multiplicity: As described in previous use cases, SSPs provision public identifiers (or TN Ranges or RNs) and their associated SED for multiple peering SSPs, and as both the carrier-of-record and transit provider. As a result, a given public identifier (or TN Range or RN) key can reside in multiple destination groups at any given time.

UC PI #4 Destination Group Modification: SSPs often change the SED associated with a given public identifier (or TN Range or RN). This involves, among other things, directly or indirectly associating them with a different point of ingress, different services, or different SED.

UC PI #5 Carrier-of-Record versus Transit Modification: SSPs may have the need to change their carrier-of-record versus transit role for public identifiers (or TN Ranges or RNs) that they previously provisioned.

UC PI #6 Modification of Authority: An SSP indicates that it is the carrier-of-record for an existing public identifier or TN Range. If the public identifier or TN Range were previously associated with a different carrier-of-record, then there are multiple possible outcomes, such as a) the previous carrier-of-record is disassociated, b) the previous carrier-of-record is relegated to transit status, or c) the new carrier-of-record is placed in inactive mode. The choice may be dependent on the deployment scenario and is out of scope for this document.

3.7. Category: Misc

UC MISC #1 Number Portability: The SSP wishes to provide, in query response to public identifiers, an associated routing number (RN). This is the case where a set of public identifiers is no longer associated with the original SSP but has been ported to a recipient SSP, who provides access to these identifiers via a switch on the Signaling System Number 7 network identified by the RN.

UC MISC #2 Data Recipient Offer and Accept: When a peering relationship is established (or invalidated), SSPs provision (or remove) data recipients in the registry. However, a peer may first need to accept its role (as a data recipient) before such a change is made effective. Alternatively, an auto-accept feature can be configured for a given data recipient.

UC MISC #3 Open Numbering Plans: In several countries, an open numbering plan is used, where the carrier-of-record is only aware of a portion of the E.164 number (i.e., the TN prefix). The carrier-of-record may not know the complete number or the number of digits in the number. The rest of the digits are handled offline (e.g., by a Private Branch Exchange, or PBX). For example, an SSP can be the carrier-of-record for "+123456789" and be the carrier-of-record for every possible expansion of that number, such as "+12345678901" and "+123456789012", even though the SSP does not know what those expansions could be. This can be described as the carrier-of-record effectively being authoritative for the TN prefix.

4. Requirements

This section lists the requirements extracted from the use cases in Section 3. The objective is to make it easier for protocol designers to understand the underlying requirements and to reference and list the requirements that they support (or not). The requirements listed here, unless explicitly indicated otherwise, are expected to be supported. Protocol proposals are also expected to indicate their compliance with these requirements and highlight ones that they don't meet (if any). Furthermore, the requirements listed here are not meant to be limiting, i.e., protocol implementations and deployments may choose to support additional requirements based on use cases that are not listed in this document.

4.1. Provisioning Mechanisms

REQ-PROV-1: Real-time provisioning.

REQ-PROV-2: (Optional) Non-real-time bulk provisioning.

REQ-PROV-3: Multi-request provisioning.

4.2. Interconnect Schemes

REQ-INTERCONNECT-1: Inter-SSP peering.

REQ-INTERCONNECT-2: Direct and Indirect peering.

REQ-INTERCONNECT-3: Intra-SSP SED.

REQ-INTERCONNECT-4: Selective peering.

REQ-INTERCONNECT-5: Provisioning of a delegated hierarchy.

4.3. SED Exchange and Discovery Requirements

REQ-SED-1: SED containing unified LUF and LRF content.

REQ-SED-2: SED containing LUF-only data using domain names.

REQ-SED-3: SED containing LUF-only data using administrative domains.

REQ-SED-4: Support for all the other REQ-SED requirements (listed in this section), concurrently, for the same public identifier (or TN Range or RN).

4.4. SED Record Content Requirements

REQ-SED-RECORD-1: Ability to provision SED record content.

REQ-SED-RECORD-2: (Optional) Communication of an associated TTL for a SED Record.

4.5. Data Management Requirements

REQ-DATA-MGMT-1: Separation of responsibility for the provisioning the points of ingress and other SED, from the responsibility of provisioning public identifiers.

REQ-DATA-MGMT-2: Ability to aggregate a set of public identifiers as destination groups.

REQ-DATA-MGMT-3: Ability to create the aggregation termed route group.

4.6. Public Identifier, TN Range, and RN Requirements

REQ-PI-TNR-RN-1: Provisioning of, and modifications to, the following aggregations: destination group and route groups.

REQ-PI-TNR-RN-2: Ability to distinguish an SSP as either the carrier-of-record provider or the transit provider.

REQ-PI-TNR-RN-3: A given public identifier (or TN Range or RN) can reside in multiple destination groups at the same time.

REQ-PI-TNR-RN-4: Modification of public identifier (or TN Range or RN) by allowing them to be moved to a different destination group via an atomic operation.

REQ-PI-TNR-RN-5: SSPs can indicate a change to their role from carrier-of-record provider to transit, or vice versa.

REQ-PI-TNR-RN-6: Support for modification of authority with the conditions described in UC PI #6.

4.7. Misc. Requirements

REQ-MISC-1: Number portability support.

REQ-MISC-2: Ability for the SSP to be offered a peering relationship and for the SSP to accept (explicitly or implicitly) or reject such an offer.

REQ-MISC-3: Support for open numbering plans.

5. 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.

A provisioning framework or protocol that implements the described use cases MUST, therefore, provide data confidentiality and message integrity. Such frameworks and protocols MUST specify mechanisms to authenticate and authorize any entity that provisions data into the registry, i.e., that the entity is who it says it is and is allowed to use the provisioning interface. The determination of whether such an entity is authorized to provision specific data elements (e.g., a certain public identifier or TN Range) -- while REQUIRED -- may be left to local policy.

6. Acknowledgments

This document is a result of various contributions from (and discussions within) the IETF DRINKS Working Group; specifically, in alphabetical order: Alexander Mayrhofer, Deborah A Guyton, Gregory Schumacher, Jean-Francois Mule, Kenneth Cartwright, Manjul Maharishi, Penn Pfautz, Ray Bellis, Richard Shockey, and Syed Ali.

The editor also wishes to thank the following for their comments and suggestions: Otmar Lendl, Sohel Khan, Peter Koch, Brian Rosen, Jon Peterson, Gonzalo Camarillo, and Stephen Farrell.

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.

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

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.

[RFC4694] Yu, J., "Number Portability Parameters for the "tel" URI", RFC 4694, October 2006.

[RFC5067] Lind, S. and P. Pfautz, "Infrastructure ENUM Requirements", RFC 5067, November 2007.

Author’s Address

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

EMail: sumanth@cablelabs.com