SUA Implementor's guide
<**draft-ietf-sigtran-sua-implementor-guide-05.txt**>

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of 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/1id-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 May 14, 2007.

Copyright Notice

Abstract

   This document contains a compilation of all defects found up until
   the publication date for SUA [RFC3868] [1]. These defects may be of
   an editorial or technical nature. This document may be thought of as
   a companion document to be used in the implementation of SUA to
   clarify errors in the original SUA document. This document updates
   RFC3868 and text within this document supersedes the text found in
   RFC3868.

Table of Contents

1 INTRODUCTION

This document contains a compilation of all defects found up until
the publication date for the SCCP User Adaptation Layer (SUA)
[RFC3868]. These defects may be of an editorial or technical nature.
This document may be thought of as a companion document to be used in
the implementation of SUA to clarify errors in the original SUA
document. This document updates RFC3868 and text within this
document, where noted, supersedes the text found in RFC3868. Each
error will be detailed within this document in the form of:

o The problem description,

o The text quoted from RFC3868,

o The replacement text,

o A description of the solution.

1.1 Terminology

The terms are commonly identified in related work SUA [RFC3868] [1].

1.2 Conventions

2 Correction to RFC3868

2.1 Routing context list in connectionless and connectionoriented messages

2.1.1 Description of the problem

The routing context parameter of a connectionless and connectionoriented message can contain a list of routing contexts. Normaly, the addressing info present in the message will yield only a single routing context. A list of routing contexts is valid only for SSNM, ASPTM and RKM messages

2.1.2 Text changes to the document

```
---------
```
Old text: (Section 3.9.6)
```
---------
```

The Routing Context parameter contains (a list of) 4-byte unsigned integers indexing the Application Server traffic that the sending ASP is configured/registered to receive. There is a one-to-one relationship between an index entry and a Routing Key or AS Name.

```
---------
```
New text: (Section 3.9.6)
```
---------
```

The Routing Context parameter contains (a list of) 4-byte unsigned integers indexing the Application Server traffic that the sending ASP is configured/registered to receive. There is a one-to-one relationship between an index entry and a Routing Key or AS Name.

A list of routing contexts is only valid for SSNM, ASPTM and RKM messages. All other messages can contain only a single Routing Context.

2.1.3 Solution description

Only 1 routing context value may be included in the routing context parameter of a connectionless and connectionoriented message.

2.2 Congestion level parameter value

2.2.1 Description of the problem

The value of the congestion level is dependant on which info is present in the SCON message. If the SCON only contains the affected

pointcode, then the congestion level has values ranging between 0 and
3. If affected pointcode and subsystemnumber is included in the SCON
message, then the value of the congestion level can be between 1 and
8.

2.2.2 Text changes to the document

```
---------
```
Old text: (Section 3.10.24)
```
---------
```

When the Congestion Level parameter is included in a SCON message
that corresponds to an N-PCSTATE primitive, the Congestion Level
field indicates the MTP congestion level experienced by the local or
affected signalling point as indicated by the Affected Point Code(s)
also in the SCON message. In this case, valid values for the
Congestion Level field are as follows:

       0 No Congestion or Undefined
       1 Congestion Level 1
       2 Congestion Level 2
       3 Congestion Level 3

When the Congestion Level parameter is included in a SCON messagethat
corresponds to an N-STATE primitive, the Congestion Level field
indicates the SCCP restricted importance level experienced by the
local or affected subsystem as indicated by the Affected Point Code
and Subsystem Number also in the SCON message. In this case, valid
values for the Congestion Level field range from 0 to 7, where 0
indicates the least congested and 7 indicates the most congested
subsystem.

```
---------
```
New text: (Section 3.10.24)
```
---------
```

2 different congestion levels ranges can be used accoring to ITU and
ANSI congestion control algorithms.

When the ANSI congestion control algorithm is used, the Congestion
Level field indicates the MTP congestion level as experienced by the
local or affected subsystem indicated by the Affected Point Code and
Subsystem Number. In this case, valid values for the Congestion
Level field range from 0 to 3, where 1 indicates the least congested
and 3 indicates the most congested condition.

        0 No Congestion or Undefined
        1 Congestion Level 1
        2 Congestion Level 2
        3 Congestion Level 3

   When the ITU congestion control algorithm is used, the Congestion
   Level field indicates the SCCP restricted importance level
   experienced by the local or affected subsystem as indicated by the
   Affected Point Code and Subsystem Number also in the SCON message.
   In this case, valid values for the Congestion Level field range from
   1 to 8, where 1 indicates the least congested and 8 indicates the
   most congested condition.

2.2.3 Solution description

   The ITU SCCP congestion control procedures are described in SCCP
   procedures [Q.714] [4] paragraph 2.6. The ANSI SCCP congestion
   control procedures are described in SCCP procedures [T1.112.4] [5]
   paragraph 5.2.4.

   The SCC message in SCCP takes the value range 1..8, so the
   corresponding SCON should also be in that range. To indicate no
   congestion, it is sufficient to send only a DAVA.

2.3 Segmentation parameter value

2.3.1 Description of the problem

   The original sequence delivery option as original demanded(= before
   the segementing) by the SCCP application is not preserved after
   segmentation. The receiving SCCP application will always receive the
   message with sequenced delivery option set to 1.

2.3.2 Text changes to the document

   Old text: (Section 3.10.23)

   The first/remaining segments field is formatted as follows:

   o bit 8 (MSB) : indicates whether this is the first segment (1) or
      not (0)

   o bits 1-7: indicate the number of remaining segments, value between
      0 and 15

         New text: (Section 3.10.23)

         The segmentation paramter consists of the following:

         o bit 0: first/remaing segment bit: first = 1, remaining = 0

         o bit 1: sequence delivery option as original demanded(= before the
            segementing) by the SCCP application. class 0 = 0, class 1 = 1.

         o bit 2-3: spare

         o bit 4-7: number of remaining segments(4 bits, values 0 -15)

         o bit 8-31:segmentation reference(3 byte integer)

2.3.3 Solution description

   The segmentation parameter gets a extra bit(out of the spare bits
   present) indicating the original requested sequence delivery option
   as originally demanded by the sending SCCP application.

2.4 DAUD response message ordering

2.4.1 Description of the problem

   Should a SCON be send before the DAVA or DRST or after? The SCON is
   send first and DAVA/DRST after in M3UA.

2.4.2 Text changes to the document

      Old text: (Section 4.5.3)

      The SGP SHOULD respond to a DAUD message with the availability and
      congestion status of the subsystem. The status of each SS7
      destination or subsystem requested is indicated in a DUNA message (if
      unavailable), a DAVA message (if available), or a DRST (if restricted
      and the SGP supports this feature). If the SS7 destination or
      subsystem is available and congested, the SGP responds with an SCON
      message in addition to the DAVA message. If the SS7 destination or
      subsystem is restricted and congested, the SGP responds with an SCON
      message in addition to the DRST. If the SGP has no information on
      the availability / congestion status of the SS7 destination or
      subsystem, the SGP responds with a DUNA message, as it has no routing
      information to allow it to route traffic to this destination or

subsystem.

    New text: ([Section 4.5.3](#))

    The SGP SHOULD respond to a DAUD message with the availability and
    congestion status of the subsystem. The status of each SS7
    destination or subsystem requested is indicated in a DUNA message (if
    unavailable), a DAVA message (if available), or a DRST (if restricted
    and the SGP supports this feature). If the SS7 destination or
    subsystem is available and congested, the SGP responds with an SCON
    message and a DAVA message. If the SS7 destination or subsystem is
    restricted and congested, the SGP responds with an SCON message and a
    DRST. If the SGP has no information on the availability / congestion
    status of the SS7 destination or subsystem, the SGP responds with a
    DUNA message, as it has no routing information to allow it to route
    traffic to this destination or subsystem.

2.4.3 Solution description

    The DAVA/DUNA/DRST/SCON messages may be send in random order.
    However if a SCON is send first and the destination is inaccessible,
    the SCON will be dropped. So it might be better to send the DAVA
    first followed by the SCON.

2.5 Host name parameter

2.5.1 Description of the problem

    The hostname is actually a Fully Qualified Domain Name(FQDN) as
    defined in [RFC1983](#). The definition of the hostname(as found in
    [RFC1983](#)) would only allow for a part of the FQDN and that does not
    uniquely identify a endpoint. Also the encoding of the FQDN is not
    clear.

2.5.2 Text changes to the document

    Old text: ([Section 3.10.2.7](#))

    This field contains a host name in "host name syntax" per [RFC 1123
    Section 2.1](#) [1123]. The method for resolving the host name is out of
    scope for this document.

    New text: ([Section 3.10.2.7](#))

     This field contains a host name in "Fully Qualified Domain Name
     syntax" per RFC 1035 section 3.1 [RFC1035] [3]. The method for
     resolving the host name is out of scope for this document.

2.5.3 Solution description

     The hostname is actually a Fully Qualified Domain Name(FQDN) which
     should be encoded following the RFC1035 section 3.1 coding rules.

2.6   ASP routing context

2.6.1 Description of the problem

     An ASP routes responses to the SGP that it received messages from;
     within the routing context which it is currently active and receiving
     traffic.

2.6.2 Text changes to the document

     Old text: (Section 1.5.2)

     An ASP routes responses to the SGP that it received messages from;
     within the routing context which it is currently active and receiving
     traffic.

     New text: (Section 1.5.2)

     An ASP routes responses to the SGP that it received messages from.
     The reponse will utilize the routing context from the received
     messages.

2.6.3 Solution description

     a. A routing context is an integer which is significant only for a
     given SGP-ASP pair. So it is circular logic to say that the ASP
     should use the RC to select the SGP - an RC value is meaningful only
     after the SGP has already assigned the RC for the the msg send to the
     ASP.

     b. An ASP can be active vis-a-vis an SGP for more than one RC - so
     it is not meaningful to say that the ASP uses "the" RC for which it
     is active. If the ASP response to a messages, it has to use the RC

of that received message in the reponse.

2.7 Parameters should only occur once in a message

2.7.1 Description of the problem

Parameters in SUA messages can be repeated as many times as possible.
This would lead to inconsistencies, such as 2 or more destination
addresses.

2.7.2 Text changes to the document

```
---------
Old text: (Section x.x)
---------


---------
New text: (Section x.x)
---------
```

2.7.3 Solution description

Unless explicitly stated or shown in a message format diagram, only
one parameter of the same type is allowed in a message.

2.8 TID label parameter

2.8.1 Description of the problem

The clarity of the definition of TID label parameters is unclear.

2.8.2 **Text changes to the document**

```
   ---------
  Old text: (Section 3.10.16)
  ---------
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Tag = 0x0110        |           Length = 8          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     start     |     end      |          label value          |
   +---------------+--------------+-------------------------------+
```

    The Start parameter is the start position of label, between 0 (LSB)
    and 31 (MSB).

    The End parameter is the end position of label, between 0 (LSB) and
    31 (MSB).

    Label value is a 16-bit integer, which is unique across an AS.


```
   ---------
  New text: (Section 3.10.16)
  ---------
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Tag = 0x0110        |           Length = 8          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     start     |     end      |          label value          |
   +---------------+--------------+-------------------------------+
```

    The Start parameter is the start position of label, between 0 (LSB)
    and 31 (MSB).

    The End parameter is the end position of label, between 0 (LSB) and
    31 (MSB).

    Label value is a 16-bit integer, which is unique across an AS. The
    label value has to match the TCAP transaction ID between the start
    and the end parameter(Logical AND operation). The rest of the TCAP
    transaction ID between 0 and the begin parameter(if begin parameter
     > 0) AND the end parameter(if end parameter value < 31) and 31 is
    wildcarded.
    An ASP that registers a label will be sent only those TID-bearing
    messages that match its label.
    An ASP that does not register a label may be sent any TID-bearing
    message.

2.8.3 Solution description

The clarity of the definition of the TID and DRM label parameters is
improved by adding what should be wildcarded in the TID/DRM and how
to use the start and end field. It is assumed that these labels are
simple values(at a certain location) that are logical ANDed(taking
into account the start and end position where to apply) onto the
received TID or DRN. If the result of the AND operation exactly
matches the "Label" field, then the message is sent to the ASP that
registered for this label via the ASPAC msg. If a another ASP sends
a already used label then this ASPAC must be rejected.

2.9 DRM label parameter

2.9.1 Description of the problem

See problem description TID label parameter

2.9.2 Text changes to the document

```
---------
Old text: (Section 3.10.15)
---------

    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x010F          |          Length = 8          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     start     |      end      |          label value         |
   +---------------+---------------+------------------------------+
```

The Start parameter is the start position of label, between 0 (LSB)
and 23 (MSB).

The End parameter is the end position of label, between 0 (LSB) and
23 (MSB).

Label value is a 16-bit integer, which is unique across an AS.

```
   ---------
  New text: (Section 3.10.15)
  ---------

     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Tag = 0x010F         |            Length = 8          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     start      |     end      |           label value         |
    +---------------+---------------+-------------------------------+
```

   The Start parameter is the start position of label, between 0 (LSB)
   and 23 (MSB).

   The End parameter is the end position of label, between 0 (LSB) and
   23 (MSB).

   Label value is a 16-bit integer, which is unique across an AS. The
   label value has to match the Destination Reference Number between
   the start and the end parameter(Logical AND operation). The rest
   of the DRN between 0 and the begin parameter(if begin parameter
    > 0) AND the end parameter(if end parameter value < 31) and 31 is
   wildcarded.
   An ASP that registers a label will be sent only those DRN-bearing
   messages that match its label.
   An ASP that does not register a label may be sent any DRN-bearing
   message.

2.9.3 Solution description

   See solution description of the TID label parameter.

2.10 Usage of the TID and DRN label

2.10.1 Description of the problem

   The use of the TID and DRM label parameters is unclear.

2.10.2 **Text changes to the document**

Old text: (Section 4.7.2.1)

   After association setup and registration, an ASP normally goes active
   for each AS it registered for. In the ASPAC message, the ASP
   includes a TID and/or DRN Label Parameter, if applicable for the AS
   in question. All the ASPs within the AS must specify a unique label
   at a fixed position in the TID or DRN parameter. The same ASPAC
   message is sent to each SG used for interworking with the SS7
   network.

   The SG builds, per RK, a list of ASPs that have registered for it.
   The SG can now build up and update a distribution table for a certain
   Routing Context, any time the association is (re-)established and the
   ASP goes active. The SG has to perform some trivial plausibility
   checks on the parameters:

   - Start and End parameters values are between 0 and 31 for TID.
   - Start and End parameters values are between 0 and 23 for DRN
   - ...
   - Start values are the same for each ASP within a RC
   - End values are the same for each ASP within a RC
   - TID and DRN Label values must be unique across the RC

   If any of these checks fail, the SG refuses the ASPAC request, with
   an error: Invalid loadsharing label .

New text: (Section 4.7.2.1)

   After association setup and registration, an ASP normally goes active
   for each AS it registered for. In the ASPAC message, the ASP can include
   a TID and/or DRN Label Parameter, if applicable for the AS
   in question.

   If at least one of the ASPs within an AS specifies a label, then all the
   ASPs within the AS must specify a unique label in the ASPAC's msg they
   send.

   Each of the ASPs within the AS must specify a unique label at a fixed
   position in the TID or DRN parameter. The ASP must send the same ASPAC
   to each SG it is attached to, for interworking with the SS7 network.

   The SG builds, per RC, a list of ASPs that have registered for it.
   The SG can now build up and update a distribution table for a certain
   Routing Context, any time the association is (re-)established and the
   ASP goes active. The SG has to perform some trivial plausibility
   checks on the parameters:

   - Start and End parameters values are between 0 and 31 for TID.
   - Start and End parameters values are between 0 and 23 for DRN
   - ...
   - Start values are the same for each ASP within a RC
   - End values are the same for each ASP within a RC
   - TID and/or DRN Label values must be unique across the RC

   If any of these checks fail, the SG refuses the ASPAC request, with
   an error, "Invalid loadsharing label."

 Old text: (Section 4.7.3.1)

   Messages not containing a destination (or "responding") TID, i.e.,
   Query, Begin, Unidirectional, are loadshared among the available
   ASPs. Any scheme permitting a fair load distribution among the ASPs
   is allowed (e.g., round robin).

   When a destination TID is present, the SG extracts the label and
   selects the ASP that corresponds with it.

   If an ASP is not available, the SG may generate (X)UDTS "routing
   failure", if the return option is used.

New text: ([Section 4.7.3.1](#))

   Messages not containing a destination (or "responding") TID, i.e.,
   Query, Begin, Unidirectional, are loadshared among the available
   ASPs. Any scheme permitting a fair load distribution among the ASPs
   is allowed (e.g., round robin).

   When a destination TID is present, the SG extracts the label and
   if the result of the AND operation exactly matches the "Label" field,
   then the message is sent to the ASP that registered for this label via the
   ASPAC msg.

   An ASP that registers a label will be sent only those TID-bearing
   messages that match its label.

   An ASP that does not register a label may be sent any TID-bearing
   message.

   If an ASP is not available, the SG may generate (X)UDTS "routing
   failure", if the return option is used.

2.10.3 Solution description

   Improving the clarity of the use of the TID and DRM label parameters:

   If the result of the AND operation exactly matches the "Label" field,
   then the message is sent to the ASP that registered for this label
   via the ASPAC msg.

   An ASP that registers a label will be sent only those TID-bearing
   messages that match its label. An ASP that does not register a label
   may be sent any TID-bearing message.

2.11   Address Range paramete

2.11.1 Description of the problem

   It should explicitly state the order of the minimum and maximum
   addresses in this parameter. The most logical order would probably
   be first the min, followed by the max.

2.11.2 **Text changes to the document**

```
 ---------
 Old text: (Section 3.10.17)
 ---------
```

  Address field:

    The Address field the following parameters:

    Parameter
      Source Address   Optional *1
      Destination Address   Optional *1

    Note 1:   The Address field must contain pairs of Source Addresses
               or pairs of Destination Addresses but MUST NOT mix Source
               Addresses with Destination Addresses in the same Address
               field.

```
 ---------
 New text: (Section 3.10.17)
 ---------
```

  Address field:

    The Address field the following parameters:

    Parameter
      Source Address   Optional *1
      Destination Address   Optional *1

    Note 1:   The Address field must contain pairs of Source Addresses
               or pairs of Destination Addresses but MUST NOT mix Source
               Addresses with Destination Addresses in the same Address
               field. The minimum address must be first and the maximun
               address must follow the minimum.

2.11.3 **Solution description**

    State the order of the minimum and maximum addresses in this
    parameter. The logical order is first the min, followed by the max.

2.12 Interpretation of the mask parameter

2.12.1 Description of the problem

   The mask paramater in the DAUD, DAVA and DUNA SUA messages can be in
   the range from 0 to 255 bits. This can go over the maximun pointcode
   range of 24 bits. Also if a ASP request via DAUD with a mask
   parameter of 24, the SG would need to return all pointcodes it know
   in his network to the ASP. (Which could be a lot).

2.12.2 Text changes to the document

Old text: (Section 3.9.18)

Mask: 8-bits

   The Mask parameter can be used to identify a contiguous range of
   Affected Destination Point Codes, independent of the point code
   format. Identifying a contiguous range of Affected PCs may be useful
   when reception of an MTP3 management message or a linkset event
   simultaneously affects the availability status of a series of
   destinations at an SG.

   The Mask parameter is an integer representing a bit mask that can be
   applied to the related Affected PC field. The bit mask identifies
   how many bits of the Affected PC field are significant and which are
   effectively "wild-carded". For example, a mask of "8" indicates that
   the last eight bits of the PC is "wild-carded". For an ANSI 24-bit
   Affected PC, this is equivalent to signalling that all PCs in an ANSI
   Cluster are unavailable. A mask of "3" indicates that the last three
   bits of the PC is "wild-carded". For a 14-bit ITU Affected PC, this
   is equivalent to signalling that an ITU Region is unavailable.

New text: ([Section 3.9.18](#))

Mask: 8-bits

   The Mask parameter can be used to identify a contiguous range of
   Affected Destination Point Codes, independent of the point code
   format. Identifying a contiguous range of Affected PCs may be useful
   when reception of an MTP3 management message or a linkset event
   simultaneously affects the availability status of a series of
   destinations at an SG.

   The Mask parameter is an integer representing a bit mask that can be
   applied to the related Affected PC field. The bit mask identifies
   how many bits of the Affected PC field are significant and which are
   effectively "wild-carded". For example, a mask of "8" indicates that
   the last eight bits of the PC is "wild-carded". For an ANSI 24-bit
   Affected PC, this is equivalent to signalling that all PCs in an ANSI
   Cluster are unavailable. A mask of "3" indicates that the last three
   bits of the PC is "wild-carded".

   The range of mask parameter is limited to 0-24 for ANSI networks and
   is NOT used for ITU networks.

2.12.3 Solution description

   The parameter is limited to 14 bits for ANSI networks and is NOT USED
   in ITU networks.

2.13 Reply on errors contained in a error message

2.13.1 Description of the problem

   If a error message arrives with a error in it, what should be send
   out? Nothing in the [RFC3868](#) describes this possibility.

2.13.2 Text changes to the document

   Old text: ([Section 3.7.1](#))

```
---------
```
New text: ([Section 3.7.1](#))
```
---------
```

Error messages MUST NOT be generated in response to other Error messages.

2.13.3 Solution description

   No error msg must be send back in response on a received error
   message(containing a error). This would otherwise possibly lead to a
   storm of exchange error messages.

2.14 Use of stream 0 for SSNM messages

2.14.1 Description of the problem

   There seems to be some confusion in paragraph 4.5.1. First it is
   mentioned NOT to use stream 0 but a few lines later you MUST use
   stream 0 and that happen all in the same context of sending SSNM
   messages(DAUD, DUNA, DAVA..). It also contradicts statements made in
   paragraph 4.1.1.

2.14.2 Text changes to the document

   ```
   ---------
   ```
   Old text: ([Section 4.5.1](#))
   ```
   ---------
   ```

      DUNA, DAVA, SCON, and DRST messages are sent sequentially and
      processed at the receiver in the order sent. SCTP stream 0 SHOULD
      NOT be used. The Unordered bit in the SCTP DATA chunk MAY be used
      for the SCON message.

      Sequencing is not required for the DUPU or DAUD messages, which MAY
      be sent unordered. SCTP stream 0 is used, with optional use of the
      Unordered bit in the SCTP DATA chunk.

```
   ---------
  New text: (Section 4.5.1)
   ---------
```

   DUNA, DAVA, SCON, and DRST messages are sent sequentially and
   processed at the receiver in the order sent. The Unordered bit
   in the SCTP DATA chunk MAY be used for the SCON message.

   Sequencing is not required for the DUPU or DAUD messages, which MAY
   be sent unordered. SCTP stream 0 is used, with optional use of the
   Unordered bit in the SCTP DATA chunk.

2.14.3 Solution description

   The SSNM messages should be send on stream 0 of the association.

2.15 Timer Ta does not exist

2.15.1 Description of the problem

   Timer Ta is mentioned in paragraph 8 but nowhere specified.

2.15.2 Text changes to the document

```
   ---------
  Old text: (Section 8)
   ---------
```

   8. Timer Values

```
     Ta                                 2 seconds
     Tr                                 2 seconds
     T(ack)                             2 seconds
     T(ias)    Inactivity Send timer    7 minutes
     T(iar)    Inactivity Receive timer 15 minutes
     T(beat)   Heartbeat Timer          30 seconds
```

```
   ---------
```
New text: ([Section 8](#))
```
   ---------
```

8. Timer Values

```
   Tr                                      2 seconds
   T(ack)                                  2 seconds
   T(ias)    Inactivity Send timer         7 minutes
   T(iar)    Inactivity Receive timer      15 minutes
   T(beat)   Heartbeat Timer               30 seconds
```

2.15.3 Solution description

Timer Ta is removed.

2.16 Error response on unsupported RKM messages

2.16.1 Description of the problem

If RKM messages are not supported by a implementation, a error
message is send back with error cause "unsupported message Type". We
should send back a error message with error cause "unsupported
message class" .

2.16.2 Text changes to the document

```
   ---------
```
Old text: ([Section 4.4.1](#))
```
   ---------
```
   If the SGP does not support the registration procedure, the SGP
   returns an Error message to the ASP, with an error code of
   "Unsupported Message Type".

```
   ---------
```
New text: ([Section 4.4.1](#))
```
   ---------
```
   If the SGP does not support the registration procedure, the SGP
   returns an Error message to the ASP, with an error code of
   "Unsupported Message Class".

```
    ---------
    Old text: (Section 4.4.1)
    ---------
```

```
---------
New text: (Section 4.4.1)
---------
```

   If the SGP determines that the requested RK partially, but not
   exactly, matches an existing RK, and that an incoming signalling
   message received at an SGP could possibly match both the requested and
   the existing RK, the SGP returns a Registration Response message to
   the ASP, with a Registration Status of "Error - "Cannot Support Unique
   Routing. An incoming signalling message received at an SGP should not
   match against more than one Routing Key.

   If the SGP determines that the received RK was already registered,
   fully and exactly, either statically or dynamically, by the sending
   ASP, the SGP returns a Registration Response message to the ASP,
   containing a Registration Result "Error - Routing Key Already
   Registered ". This error applies whether the sending ASP/IPSP is in
   ASP-ACTIVE or ASP-INACTIVE for the corresponding AS. For this error
   code, the RC field in the Registration Response message MUST be
   populated with the actual value of RC in SGP corresponding to the
   specified RK in the Registration Request message.

   If an SGP determines that a received Routing Key does not currently
   exist, and the SGP supports dynamic configuration but requires that
   the Routing Key first be manually provisioned at the SGP, the SGP
   returns a Registration Response message to the ASP, containing a
   Registration Result "Error - Routing Key not Currently Provisioned.

```
---------
Old text: (Section 4.4.1)
---------
```

   An ASP MAY modify an existing Routing Key by including a Routing
   Context parameter in the REG REQ. If the SGP determines that the
   Routing Context applies to an existing Routing Key, the SG MAY adjust
   the existing Routing Key to match the new information provided in the
   Routing Key parameter. A Registration Response "Routing Key Change
   Refused" is returned if the SGP does not accept the modification of
   the Routing Key.

New text: ([Section 4.4.1](#))

   An ASP MAY request modification of an existing Routing Key by
   including a Routing Context parameter in a Registration Request
   message. Upon receipt of a Registration Request message containing a
   Routing Context, if the SGP determines that the Routing Context
   applies to an existing Routing Key, the SGP MAY adjust the existing
   Routing Key to match the new information provided in the Routing Key
   parameter. A Registration Response "ERR ? Routing Key Change Refused"
   is returned if the SGP does not support this re-registration procedure
   or RC does not exist. Otherwise, a Registration Response "Successfully
   Registered" is returned.

2.16.3 Solution description

   Send back a error message with "unsupported message class". If >RKM
   messages are not supported, the implementation actually rejects a
   whole class of messages, not just a single one. Other error messages
   are send back depending on the partial or complete match of the
   Routing key with the provisioned data.

2.17 Filler/padding in Global title parameter

2.17.1 Description of the problem

   The global title digits part of the global title parameter contains
   filler bytes. They should be called pading bytes so that they are
   not included in the calculation of the length of the global title
   parameter.

2.17.2 **Text changes to the document**

```
   ---------
   Old text: (Section 3.10.2.3)
   ---------
      Global Title:

      Octets contain a number of address signals and possibly filler as
      shown:

       0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |2 addr.|1 addr.|4 addr.|3 addr.|6 addr.|5 addr.|8 addr.|7 addr.|
       | sig. | sig.  | sig. | sig.  | sig. | sig.  | sig. | sig.  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |        .............       |filler |N addr.|   filler      |
       |                            |if req | sig.  |               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      All filler bits SHOULD be set to 0.



   ---------
   New text: (Section 3.10.2.3)
   ---------
      Global Title:

      Octets contain a number of address signals and possibly filler and
      padding as shown:

       0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |2 addr.|1 addr.|4 addr.|3 addr.|6 addr.|5 addr.|8 addr.|7 addr.|
       | sig. | sig.  | sig. | sig.  | sig. | sig.  | sig. | sig.  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |        .............       |filler |N addr.|   padding     |
       |                            |if req | sig.  |               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      All filler and padding bits SHOULD be set to 0.
```

2.17.3 **Solution description**

   Insert padding into definition of the global title parameter.

2.18 **Inclusion of routing context in the Routing key parameter**

2.18.1 **Description of the problem**

   The Routing conext is missing from the Routing key parameter of the
   REG message, so leading to a inconsistency with section 4.4.1 where
   it is mentioned that the RC has to be present in order to change the
   registration data of a certain RC. If the RC is not present, then
   the registration data can not be identified and changed.

2.18.2 **Text changes to the document**

   Old text: (Section 3.10.14)

      The Key field contains the following parameters:

          Parameter
             Traffic Mode Type   Optional
             Network Appearance   Optional *1
             Source Address   Optional
             Destination Address   Optional
             Address Range   Optional

      Note 1:   The Network Appearance parameter must be included in the
                 Routing Key when the ASP is able to register in multiple
                 SS7 Network contexts

 New text: ([Section 3.10.14](#))

    The Key field contains the following parameters:

        Parameter
            Traffic Mode Type   Optional
            Network Appearance   Optional *1
            Source Address   Optional
            Destination Address   Optional
            Address Range   Optional
            Routing Context   Optional *2

    Note 1:   The Network Appearance parameter must be included in the
               Routing Key when the ASP is able to register in multiple
               SS7 Network contexts.

    Note 2:   The Routing Context parameter is included in the Routing
               Key when the ASP wishes to alter an existing Routing Key
               which corresponds to the indicated Routing Context. The
               Routing Context parameter MUST only occur once in the Key
               parameters.

2.18.3 Solution description

   Include the routing context parameter in the routing key parameter.
   And keep the text of [section 4.4.1](#).

2.19 New registration status parameter value

2.19.1 Description of the problem

   A new registartion status parameter value is required in case that a
   routing key chnage is refused.

2.19.2 Text changes to the document

```
 ---------
Old text: (Section 3.9.22)
 ---------
Registration Status: 32-bits (unsigned integer)

      The Registration Status field indicates the success or the reason
      for failure of a registration request.

    Its values may be:
              0            Successfully Registered
              1            Error - Unknown
              2            Error - Invalid Destination Address
              3            Error - Invalid Network Appearance
              4            Error - Invalid Routing Key
              5            Error - Permission Denied
              6            Error - Cannot Support Unique Routing
              7            Error - Routing Key not Currently Provisioned
              8            Error - Insufficient Resources
              9            Error - Unsupported RK parameter Field
             10            Error - Unsupported/Invalid Traffic Mode Type
             11            Error - Routing Key Change Refused




 ---------
New text: (Section 3.9.22)
 ---------
Registration Status: 32-bits (unsigned integer)

      The Registration Status field indicates the success or the reason
      for failure of a registration request.

    Its values may be:
              0            Successfully Registered
              1            Error - Unknown
              2            Error - Invalid Destination Address
              3            Error - Invalid Network Appearance
              4            Error - Invalid Routing Key
              5            Error - Permission Denied
              6            Error - Cannot Support Unique Routing
              7            Error - Routing Key not Currently Provisioned
              8            Error - Insufficient Resources
              9            Error - Unsupported RK parameter Field
             10            Error - Unsupported/Invalid Traffic Mode Type
             11            Error - Routing Key Change Refused
             12            Error - Routing Key already registered
```

2.19.3 Solution description

Add new Registration response "Error - Routing key already
registered".

3 Security considerations

No new treats have been identified besides the already known in SUA
[RFC3868] [1].

[4](#) Acknowledgments

The authors wish to thank B. Nagelberg, B. Bidulock, T. Asveren, S. Karl, K. Morneault and many others for their invaluable comments.

[5](). References

[1]   Loughney, J., Sidebottom, G., Verwimp, G., Coene, L., Keller,
      J., and B. Bidulock, "Signalling Connection Control Part User
      Adaptation Layer (SUA)", RFC 3868, October 2004.

[2]   Malkin, G., "Internet Users' Glossary", RFC 1983, August 1996.

[3]   Mockapetris, P., "Domain names - Implementation and
      Specification", RFC 1035, November 1987.

[4]   ITU, "Q.714 : SCCP procedures", Q. 714, July 1997.

[5]   ANSI, "T1.112.4 : SCCP procedures", T. 1.112.4, December 1993.

Appendix A   Changes Control

A.1   Changes from v00 to v01

   - Change of boilerplate

   - Typos.

   - Paragraph 2.6 ASP routing context: replacement text for section
   1.5.2

   - Paragraph 2.10 Usage of TID and DRM label parameter: text
   clarification for solution description

   - Paragraph 2.8 Use of ANSI intermediate signaling network
   identification (ISNI) parameter: Removed, no text proposed.

A.2   Changes from v01 to v02

   - Typos.

   - Paragraph 2.17 Filler/padding in Global title parameter: new

   - Paragraph 2.18 Inclusion of routing context in the Routing key
   parameter: new

   - Paragraph 2.8 TID label parameter:Changed: Another attempt at
   clarifying what a SG could be doing with TID label.

   - Paragraph 2.9 DRM label parameter:Changed: Another attempt at
   clarifying what a SG could be doing with DRM label.

   - Paragraph 2.10 Usage of TID and DRM label parameter:Changed:
   Another attempt at clarifying what a SG could be doing with TID and
   DRM labels.

   -

A.3   Changes from v02 to v03

   - Typos.

   - Paragraph 2.16:Error response on unsupported RKM messages: Changed

   - Paragraph 2.19:New registration status parameter value: New

A.4 Changes from v03 to v04

   - None.

Authors' Addresses

    Lode Coene
    Siemens
    Atealaan 32
    Herentals 2200
    Belgium

    Phone: +32-14-252081
    Email: lode.coene@siemens.com

    John Loughney
    Nokia
    Itdmerenkatu 11-13
    Espoo 00180
    Finland

    Phone: +358 50 483 6242
    Email: john.loughney@nokia.com

Full Copyright Statement

Intellectual Property

Acknowledgment