

# 3GPP TR 29.903 V5.0.0 (2001-12)

---

*Technical Report*

## **3rd Generation Partnership Project; Technical Specification Group Core Networks; Feasibility Study on SS7 signalling transport in the core network with SCCP-User Adaptation Layer (SUA) (Release 5)**



The present document has been developed within the 3<sup>rd</sup> Generation Partnership Project (3GPP<sup>TM</sup>) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP<sup>TM</sup> system should be obtained via the 3GPP Organizational Partners' Publications Offices.

---

---

Keywords

3GPP, CN4, SUA, SS7, Sigtran

**3GPP**

---

Postal address

---

Office address

650 Route des Lucioles - Sophia Antipolis  
Valbonne - FRANCE  
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

---

Internet

<http://www.3gpp.org>

---

**Copyright Notification**

No part of this document may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2000, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).  
All rights reserved.

# Contents

Foreword.....	5
1 Scope .....	6
2 References .....	6
2.1 Normative References .....	6
2.2 Informative References .....	7
3 Definitions and Abbreviations .....	8
3.1 Definitions .....	8
3.2 Abbreviations .....	8
4 Introduction .....	9
5 SUA Overview .....	9
5.1 Sigtran Background .....	9
5.2 SUA Functionality .....	10
5.3 Mapping Between SCCP Messages and SUA Messages .....	11
5.4 Status in IETF.....	11
6 M3UA Overview .....	12
6.1 M3UA Functionality .....	12
6.2 M3UA Implementation .....	12
6.3 M3UA Adoption in 3GPP .....	13
7 SUA Implementation.....	13
7.1 SUA In an All IP Environment.....	13
7.1.1 Architecture .....	14
7.1.2 Routing SUA Messages in an Intra-PLMN Environment.....	15
7.1.3 Routing SUA Messages in an Inter-PLMN Environment.....	16
7.1.4 Message Segmentation .....	16
7.2 Interworking with Legacy SS7 Network .....	16
7.2.1 Architecture .....	16
7.2.2 Global Title Management .....	17
7.2.3 Message Segmentation .....	17
7.2.4 SUA Interworking with SCCP Network Management Function .....	17
7.2.5 AMF implementation example in interworking with legacy SS7 network.....	18
7.2.5.1 Point Codes Example.....	18
7.3 Interworking with SCCP/M3UA .....	20
7.3.1 Architecture .....	20
7.3.2 Global Title management.....	20
7.3.3 Message Segmentation .....	20
7.3.4 SUA Interworking with SCCP Network Management Function .....	20
7.3.5 Interworking in native SS7 networks.....	21
7.3.6 Interworking in SS7 and SigTran Networks .....	21
7.3.7 Interworking in 3GPP networks.....	25
7.3.8 SCCP and SUA interworking in detail .....	26
7.3.8.1 Establishment of SUA connectivity.....	27
7.3.8.2 SEP Failover .....	27
7.3.8.3 Successful ASP Failover Scenario.....	28
7.3.9 Interworking Conclusions.....	28
8 Services Impact .....	28
8.1 Calling line identification presentation (CLIP) .....	28
8.2 Calling line identification restriction (CLIR) .....	28
8.3 Connected line identification presentation (COLP).....	28
8.4 Connected line identification restriction (COLR) .....	28
8.5 Call Forwarding Unconditional (CFU).....	29
8.6 Call Forwarding on mobile subscriber Busy (CFB) .....	29
8.7 Call Forwarding on No Reply (CFNRy) .....	29

8.8	Call Forwarding on mobile subscriber Not Reachable (CFNRc) .....	29
8.9	Call Waiting (CW) .....	29
8.10	Call hold (HOLD) .....	29
8.11	Multiparty services (MPTY) .....	29
8.12	Closed User Group .....	29
8.13	Advice of Charge services .....	29
8.14	Barring of All Outgoing Calls (BAOC) .....	29
8.15	Barring of Outgoing International Calls (BOIC) .....	29
8.16	Barring of Outgoing International Calls except those directed to the Home PLMN Country (BOIC-exHC) .....	29
8.17	Barring of All Incoming Calls (BAIC) .....	30
8.18	Barring of Incoming Calls when roaming outside the home PLMN country (BIC-Roam) .....	30
8.19	Explicit Call Transfer (ECT) .....	30
8.20	Completion of Calls to Busy Subscriber (CCBS) .....	30
8.21	Support of Private Numbering Plan (SPNP) .....	30
8.22	Multiple Subscriber Profile (MSP) .....	30
8.23	enhanced Multi-Level Priority and Pre-emption (eMLPP) .....	30
8.24	SMS .....	30
8.25	CAMEL .....	30
8.26	Mobile Number Portability .....	31
9	Security .....	31
10	Network Evolution and Interworking Scenarios .....	32
11	Benefits and Drawbacks .....	33
11.1	Benefits: .....	33
11.1.1	Benefits perceived by some companies: .....	33
11.1.2	Benefits agreed by all companies .....	33
11.2	Drawbacks .....	34
11.2.1	Drawbacks outlined by some companies .....	34
11.2.2	Drawbacks agreed by all companies .....	34
11.3	Neutral Points agreed by all companies .....	34
12	Open Issues .....	34
13	Conclusion .....	35
14	Work Plan .....	35
<b>Annex A:</b>	<b>Procedure for Message Routing with DNS/ENUM .....</b>	<b>36</b>
A.1	Routing Using Provided E.164 (MSISDN) Number .....	36
A.2	Routing Using Provided E.212 (IMSI) Number .....	36
A.2.1	Routing using E.214 addressing information .....	36
A.2.2	Routing using E.212 addressing information .....	37
<b>Annex B:</b>	<b>Document History .....</b>	<b>39</b>

---

# Foreword

This Technical Report has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TR, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

Where:

x is the first digit:

- 1 presented to TSG for information;
- 2 presented to TSG for approval;
- 3 Indicates TSG approved document under change control.

y is the second digit incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z is the third digit incremented when editorial only changes have been incorporated in the specification.

---

# 1 Scope

The scope of this Technical Report (TR) is to capture the results of a feasibility study on SS7 signalling transport (e.g. MAP & CAP) in a 3GPP core network with SCCP-User Adaptation (SUA) for Release-5.

With this purpose in mind, this TR evaluates the advantages and disadvantages associated with the implementation of SUA in the core network, and compares it with the SCCP/M3UA option. Therefore, an overview of M3UA is provided in this document for reference. This TR covers all scenarios such as SUA peer to peer as well as interworking with legacy SS7 network, plus the interworking between SUA and SCCP/M3UA. This TR also identifies and studies the technical issues related to SUA implementation and proposes the possible technical solutions that will enable the efficient implementation of SUA, with minimum impacts on the available services.

More generally, the aim of this TR is to identify and strive to solve all issues introduced by such evolution of the core network signalling. At the end of the feasibility study, the open issues are reported and their importance is assessed. Also discussed are the benefits and drawbacks with respect to the introduction of SUA into 3GPP core network signalling.

---

# 2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

For a specific reference, subsequent revisions do not apply.

For a non-specific reference, the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

## 2.1 Normative References

- [1] 3GPP TS 21.905: "3G Vocabulary".
- [2] 3GPP TS 23. 040: "Technical realization of the Short Message Service (SMS)".
- [3] 3GPP TS 23. 903: "Technical realization of Completion of Calls to Busy Subscriber (CCBS)".
- [4] 3GPP TS 25. 305: " Stage 2 Functional Specification of UE Positioning in UTRAN".
- [5] 3GPP TS 29.202: "SS7 Signalling Transport in Core Network; Stage 3".
- [6] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".
- [7] 3GPP TS 29.078: "Customised Applications for Mobile network Enhanced Logic; (CAMEL) Phase 3; CAMEL Application Part (CAP) specification".
- [8] 3GPP TS 29.013: "Signalling interworking between ISDN supplementary services; Application Service Element (ASE) and Mobile Application Part (MAP) protocols".
- [9] 3GPP TS 29.018: " Serving GPRS Support Node (SGSN) – Visitor Location Register (VLR) Gs interface layer 3 specification".
- [10] 3GPP TS 29.205: "Application of Q.1900 Series to Bearer Independent; CS Core Network Architecture – Stage 3".
- [11] 3GPP TS 29.232: "Media Gateway Controller (MGC) – Media Gateway (MGW); Interface; Stage 3".

- [12] 3GPP TS 29.066: " Support of Mobile Number Portability (MNP); Technical Realisation".
- [13] 3GPP TS 33.200 "Network Domain Security".
- [14] IETF RFC 2960: Stream Control Transmission Protocol (SCTP).  
<http://www.ietf.org/rfc/rfc2960.txt>
- [15] IETF INTERNET-DRAFT: SS7 SCCP-User Adaptation Layer (SUA).  
<http://www.ietf.org/internet-drafts/draft-ietf-sigtran-sua-08.txt>
- [16] IETF INTERNET-DRAFT: SS7 MTP3-User Adaptation Layer (M3UA).  
<http://www.ietf.org/internet-drafts/draft-ietf-sigtran-m3ua-09.txt>
- [17] IETF RFC 2916: E.164 number and DNS (ENUM).  
<http://www.ietf.org/rfc/rfc2916.txt>
- [18] IETF RFC 1034 Domain Names –Concepts and Facilities.  
<http://www.ietf.org/rfc/rfc1034.txt>
- [19] IETF RFC 1035 Domain Names –Implementation And Specification.  
<http://www.ietf.org/rfc/rfc1034.txt>
- [20] IETF RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record.  
<http://www.ietf.org/rfc/rfc2915.txt>
- [21] IETF INTERNET-DRAFT: On the Use of SCTP with IPsec.  
<http://www.ietf.org/internet-drafts/draft-ietf-ipsec-sctp-01.txt>

## 2.2 Informative References

- [22] IETF RFC 2719: Framework Architecture for Signalling Transport  
<http://www.ietf.org/rfc/rfc2719.txt>
- [23] ITU-T Recommendation E.164: "Numbering plan for the ISDN era"
- [24] ITU-T Recommendation E.212: "Identification plan for land mobile stations"
- [25] ITU-T Recommendation E.214: "Structuring of the land mobile global title for the signalling connection control part"
- [26] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Functional description of the Signalling Connection Control Part".
- [27] ITU-T Recommendation Q.712: "Definition and function of SCCP messages".
- [28] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; SCCP formats and codes".
- [29] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling Connection Control Part procedures".
- [30] ANSI T1.112 (1996): "Telecommunication – Signalling No. 7 – Signaling Connection Control Part (SCCP)"
- [31] R3-011486: "Radio Network Signalling Bearer for RANAP and RNSAP in Rel5 IP transport option"
- [32] R3-011490: " SUA vs. M3UA for RANAP, RNSAP TNL in IP UTRAN "

---

## 3 Definitions and Abbreviations

### 3.1 Definitions

**IPSP:** Signalling Point in the IP network

**Mobile Number:** In this document the expression "Mobile Number" is used to indicate any of the E.164, E.212 and E.214 numbers of the mobile.

### 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AMF	Address Mapping Function
ASP	Application Server Process
AP	Application level protocol (SCCP User Protocols)
AS	Application Server
BG	Border Gateway
AAL5	ATM Adaptation Layer type 5
ATM	Asynchronous Transfer Mode
BSSAP+	Base Station System Application Part
CAMEL	Customized Application for Mobile Network Enhanced Logic
CAP	CAMEL Application Part
CC	Country Code
NDC	National Destination Code
CCBS	Call Completion to Busy Subscriber
DNS	Domain Name System
ENUM	Electronic Number (RFC 2916)
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
GTT	Global Title Translation
HPLMN	Home Public Land Mobile Network
VPLMN	Visitor Public Land Mobile Network
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IWF	Interworking Function
LDAP	Lightweight Directory Access Protocol
M3UA	MTP3-User Adaptation
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MNP	Mobile Number Portability
MTP	Message Transfer Part
MTP1	Message Transfer Part layer 1
MTP2	Message Transfer Part layer 2
MTP3	Message Transfer Part layer 3
NAPTR	The Naming Authority Pointer
MTU	Maximum Transfer Unit
NPDB	Number Portability Database
PC	Point code
PCAP	Positioning Calculation Application Part
PDH	Plesiochronous Digital Hierarchy
RANAP	Radio Access Network Application Part
RNSAP	Radio Network Subsystem Application Part
SG	Signalling Gateway
SMMT	Short Message Mobile Terminated
SMMO	Short Message Mobile Originated
SMS	Short Message Service
SNM	SUA Network Management



SSAP	Supplementary Service Application Part
SSCF	Service Specific Coordination Function
SSCOP	Service Specific Connection Oriented Protocol
SSN	SCCP subsystem number
SCCP	Signalling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SUA	SCCP-User Adaptation layer
T-BCSM	Terminating Basic Call State Model
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TPDU	Transfer Protocol Data Unit
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifiers

---

## 4 Introduction

The purpose of this technical report (TR) is *i)* to discuss the advantages and disadvantages of using the SUA protocol to transport MAP and/or CAP signalling over an IP based core network, and *ii)* to propose SUA as an alternative option for MAP/CAP transport in Rel-5.

---

## 5 SUA Overview

SCCP-User Adaptation (SUA) is a new protocol, currently developed by IETF (see 0), for the transport of any SS7 SCCP-User signalling (e.g. TCAP etc.) over IP using the Stream Control Transport Protocol (SCTP). SUA aims to be modular and symmetric, to allow it to work in diverse architectures, such as a Signalling Gateway to IP Signalling Endpoint architecture as well as a peer-to-peer IP Signalling Endpoint architecture.

### 5.1 Sigtran Background

Stream Control Transmission Protocol (SCTP), defined by the Signal Transport (SIGTRAN) working group of the Internet Engineering Task Force (IETF), is a transport level datagram transfer protocol that operates on top of an unreliable datagram service, such as Internet Protocol (IP). Like TCP, SCTP provides a reliable transport service, ensuring that data is transported across the network without error and in sequence. SCTP works on the basic concepts of associations and streams. An SCTP association is similar to a TCP connection, except it can support multiple IP addresses at either or both ends. An SCTP association is comprised of multiple logical streams, ensuring the sequenced delivery of user messages within a single stream. SCTP achieves the reliable message transport service by retransmitting lost messages in a similar fashion to TCP. However, unlike TCP, the retransmission by SCTP of a lost message in one stream does not block the delivery of messages in other streams. The use of multiple streams within SCTP resolves the issue of head-of-line blocking associated with the use of TCP. The basic SCTP functionality includes:

- Acknowledged error-free non-duplicated transfer of data streams

- Data fragmentation to conform to Message Transfer Unit (MTU) size

- Sequenced delivery of user messages within multiple streams with an option for order of arrival and delivery of individual user messages

- Bundling of multiple user messages into a single SCTP packet

- Network level fault tolerance due to the support of multi-homing at either or both ends of an association

The SCCP-User Adaptation Layer (SUA), defined by the SIGTRAN working group of the Internet Engineering Task Force (IETF), transports signalling messages from SCCP users, such as Transaction Capabilities Application Part (TCAP), Radio Access Network Application Part (RANAP) and Radio Network Subsystem Application Part (RNSAP), over the Internet Protocol (IP) network, using the Stream Control Transmission Protocol (SCTP). SUA allows the

seamless interoperation between SCCP users in the SS7 and IP domains. RANAP and RNSAP transport and their associated protocol stacks are being studied by the "IP Transport in UTRAN" work item in the RAN3 working group.

## 5.2 SUA Functionality

The SUA delivery mechanism provides the following functionality:

Support for transfer of SS7 SCCP-User messages;

Support for SCCP connectionless service;

Support for SCCP connection oriented service;

Support for the seamless operation of SCCP-User protocol peers;

Support for the management of SCTP transport associations between a Signalling Gateway and one or more IP-based signalling nodes to the degree specified by the SCCP user application;

Support for distributed IP-based signalling nodes; and

Support for the asynchronous reporting of status changes to management.

Support Address Mapping Function (AMF) for more/enhanced services provided by SCCP GTT such as address mapping with IP addresses or hostnames.

## 5.3 Mapping Between SCCP Messages and SUA Messages

For the seamless support transfer of SCCP-User Part messages, SCCP messages can be mapped into associated SUA messages.

SUA NAME	SCCP NAME	SCCP Full Name	Classes				Mgt. Msg.	SUA Usag e
			0	1	2	3		
Connectionless Messages								
CLDT	UDT	Unitdata	x	x	-	-	-	-
CLDT	XUDT	Extended unitdata	x	x	-	-	-	-
CLDT	LU DT	Long unitdata	x	x	-	-	-	-
CLDR	UDTS	Unitdata service	x	x	-	-	-	-
CLDR	XUDTS	Extended unitdata service	x	x	-	-	-	-
CLDR	LU DTS	Long unitdata service	x	x	-	-	-	-
Connection-Oriented Messages								
CODT	DT1	Data form 1	-	-	x	-	-	-
CODT	DT2	Data form 2	-	-	-	x	-	-
CODT	ED	Expedited data	-	-	-	x	-	-
CODA	AK	Data acknowledgement	-	-	-	x	-	-
CODA	EA	Expedited data acknowledge	-	-	-	x	-	-
CORE	CR	Connection request	-	-	x	x	-	-
COAK	CC	Connection confirm	-	-	x	x	-	-
COREF	CREF	Connection refused	-	-	x	x	-	-
RELRE	RLSD	Released	-	-	x	x	-	-
RELCO	RLC	Release complete	-	-	x	x	-	-
RESRE	RSR	Reset request	-	-	-	x	-	-
RESCO	RSC	Reset confirm	-	-	-	x	-	-
COIT	IT	Integrity test	-	-	x	x	-	-
COERR	ERR	Protocol Data Unit Error	-	-	x	x	-	-
SS7 MGT Messages								
SCON	SSC	Destination /subsystem-congested	-	-	-	-	x	-
DAVA	SSA	Destination /subsystem-allowed	-	-	-	-	x	-
DUNA	SSP	Destination subsystem-prohibited	-	-	-	-	x	-
DAUD	SST	Destination /subsystem-status-test	-	-	-	-	x	-
n/a	SOR	Subsystem-oos-req	-	-	-	-	x	-
n/a	SOG	Subsystem-oos-grant	-	-	-	-	x	-
DRST	n/a	Destination Restricted	-	-	-	-	x	-
SUA MGT Messages								
ASPUP	n/a	n/a	-	-	-	-	-	x
ASPDN	n/a	n/a	-	-	-	-	-	x
ASPAC	n/a	n/a	-	-	-	-	-	x
ASPIA	n/a	n/a	-	-	-	-	-	x
NTFY	n/a	n/a	-	-	-	-	-	x
ERR	n/a	n/a	-	-	-	-	-	x

NOTE: SUA messages (CLDT, CLDR) support all 6 SCCP connectionless messages.

- = Message not applicable for this protocol class.

X = Message applicable for this protocol class.

n/a = not applicable

NOTE: Please refer to section 0 and 0 for detail usage of SS7 MGT messages.

## 5.4 Status in IETF

At the present time, SUA is still under development by the SIGTRAN Working Group in IETF. The latest version is 8 and it has passed SIGTRAN working group last call and will be submitted for IETF last call very soon.

## 6 M3UA Overview

In order to compare SUA and M3UA, it is necessary to give a brief introduction of M3UA and its implementation and its adoption in 3GPP in this technical report.

MTP3-User Adaptation (M3UA) is a protocol, currently developed by IETF0, for the transport of any SS7 MTP3-User signalling (e.g. ISUP, SCCP and TUP) over IP using the Stream Control Transport Protocol (SCTP). M3UA can also work in diverse architectures, such as a Signalling Gateway to IP Signalling Endpoint architecture as well as a peer-to-peer IP Signalling Endpoint architecture.

### 6.1 M3UA Functionality

The M3UA delivery mechanism provides the following functionality:

Support for transfer of SS7 MTP3-User Part messages;

Support for the management of SCTP transport protocol between a Signalling Gateway and one or more IP-based signalling nodes to ensure transport availability to MTP3 user signalling applications;

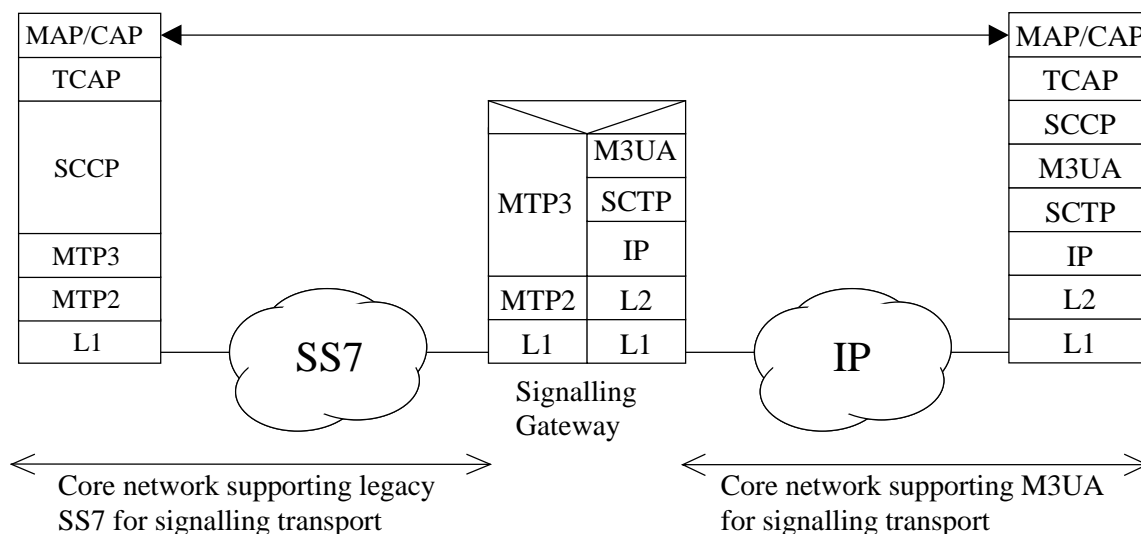
Support for the seamless operation of MTP3-User protocol peers;

Support for distributed IP-based signalling nodes; and

Support for the asynchronous reporting of status changes to management.

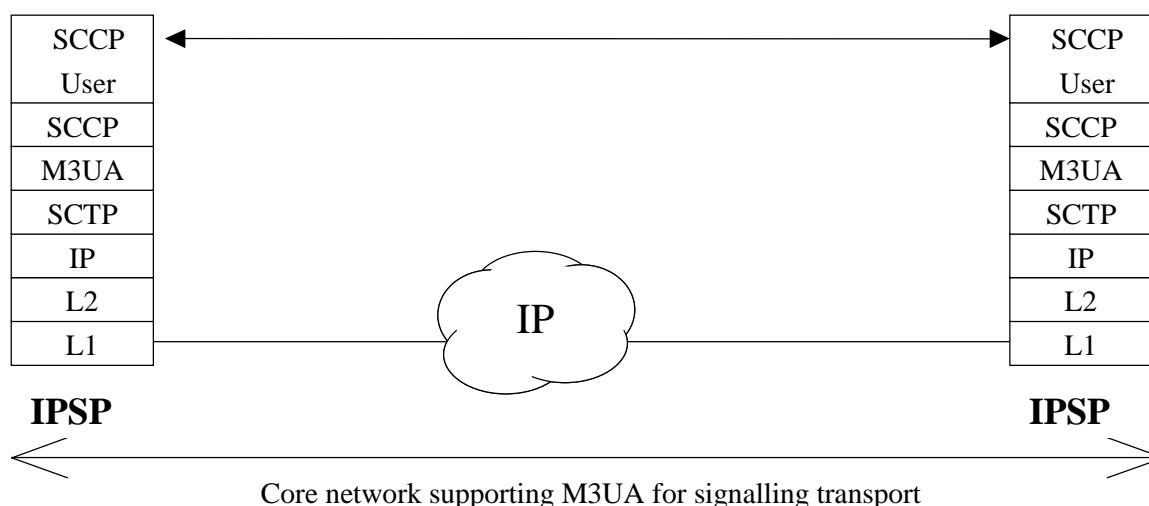
### 6.2 M3UA Implementation

The usage of M3UA to transport MAP and TCAP messages is illustrated in Figure 1.



**Figure 1: Transportation of MAP and CAP via M3UA**

An example of SCCP transport between IPSPs is illustrated in Figure 2. SCCP messages are exchanged directly between two IP resident IPSPs with SCCP user protocol like TCAP, RANAP and RNSAP.



**Figure 2: Transportation of SCCP-user messages via M3UA in all IP network**

## 6.3 M3UA Adoption in 3GPP

Now SCCP/M3UA is the only specified protocol for IP based transportation of 3GPP SS7 like core network signalling in Release 4. Please refer to 3GPP TS 29.2020 for transporting MAP & CAP messages in a 3GPP core network using M3UA. Also see 3GPP TS 29.2050 and 3GPP TS 29.2320 for M3UA usage in Mc interface between MSC and MGW. Meanwhile, M3UA is specified as an option for RANAP in 3GPP TS 25.412 and RNSAP in 3GPP TS 25.422 to transport SCCP messages in a packet switched domain.

# 7 SUA Implementation

The transport of the signalling protocols which can be identified as SCCP-users, such as TCAP, BSSAP+, PCAP, SSAP, RANAP and RNSAP, and in turn the transport of TCAP-users such as MAP and CAP, shall be accomplished in accordance with the defined protocol architectures defined in the following sub-clauses.

SUA transports any SS7 SCCP user signalling messages over IP using SCTP between two signalling endpoints. The protocol is able to work in diverse architectures such as an SG to IP signalling endpoint architecture as well as a peer-to-peer IP signalling endpoint architecture. This support allows SUA to carry a protocol that uses the transport services of SCCP, but is contained within an IP network. Depending upon the upper layer protocol supported, the SUA will need to support SCCP connectionless service, SCCP connection oriented service or both services.

## 7.1 SUA In an All IP Environment

SUA allows extra flexibility in developing networks, especially when interaction between legacy systems is not needed.

**NOTE:** SUA, apart from carrying SCCP-User protocols, can also provide an Address Mapping Function (AMF) to route the messages to the next or destination node. The Address Mapping Function, apart from the translations providing the GTT services defined for SS7 networks, modelled in [ITU-T Q.714].

SUA can provide the mapping service through various approaches such as local table lookup or external database access (e.g. ENUM servers) as well as their combination as described below. Please note that these are implementation options.

**Only Local Tables.** This option is done in current SS7 network and most likely will be done in future M3UA implementation, and so will not be explained further in this report.

**Only external database (e.g. enhanced ENUM/DNS Servers).** One could store all the numbers in the external databases (E.164 and E.212/E.214).

Both local tables and external database. In this option external database will be accessed only if mapping cannot be performed using the data from local tables.

This FSY does not recommend one of the options.

Note1: The current ENUM doesn't support E.212 addressing which is required by SCCP GTT, nature address of indicator etc therefore ENUM enhancement is required/needed.

Note2: In order to provide AMF, a proprietary DNS solution can be used.

The Address Mapping Function will be invoked when the routing indicator of the Called Party Address Field is set to:

- Routing is on Global Title
- Routing is on Hostname
- Routing on IP address (or PC)
- Routing on SSN+PC or SSN+IP Address and the address presented is not the one of the relay node
- Routing on SSN and the SUA-user is on the local node

Input to the Address Mapping Function shall be one of the following

- Global Title Information + optional SSN
- Point Code + SSN
- Host Name + optional SSN
- IP Address + SSN
- SSN

Or generally spoken:

- Any valid input address

Note: SSN number is required by SUA to identify the service requested by the upper application layers in ITU-T compliant networks. ANSI networks use a Translation Type instead to identify the service.

The output of the Address Mapping Function shall be one of the following:

- Route on GT: SCTP association ID towards next relay node, (new) GT and optionally SSN and/or Network Appearance.
- Route on SSN+ PC or SSN + IP address: SCTP association ID towards the destination node, SSN and optionally Network Appearance and/or IP address/PC.
- Route on Hostname: SCTP association ID towards next relay node, (new) Hostname and optionally SSN and/or Network Appearance.
- Route on SSN: A local SUA-user (combined relay/end node).

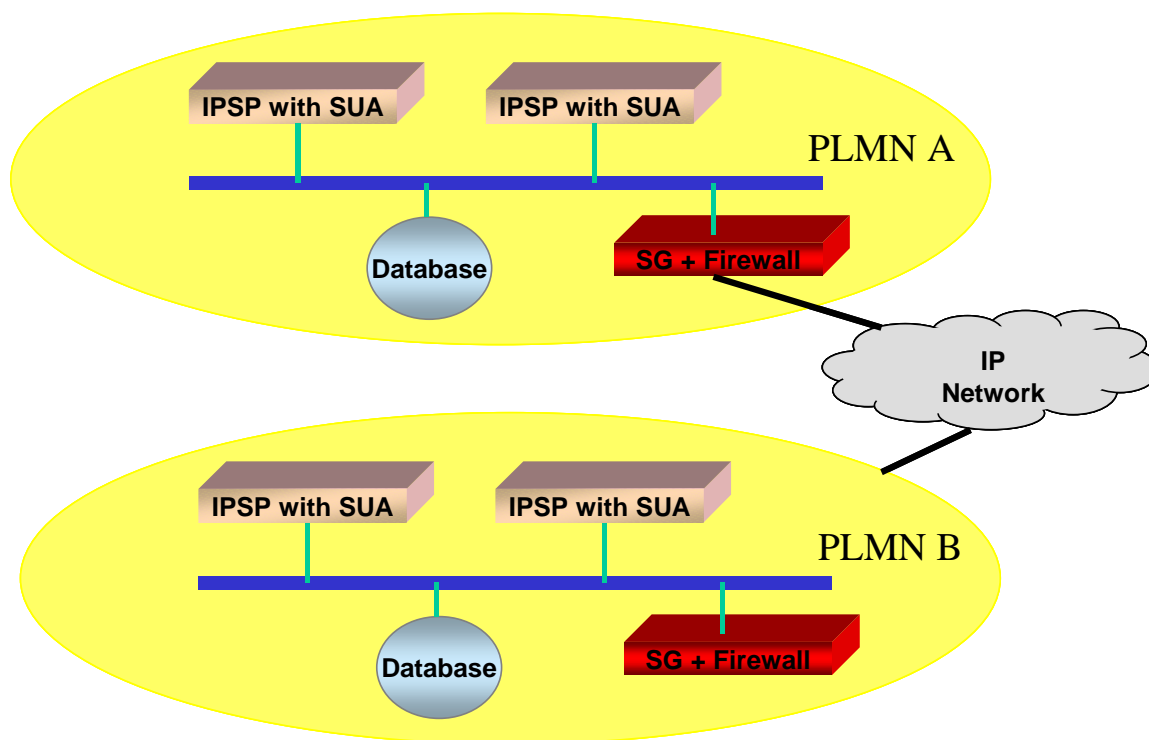
Or generally spoken:

- Any valid output address.

## 7.1.1 Architecture

As described above, SUA locates the next or destination IP node through the Address Mapping Function. In the architecture we also show the presence of Signalling Gateways at the border of the PLMN. As we will see in the later sections, in certain cases, the Signalling Gateway acts as a relay point for messages flowing to/from the PLMNs. In such cases, the SUA messages will be routed by the SG to the destination SUA node based on the GT information or some other means. The SG may be required for other reasons such as security, interfacing with a legacy SS7 network and so on.

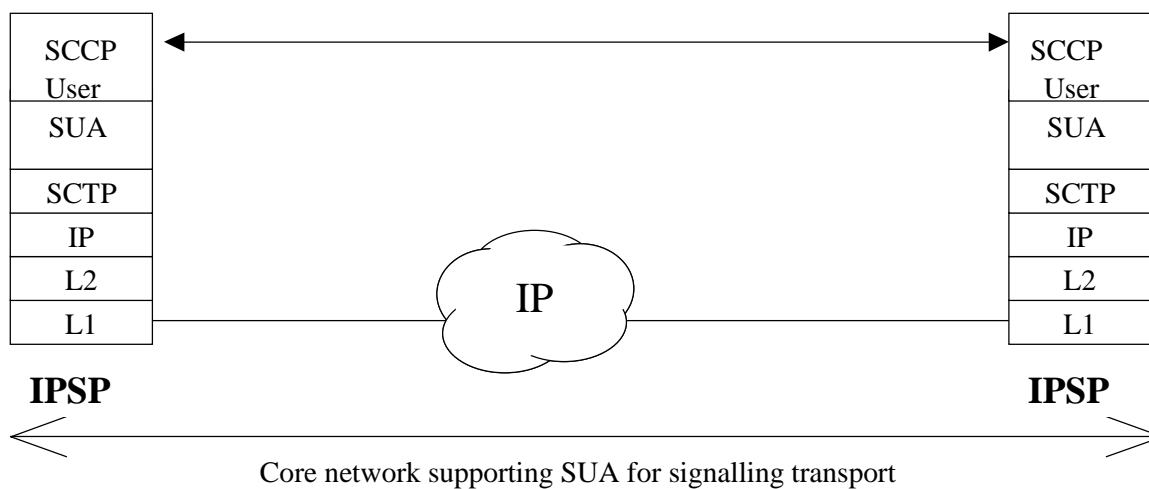
Figure 3 shows a possible realisation of the architecture.



**Figure 3: SUA implementation in an all IP network**

NOTE: SG may provided with SUA Relay function.

Figure 4 shows an example of protocol architecture for SUA transport between IPSPs in all IP scenario.



**Figure 4: Transportation of SCCP-user messages via SUA in an all IP network**

### 7.1.2 Routing SUA Messages in an Intra-PLMN Environment

SUA nodes in figure 3 could be provided with the local tables or external databases to perform the Address Mapping Function. For efficiency, the information in the local tables and/or external database should be sufficient to provide intra-PLMN routing. SUA shall be able to perform the following translations.

- a) Global Title + optional SSN to IP Address + SSN

- b) Host Name + optional SSN to IP Address + SSN
- c) Global Title + optional SSN to IP Address + Global title+ SSN

### 7.1.3 Routing SUA Messages in an Inter-PLMN Environment.

As mentioned above, each SUA node can be provided with local tables and/or external databases containing necessary information for routing the messages within the PLMN. In inter-PLMN roaming cases it relies on the services provided by the AMF for routing the message to the node in a different PLMN. SUA shall be able to perform the following translations.

- a) Global Title + optional SSN to IP Address + SSN
- b) Host Name + optional SSN to IP Address + SSN
- c) Global Title + optional SSN to IP Address + Global title+ SSN

### 7.1.4 Message Segmentation

In an all IP environment, SCTP is responsible for fragmenting the SUA messages. (SUA and M3UA can't fragment/reassemble.) When needed, SCTP fragments user messages to ensure that the SCTP packet passed to the lower layer conforms to the path MTU. On receipt, fragments are reassembled into complete messages before being passed to the SUA layer.

## 7.2 Interworking with Legacy SS7 Network

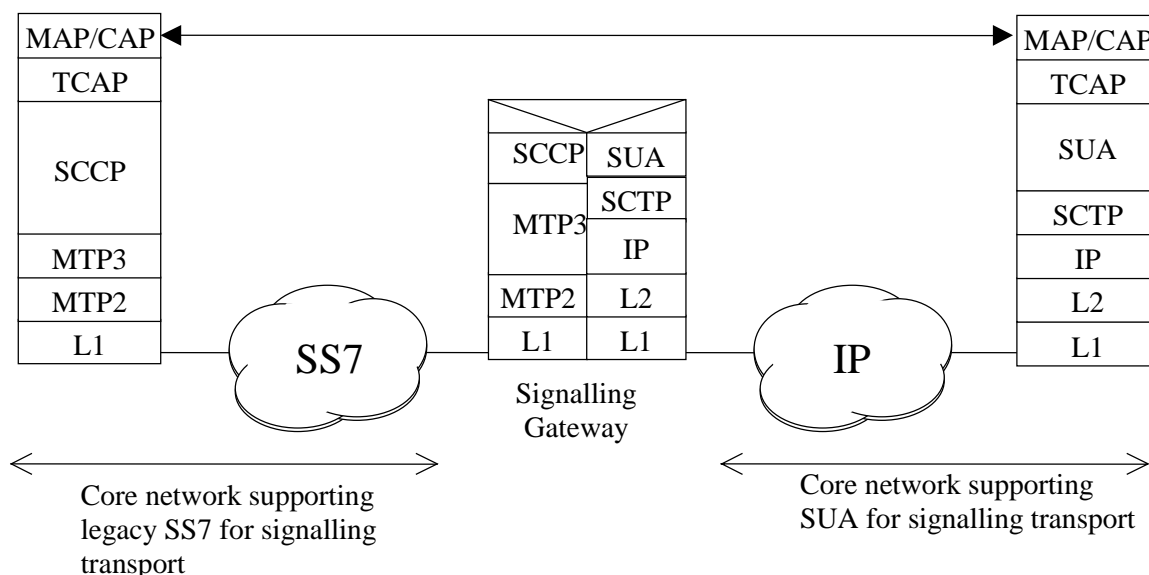
When interworking between SS7 and IP domains is needed, the SG (Signalling Gateway) has to act as the gateway node between the SS7 network and the IP network. The SG will transport the SCCP-User signalling traffic from the SS7 network to the IP-based signalling node and vice-versa.

Comparing to M3UA, please note that there is no difference in case of interworking with legacy SS7 network between SUA and M3UA. One primary requirement when SIGTRAN working group develops the protocols is not to impact existing SS7 nodes. That's why SG is introduced and needed no matter M3UA or SUA is implemented. From SS7 domain's point of view, there are no IP nodes visible to them. The SGs are still viewed as traditional SS7 nodes. Both M3UA and SUA do not introduce change to the legacy SS7 system itself in the backhaul case (SS7 interworking).

### 7.2.1 Architecture

Figure 5 illustrates an architecture that carries an SS7 application protocol (e.g. RANAP, TCAP) between an IP network and an SS7 network.





**Figure 5: SS7 to IP Architecture via SUA**

### 7.2.2 Global Title Management

In a heterogeneous network environment, where multiple IP networks are interconnected with SS7 networks, it is possible that the originating node does not know whether the destination signalling point is in the IP domain or in the SS7 domain. So it is possible that the originating signalling node shall use the services of a gateway to route the message to the destination. Hence, the gateway (*Note: This gateway can be a SG or a separate entity*) providing the GTT services should be able to determine, based on Global Title, the location of the destination (IP or SS7), and route the message to the appropriate entity.

### 7.2.3 Message Segmentation

The fragmentation and assembly on the IP side is handled by the SCTP. For messages, from and to the SS7 networks, message segmentation is provided by the SCCP or SUA layer at the SG.

This matter has been fully considered in the SUA draft. SCTP will handle all IP layer segmentation. SUA handles all of the SCCP segmentation issues. They will not cause any interworking issues.

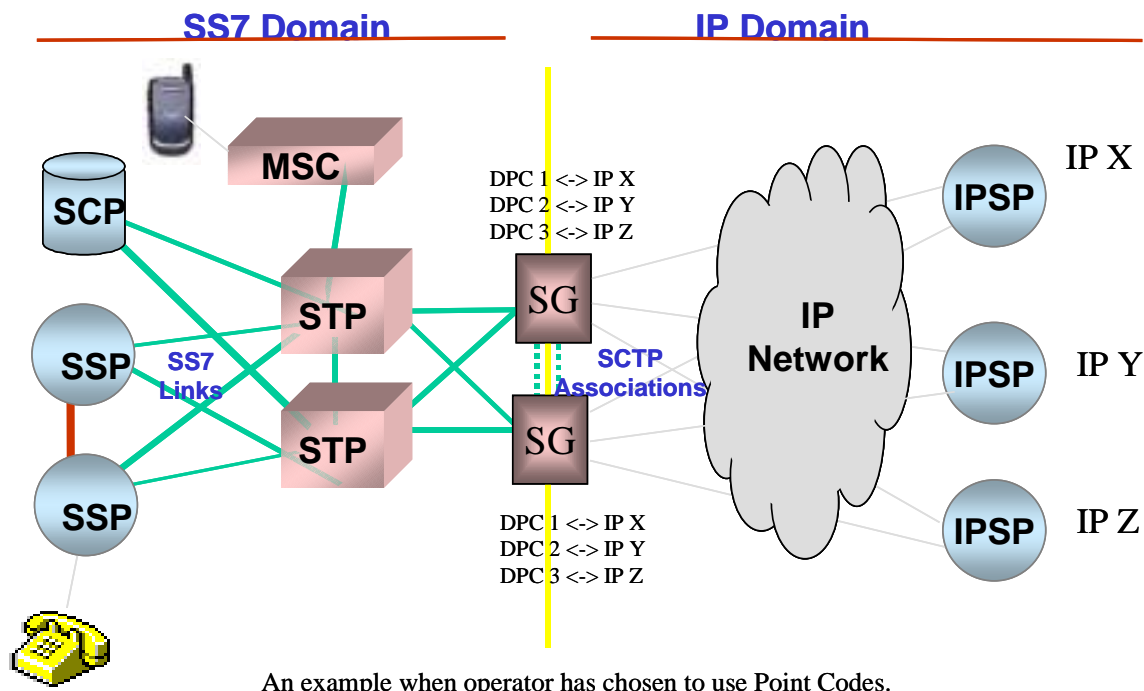
### 7.2.4 SUA Interworking with SCCP Network Management Function

The SUA interworking with SCCP management consists on the sending of DUNA, DAVA, DAUD or SCON messages on receipt of SSP, SSA, SST or SSC to the appropriate ASPs. SUA only interact with SCCP layer and there is no message mapping between SUA and MTP3.

When an SCCP Subsystem Management (SCMG) message is received from the SS7 network, it has to be determined whether there are concerned Application Servers, interested in subsystem status changes. The SUA management function is informed with the N-State indication primitive upon which it formats and transfers the applicable SNM message to the list of concerned ASPs.

When MTP-3 Management indications are received (MTP-PAUSE, MTP-RESUME, MTP-STATUS), SCCP Subsystem Management determines whether there are concerned local SCCP-users. When these local SCCP-users are in fact Application Servers, serviced by ASPs, SUA management is informed with the PC-State indication primitive upon which it formats and transfers the applicable SNM message (DUNA, DAVA or SCON) to the list of concerned ASPs. Vice versa SUA uses the applicable AS/ASP management mechanisms for error handling. When an SG determines that the transport of SS7 messages is encountering problem, the SG triggers SS7 SCCP management messages to originating SS7 nodes, per the procedures of the relevant SCCP standard.

## 7.2.5 AMF implementation example in interworking with legacy SS7 network



**Figure 6: SS7/SIGTRAN interworking example**

Currently, SUA has completed working group last call and has been reissued as version 8. The concept of the AMF is clearly defined in that document. However, below is an example, which shows how the AMF can use the Point Codes or Global Titles for this.

### 7.2.5.1 Point Codes Example

The routing context can be thought of as simply an integer, that specifies which routing key is being used. For example, an SG could have connections to 3 different Application Servers, where each AS is representing a Point Code.

```
SG ----- AS (DPC X)
|
+----- AS (DPC Y)
|
+----- AS (DPC Z)
```

So, the SG could assign Routing Contexts for each AS as the following:

```
Routing Contexts
-----
1      DPC X
2      DPC Y
3      DPC Z
```

Now, the AMF I've always considered as a function that can be used to resolve the SS7 address (Routing Key) to the IP address). So, for example, at startup, the SG may know that it needs to establish connections for the above. So, it uses some external database/local config file to get the IP addresses.

So, for example, there may be some external database which knows:

```
DPC X  IP A
DPC Y  IP B
DPC Z  IP C
```

So, the SG would initialize 3 SCTP associations:

```
SCTP1      IP A
SCTP2      IP B
SCTP3      IP C
```

Then the AMF would probably have a table like this:

SCTP Assoc.	RC	RK
SCTP1	1	DPC X
SCTP2	2	DPC Y
SCTP3	3	DPC Z

At the SCCP/SUA interworking at the SG, when a message comes in from the SS7 network for DPC X, the AMF would look into the table, see that RC = 1 and goes out on SCTP Association 1.

Global Titles example

```
SG ----- AS (GT R)
|
+----- AS (GT S)
|
+----- AS (GT T)
```

So, the SG could assign Routing Contexts for each AS as the following:

Routing Contexts	
1	GT R
2	GT S
3	GT T

Now, the AMF I've always considered as a function that can be used to resolve the SS7 address (Routing Key) to the IP address). So, for example, at startup, the SG may know that it needs to establish connections for the above. So, it uses some external database/local config file to get the IP addresses.

So, for example, there may be some external database which knows:

```
GT R  IP A
GT S  IP B
GT T  IP C
```

So, the SG would initialize 3 SCTP associations:

```
SCTP1      IP A
SCTP2      IP B
SCTP3      IP C
```

Then the AMF would probably have a table like this:

SCTP Assoc.	RC	RK
SCTP1	1	GT R
SCTP2	2	GT S
SCTP3	3	GT T

At the SCCP/SUA interworking at the SG, when a message comes in from the SS7 network for GT R, the AMF would look into the table, see that RC = 1 and goes out on SCTP Association 1.

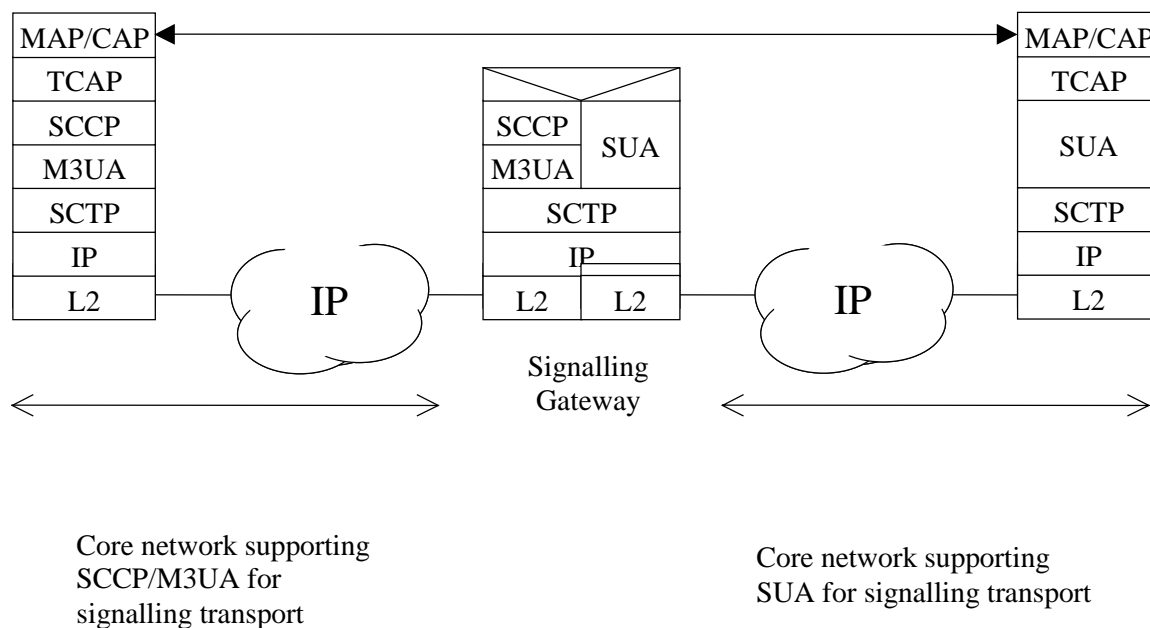
## 7.3 Interworking with SCCP/M3UA

This is very similar to the case when interworking with SCCP/MTP3 in a legacy SS7 network. As illustrated in Figure 7 below, the interworking could be implemented via an SG that effectively relays the signalling messages across the two networks with incompatible signalling transports. In this case, all the SCCP-user messages carried across the two networks pass through the SGW. The SG features an adaptation function on top of SCCP and SUA, which relays messages between these two protocols. The adaptation function of the SG is implementation specific and need not to be standardized.

Please note that SG is needed when operators start to migrate its signalling network from SS7 based to be IP based no matter if M3UA or SUA is used. There are two domains besides SGW. One side is SS7 domain, and another side is IP domain. From the SS7 nodes in SS7 domain, they can only see the SGW as a legacy SS7 nodes, they doesn't feel the change of introduction of IP signalling nodes (no matter M3UA based or SUA based). From the SUA nodes in IP domain, there is no fundamental difference between interworking with SS7 and interworking with SCCP/M3UA as SUA at SGW only deals with SCCP layer, it doesn't care about what is under SCCP, M3UA or MTP3. This has been clearly addressed in SUA FS. From M3UA node point of view, it just simply view SGW as another M3UA node.

### 7.3.1 Architecture

Figure 7 illustrates an architecture that carries an SS7 application protocol (e.g. RANAP, TCAP) between a M3UA IP based network and a SUA IP based network.



**Figure 7: SUA and M3UA interworking with SG**

### 7.3.2 Global Title management

GTT can be done at the SCCP or SUA layer of the SG.

### 7.3.3 Message Segmentation

Since both M3UA and SUA use SCTP, message fragmentation can be handled at the SCTP layer. See section 7.1.5 for more detail.

### 7.3.4 SUA Interworking with SCCP Network Management Function

From SUA point of view, this interworking is similar to section 7.2.4 of SUA interworking with legacy SS7 scenario. As the same, the SUA interworking with SCCP management consists on the sending of DUNA, DAVA, DAUD or

SCON messages on receipt of SSP, SSA, SST or SSC to the appropriate ASPs. Again, SUA only interact with SCCP layer and there is no message mapping between SUA and M3UA.

At M3UA side, M3UA is used in a peer –to-peer fashion, the M3UA layer in an IPSP maintains the state of remote IPSPs. The status is updated by utilizing M3UA Application Server Process Maintenance (ASPM) messages. In this case, SS7 network inter-working is not required, therefore there is no M3UA network management status information for the SCCP and SCCP-User protocols to consider. Any MTP-PAUSE, -RESUME or -STATUS indications from the M3UA to the SCCP should consider the status of the SCTP Association and underlying IP network and any congestion information received from the remote site. The M3UA at SG indicates MTP- primitives to local MTP3-Users (e.g. SCCP) by means of an MTP-Status primitive, as per current MTP3 procedures, to invoke appropriate upper layer responses.

At SUA side, it is identical comparing to interworking with legacy SS7 network. When MTP-3 Management indications are received (MTP-PAUSE, MTP-RESUME, MTP-STATUS), SCCP Subsystem Management determines whether there are concerned local SCCP-users. When these local SCCP-users are in fact Application Servers, serviced by ASPs, SUA management is informed with the PC-State indication primitive upon which it formats and transfers the applicable SNM message (DUNA, DAVA or SCON) to the list of concerned ASPs.

When an SCCP Subsystem Management (SCMG) message is received from the M3UA network, it has to be determined whether there are concerned Application Servers, interested in subsystem status changes. The SUA management function is informed with the N-State indication primitive upon which it formats and transfers the applicable SNM message to the list of concerned ASPs. Vice versa SUA uses the applicable AS/ASP management mechanisms for error handling. When an SG determines that the transport of SS7 messages is encountering problem, the SG triggers SS7 SCCP management messages to originating SS7 nodes, per the procedures of the relevant SCCP standard.

### 7.3.5 Interworking in native SS7 networks

In SS7 both MTP3 and SCCP have several national variants (ETSI, ANSI, China, etc.) that are incompatible with each other. In addition to national variants there is the international version of both protocols (ITU-T) to enable worldwide connectivity between national SS7 networks. As a conclusion it is stated that in SS7 networks whenever there is a need for connectivity between different countries or even between different operators' networks, the application of a Signalling Gateway alike at the edge of each network is a necessity. This applies both for MTP3 and for SCCP. Here the Signalling Gateway is an SP that has an interface to all SS7 networks that are to be connected through it.

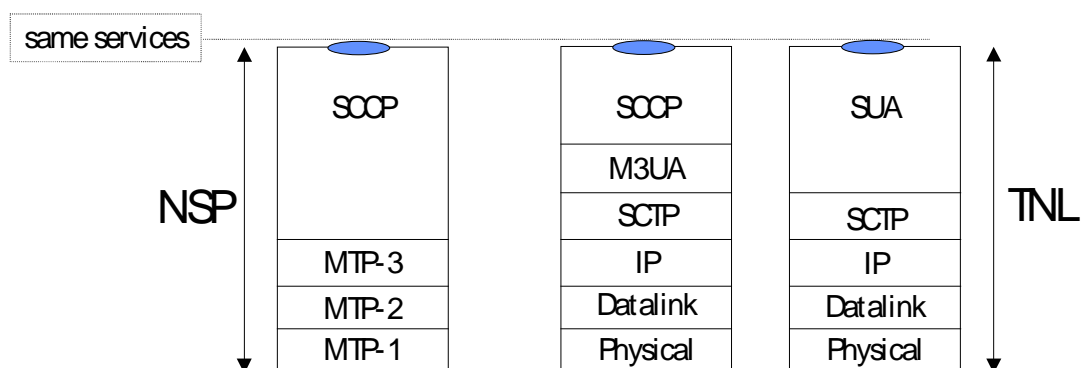


Figure 8: Global SS7 networking

The use of SCCP on top of M3UA makes the availability of a Signalling Gateway a must also in SCCP/M3UA networks. Only in SUA-only environment there is no need for interworking within the signalling network itself.

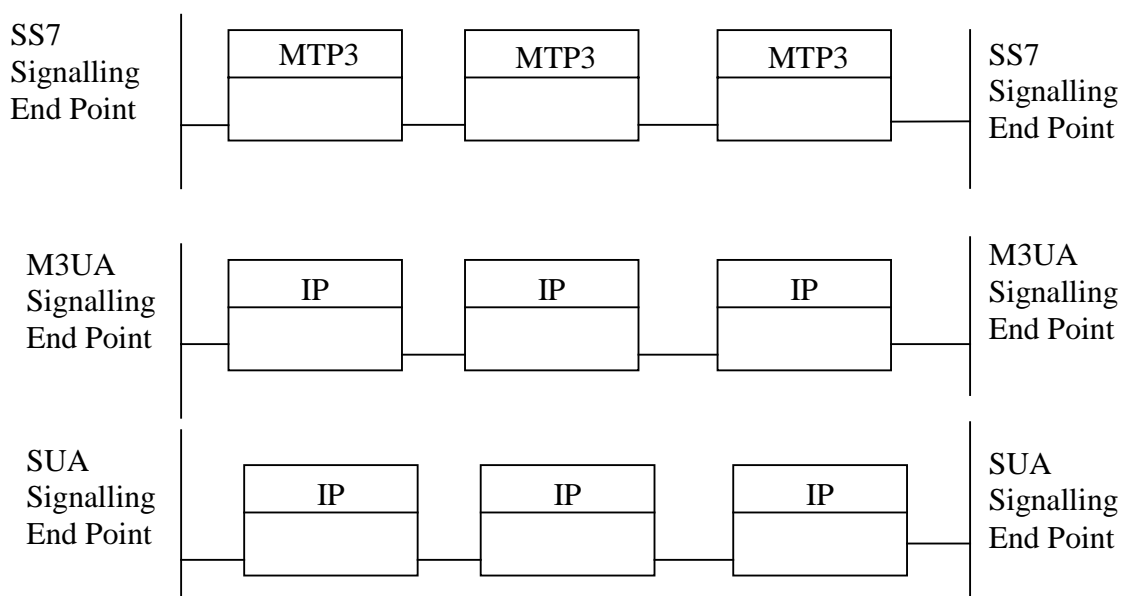
### 7.3.6 Interworking in SS7 and SigTran Networks

In SS7 networks the nodes involved in signalling/signalling transport are called Signalling Points (SP). A signalling Point can be either a Signalling End Point (SEP) or a Signalling Transfer Point (STP). The Transport Network Layer of the SS7 network is called Network Service Part (NSP). In the following figure there are the TNL/NSP of the traditional SS7, of Rel4 IP option and of the proposed SUA based Rel5 IP option.



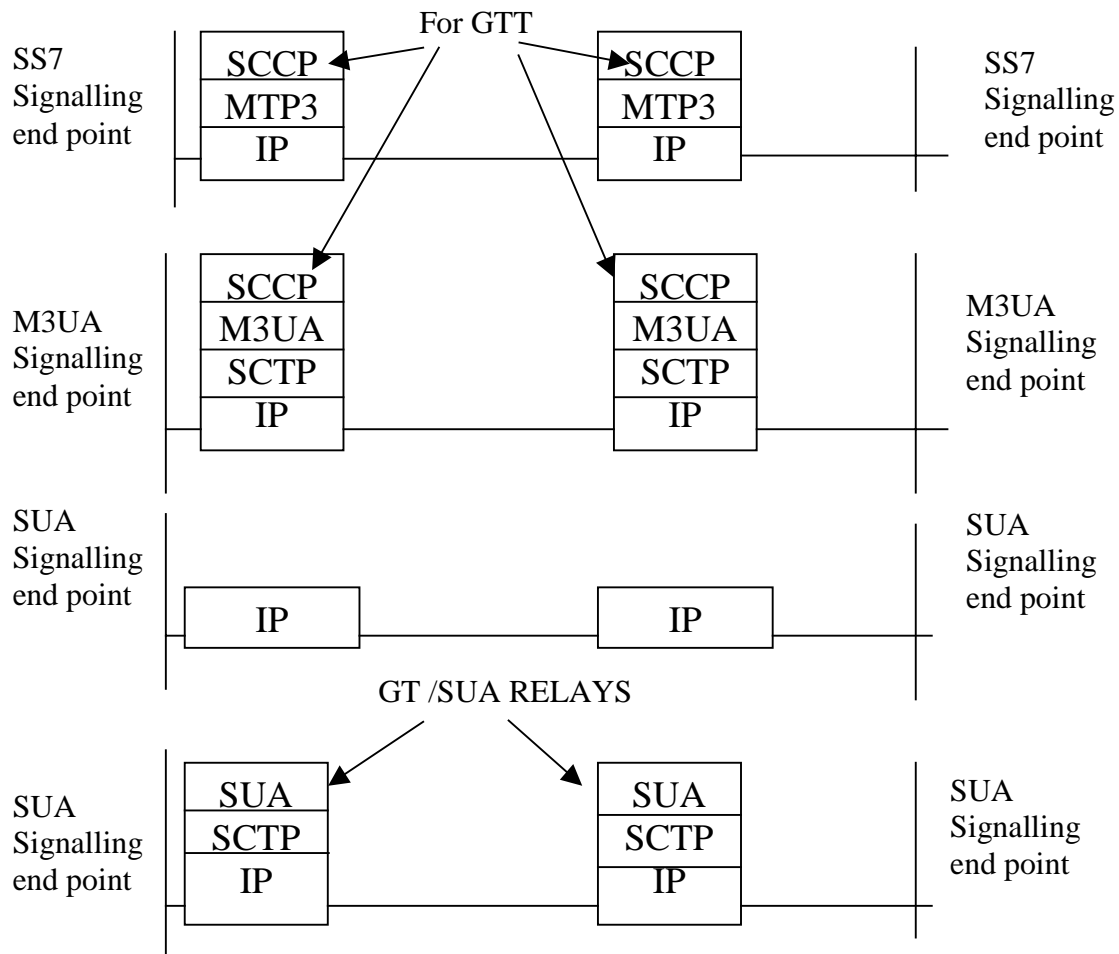
**Figure 9: Network Service Part / Transport Network Layer protocols**

A couple of remarks related to the figure above: In SS7 networks it is the responsibility of a Signalling Transfer Point (STP) to act as a router while the routing is based on MTP-3 (link-by-link) and SCCP (end-to-end). In case of SigTran Internet Protocol provides the networking. It is the role of an ordinary IP router to route the signalling message from the originating Signalling End Point to the destination Signalling End Point. The following figure further illustrates the protocols used in the signalling network between the Signalling End Points. The peer application protocols are only in the Signalling End Points.



**Figure 10: Signalling networking in case of SS7 (top), SCCP/M3UA (middle) and SUA (bottom) – Single Network Case**

Figure 10 shows one MTP network scenario. In such a network, a specific GTT node is not needed, as one can assume the uniqueness of the point code.

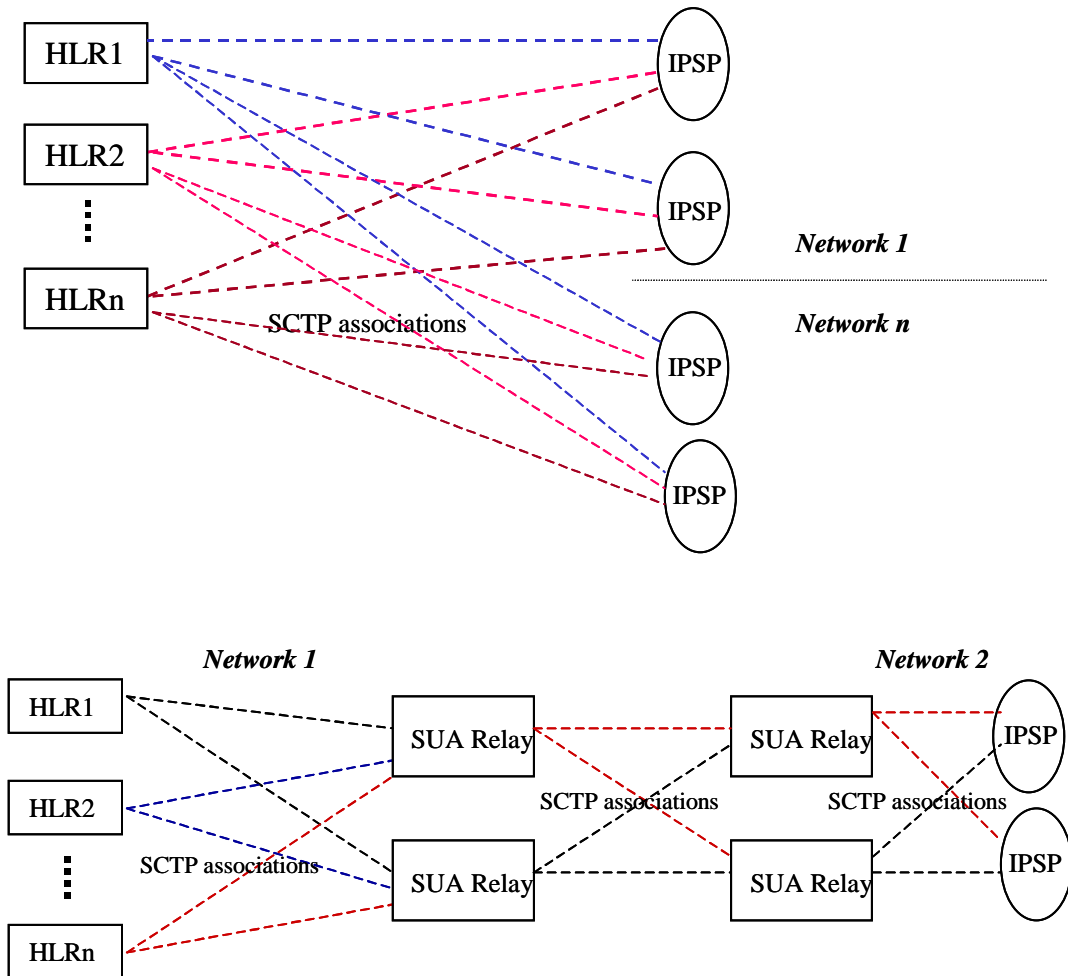


**Figure 11: Signalling networking in case of SS7 (top), SCCP/M3UA (middle), SUA (third) and SUA Relay (bottom) – Multiple Network Case**

For the inter-operator roaming case the corresponding protocol stacks are shown in Figure 11. Note for SUA two different figures are shown. In the first case, only the IP network infrastructure used. To accomplish this, each signalling network knows the endpoints to which it is signalling directly. It can use a method determine how the distant network distributes its subscriber numbers (IMSI / PSTN / ISDN) at the HLRs, such as DNS. In addition each signalling end point must have a SCTP connection to each communication network node in the distant network. The alternative shown in the last figure assumes that each operator has gateways (SUA relays) to each other. This means that the sending operator only needs to know to which operator to send the message to. In addition, it is only required to have SCTP connections between the SUA relays.

From the figures it is seen that in case of SS7 (topmost) the MTP level 3 is involved in every single routing point (i.e., STP) in the network, while in case of SigTran the IP is the protocol involved in routing in the intermediate network. This is the same IP that is used for the routing of all other IP traffic in the given network. In case of SCCP/M3UA (middle) when there is a need for a Global Title Translation (GTT) somewhere in the network, M3UA and SCCP get involved. The GTT must be done in cases where the originating SP is not in the same network as the Signalling Point Code of its peer destination SP. In inter network roaming cases this is a likely scenario (e.g., number of HLRs and MSCs). The signalling message is routed to this GTT-capable SP. This SP then performs the GTT for the Global Title in the received SCCP signalling message. The translation gives the Signalling Point Code of the destination Signalling Point. SCCP attaches this SPC to the routing label it then passes down to MTP-3 (or M3UA) who then routes the message to its destination. In case of SUA (bottom), GTT is only required in the originating SP, because the signalling can be done end-to-end because all involved addresses can have global significance. Global Title Translation is required when Point Codes involved in the transaction are not globally unique. SUA does allow the use of SUA-relay functions, in order to aid network management and inter-operator signalling. However, by using/resolving the Global Titles at the originating node to IP addresses, SUA can work end-to-end and does not require further GTT-functions or STP functional nodes in intermediate nodes, which increase network complexity and expense. It is also noted that the UMTS application protocols (like, MAP/TCAP) do not require Signaling Point Code addressing as such but it is there as one alternative (to GT and SSN or their combination) due to the underlying MTP-3. The network configuration in this case corresponds to the top figure of figure 12.

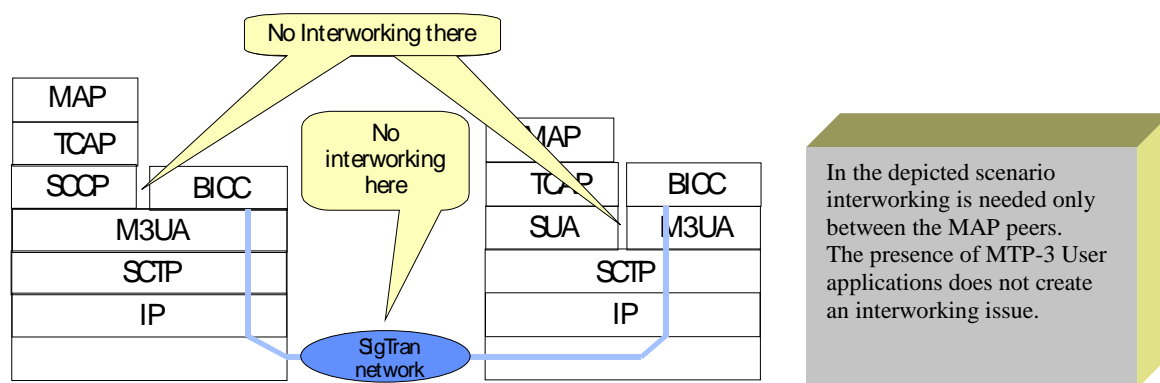
Figure 12 depicts the two way that SCTP associations can be established among IP based signaling nodes, the top one shows the mash network with SCTP associations established between each other. The bottom one shows SCTP associations between two signaling end nodes are bridged through SUA Relay nodes.



**Figure 12: Interconnecting Operator Networks with SUA**

The networking aspect described above is important also because of the following consideration. In the discussions in RAN WG3 the concern has been raised that as there is the Bearer Independent Call Control protocol (BICC) used in the UMTS Core Network and as it is an MTP3 User, inherently incapable of using SCCP or SUA, its presence together with SUA would create an interworking issue. However, the description above showed this concern to be invalid. The interworking is only needed for the peer SCCP User protocols. If there are two BICC peers communicating with each other, then they share the signalling network (i.e., IP network) with SUA Users between their corresponding Signalling End Points. In the Signalling End Points the signalling stacks are e.g., as follows:



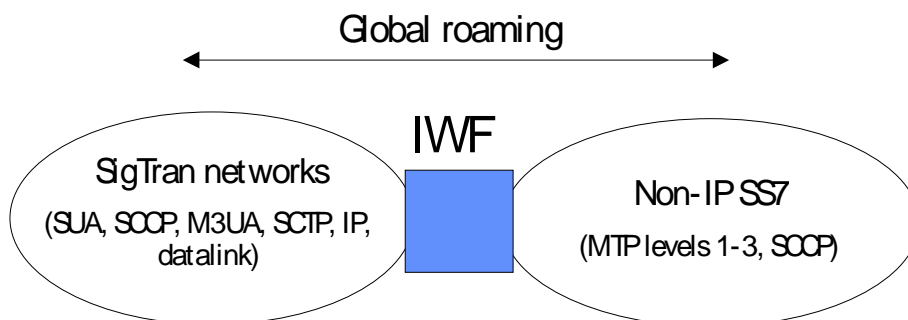


**Figure 13: MTP-3 User (BICC) and SCCP User (MAP) in the same network**

As it is shown in the figure, there are now two Signalling Users present, one is a genuine SCCP User (MAP) while the other is an MTP-3 User (BICC). In the node on the right there are two SCTP Users, one is SUA and the other is M3UA. The same SCTP instance is used to serve both of its users there. In the node on the left the stack is different; there we have two M3UA Users, one is the BICC while the other is the SCCP. The same M3UA instance can serve both of its users. There is no interworking involved that would be caused by the presence of both MTP-3 Users (BICC) using M3UA and SCCP Users (MAP) using SUA.

### 7.3.7 Interworking in 3GPP networks

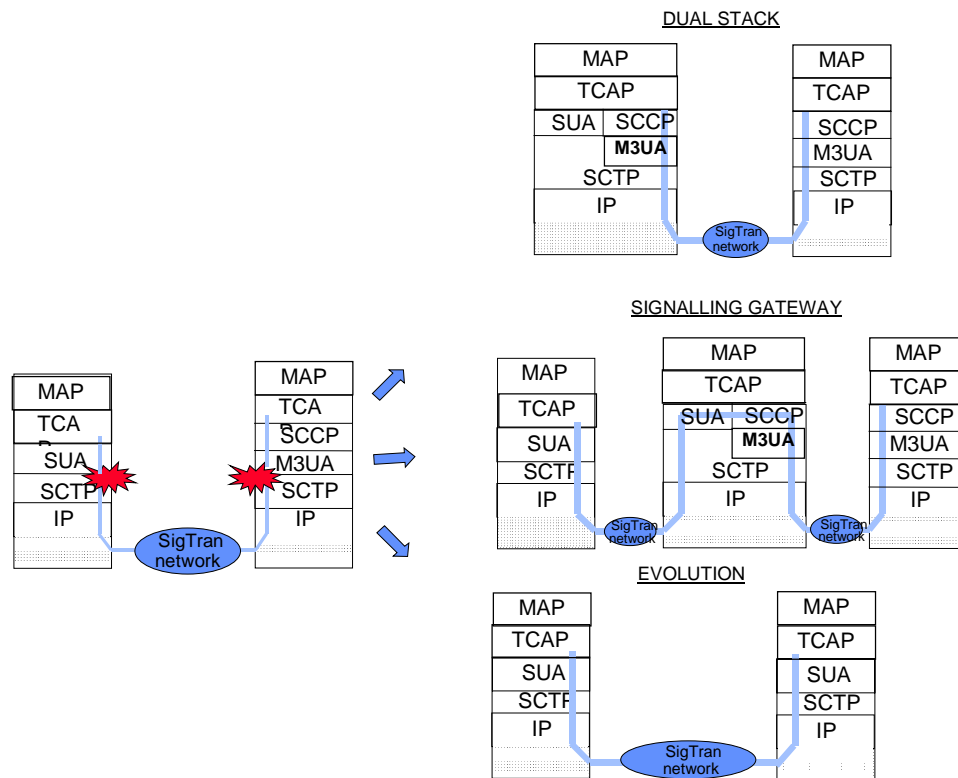
Regardless of which used SigTran adaptation layer is used, there is a need for interworking between the non-IP SS7 network domains and SigTran network domains. The Signalling Gateway needs to offer the protocols and their interworking as shown in Figure 9.



**Figure 14: Interworking in 3G networks between SigTran and non-IP SS7**

Interworking within the SigTran domain is necessary if one of the peer Application protocols peers (e.g., MAP) is using SCCP/M3UA-based SigTran stack while the other is using SUA-based stack. As it was described earlier, there is still no need for interworking in the signalling transport network as such, because of the fact that the signalling transport within the intermediate transport network is carried out by IP protocol and IP routers in both cases. The SCTP and its adaptation layer are implemented only in the Signalling End Point where the Application protocol peers are implemented. The only reason for any interworking in the network would result from the use of more than one SCCP variant in the SCCP/M3UA side of the SigTran domain. In this case the interworking would be purely between the two variants of SCCP.

In the following figure some of the SUA-SCCP interworking options are illustrated.



**Figure 15: Interworking between the SCCP User peers**

As a conclusion for now it is said that the Signalling Interworking Function as such is needed in the 3GPP networks regardless of the application of SUA. This is the case in order to provide global roaming in SS7 environment in general, due to national variants of both MTP-3 and SCCP, and in order to connect non-IP and IP (SigTran) signalling domains together. SUA introduces a need for interworking between the peer SCCP User application protocols in case the other end point is using SCCP/M3UA bearer. However, the intermediate signalling network does not need to be affected by this interworking.

### 7.3.8 SCCP and SUA interworking in detail

SUA is designed to interwork with SCCP seamlessly at a Signaling Gateway. SUA has a class of messages for informing the SS7 network of the availability of the nodes in the IP network, and a class of messages for informing the IP network of the availability of nodes within the SS7 network. For applications running over SCCP or SUA, there is no impact on the interworking of SCCP and SUA at the Signaling Gateway.

Below there are examples of interworking between applications running in the IP domain and applications running in the SS7 domain. The Sigtran Working Group recommends that more than one Application Server Process (ASP) be made available as a Signaling End Point (SEP) within the IP network. MAP would be terminated at the ASP in the IP network.

Because SUA over SCTP does not require the services of MTP3, there is no mapping needed for MTP3 primitives. SigTran has defined a standard model which all adaptation layer protocols support (e.g. – M3UA, SUA, etc.) for reporting of the status of network entities to the SS7 network and from the SS7 network. The Signaling Gateway fully handles all interworking between the SS7 networks and the SigTran networks and the reporting status of the elements.

### 7.3.8.1 Establishment of SUA connectivity

Each involved node is configured with the connections that need to be setup.

ASP 1	ASP 2	SG	SEP
(Primary)	(Backup)		
-----Establish SCTP Association-----			
	-Estab. SCTP Assoc-		
		--Align SS7 link---	

Each IP SEP declares to the SG that it is running.

```

+-----ASP Up----->
<-----ASP Up Ack-----+
      +-----ASP Up----->
      <---ASP Up Ack-----+

```

The Primary IP SEP declares to the SG that it is active. The SG notifies all IP SEPs.

```

+-----ASP Active----->
<-----ASP Active Ack-----+
<-----NTFY (ASP Active)-----+
                                <-NTFY (ASP Active)-+
                                SSA=Destination
                                Subsystem
                                Allowed

```

The SG represents the availability of ASP 1 to the SEP.

```

+-----SSA----->

```

The SEP declares its availability to the SG. Similarly, the SG informs the active ASP of the availability of the SEP as dictated by SGs concerned list. N.B. The SG maps the SS7 address of the SEP to an IP address, which the SG knows ASP 1 will understand.

```

DAVA=Destination
Available
                                <-----SSA-----+
                                <-----DAVA-----+

```

Traffic can now flow. A connectionless flow is shown for simplicity. Nevertheless, the SG is responsible for mapping IP to SS7 addresses and vice-versa. Only the Routing Context for ASP 1 persists from ASP 1 to SEP.

```

+-----CLDT----->
                                +-----UDT----->

```

### 7.3.8.2 SEP Failover

The SEP knows that the SG is 'concerned' about its availability. Similarly, the SG knows that ASP 1 is concerned about the SEPs availability; therefore the incoming SSP is translated into DUNA. ASP 1 uses a DAUD to instruct the SG to invoke the SS7 Sub-system Test procedure.

ASP 1	ASP 2	SG	SEP
(Primary)	(Backup)		
		<-----SSP-----+	
		<-----DUNA-----+	
		+-----DAUD----->	
		+-----SST----->	

### 7.3.8.3 Successful ASP Failover Scenario

The following is an example of a successful failover scenario, where there is a failover from ASP 1 to ASP 2, i.e. Primary to Backup. During the failover, the SG buffers any incoming data messages from the SEP, forwarding them when the Backup becomes available. Traffic can flow normally after the failure.

ASP 1	ASP 2	SG	SEP
(Primary)	(Backup)		
+----- signaling connection lost -----+			
		<-NTFY (ASP Inact.)--+	
		+----ASP Active----->	
		<--ASP Active Ack----	

### 7.3.9 Interworking Conclusions

Based on this contribution the following is concluded.

Signalling Gateway Function is needed in 3GPP networks in order to provide global roaming and in order to interconnect non-IP and IP-signalling (SigTran) networks. This is irrespective of the type of SigTran adaptation layer.

Co-Existence of MTP-3 User application protocols (e.g., BICC) and SUA does not generate need for interworking.

Interworking of SUA and SCCP is needed to connect two application protocol peers (e.g., MAP), one using SCCP/M3UA and the other using SUA. M3UA and SUA as SigTran protocols have common network layer in the intermediate signalling network.

Interworking of SUA and SCCP is an integral part of the SUA specification. The Signalling Gateway functionality is a key feature of SUA protocol. In interworking the Signalling Gateway represents the SUA endpoint to SCCP/M3UA endpoint and vice versa.

---

## 8 Services Impact

The support of SUA in a network shall not affect the handling of supplementary service for the subscribers. As discussed earlier in this document, SUA fully supports TCAP, and hence CAP and MAP protocols are supported. Therefore, any applications that use either MAP or CAP protocol (e.g. SMS, CAMEL, etc) shall not be impacted by using the SUA protocol in the core network. In this section services specified for 3G networks will be listed along with their impact due to the introduction of SUA in the core network.

### 8.1 Calling line identification presentation (CLIP)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.081

### 8.2 Calling line identification restriction (CLIR)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.081

### 8.3 Connected line identification presentation (COLP)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.081

### 8.4 Connected line identification restriction (COLR)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.081

## 8.5 Call Forwarding Unconditional (CFU)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.082

## 8.6 Call Forwarding on mobile subscriber Busy (CFB)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.082

## 8.7 Call Forwarding on No Reply (CFNRy)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.082

## 8.8 Call Forwarding on mobile subscriber Not Reachable (CFNRc)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.082

## 8.9 Call Waiting (CW)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.083

## 8.10 Call hold (HOLD)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.083

## 8.11 Multiparty services (MPTY)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.084

## 8.12 Closed User Group

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.085

## 8.13 Advice of Charge services

No impact. All the SCCP functions required for this service are fully supported by SUA. See 22.086

## 8.14 Barring of All Outgoing Calls (BAOC)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.088

## 8.15 Barring of Outgoing International Calls (BOIC)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.088

## 8.16 Barring of Outgoing International Calls except those directed to the Home PLMN Country (BOIC-exHC)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.088

## 8.17 Barring of All Incoming Calls (BAIC)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.088

## 8.18 Barring of Incoming Calls when roaming outside the home PLMN country (BIC-Roam)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.088

## 8.19 Explicit Call Transfer (ECT)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.091

## 8.20 Completion of Calls to Busy Subscriber (CCBS)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.093

## 8.21 Support of Private Numbering Plan (SPNP)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.095

## 8.22 Multiple Subscriber Profile (MSP)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.097

## 8.23 enhanced Multi-Level Priority and Pre-emption (eMLPP)

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.067

## 8.24 SMS

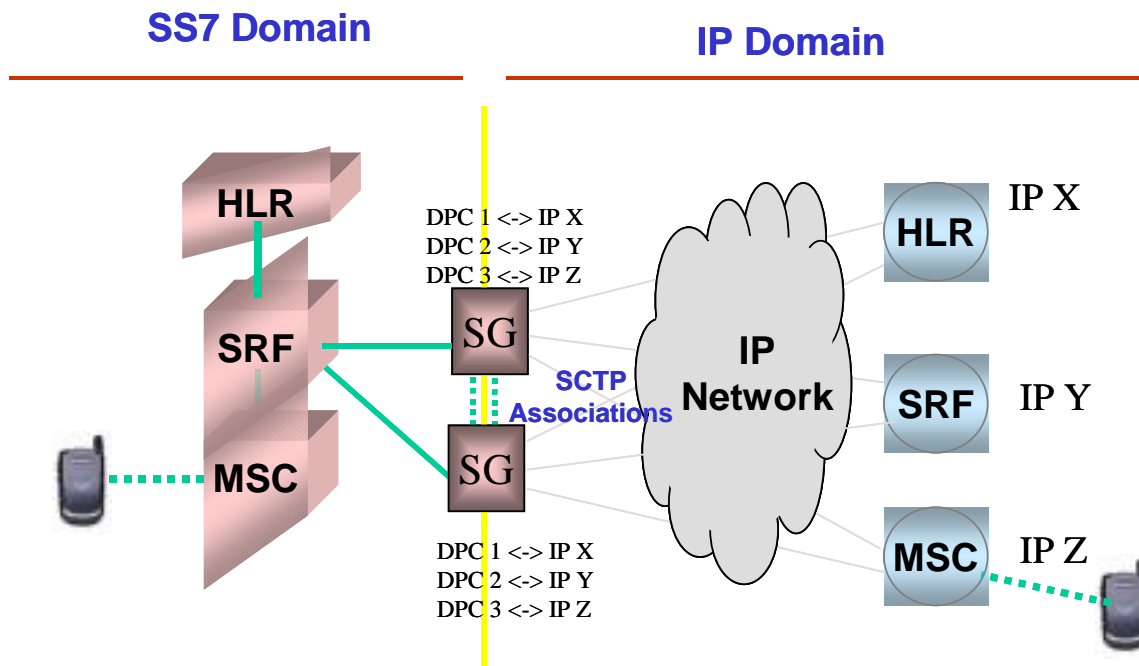
No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 23.040

## 8.25 CAMEL

No impact. All the SCCP functions required for this service are fully supported by SUA. See TS 22.078

## 8.26 Mobile Number Portability

No impact. All the SCCP functions required for MNP are fully supported by SUA. See TS 22.066



MNP example with one PLMN in SS7 domain and another PLMN in IP domain.

**Figure 16: An illustration example of MNP**

Given an example here, in a scenario where the donor HLR returns a DPC (or GT) of the HLR where MS has ported to, the MSC->SRF shall send the SRI to that HLR via the SG. The SG maps the DPC (or GT) to an IP address associated with that HLR. That HLR shall send the response to the MSC via the SG. Subsequently the MSC uses the MSRN to route the call to the ported MS.

## 9 Security

SUA could be protected by IPsec at the IP layer. The application of IPsec for native IP protocols is defined in TS 33.200 "Network Domain Security" (see [4]), where the protection of MAP over SS7 is separately defined at the application layer.

For SUA, it is reasonable to assume that all the network entities are IP capable. We can further assume that each network entity is able to negotiate security associations with its intra-domain peer by Internet Key Exchange (IKE) protocol. The negotiation and management of inter-domain security association for SUA should align with the specifications in TS 33.200 for native IP protocols.

Compared with MAP over SS7, the security of SUA is enhanced in the sense that a security association will be established for especially one peer in one direction. Network wide security associations as they have been used for MAP over SS7 will be used for all the peers between two given networks. If any peer happens to use the security association in an improper way and to weaken it, then all the protection for the communications between the two networks during the lifetime of the network wide security association may be jeopardized.

In IETF RFC 2719 "Framework Architecture for Signaling Transport" (see [10]), it was suggested to use IPsec to protect the signaling at the IP layer. It was pointed out that "it is recommended that IPsec or some equivalent method be used, especially when transporting SCN signalling over public Internet."

A recent IETF internet draft "On the Use of SCTP with IPsec" (see [19]) described functional requirements for IPsec and IKE to facilitate their use for securing SCTP traffic. It further addressed the detailed IPsec extensions to cope with multiple destination addresses used in SCTP for a given Security Association (SA).

Therefore, using IPsec to protect SUA is consistent with SCTP specifications in IETF.

Meanwhile, the COOKIE mechanism for SCTP provides extra security.

---

## 10 Network Evolution and Interworking Scenarios

It is the trend that the operators gradually migrate their SS7 based signalling network into IP based signalling network. Assuming the operators eventually will get a pure IP network. Sooner or later, the legacy SS7 network nodes have to be upgraded to support IP, both M3UA and SUA will make change to legacy system itself in all IP case. In an all IP environment, there is no message can not be routed through its IP address. The GT->PC->IP address translation can be considered as a waste and extra cost to network performance. Also, more translations required introduce more possibilities for mis-configuration.

Additionally, it is doubtful that Point Code -> IP address functionality needed in M3UA could be located locally only. IP host tend to be quite dynamic & require some co-ordination as hosts and their interfaces change. Also, SUA can handle the Global title -> IP address functionally locally as well, but introduces the able to centralize this function as well (please note that SUA allows point code -> IP address functionality as well). In a realistic scenario, operators could add hosts and/or interfaces to HLRs/HSSs as their subscriber base grows. By adding a centralized server (even a O&M server) which describes what the local GT, Point Code & IP addresses of the network elements & interfaces are, Network management is greatly simplified. It can be viewed as advantageous for any network, not just SUA - but also for M3UA.

A number of concerns have been expressed about the interaction between Release 99, Release 4 and Release 5 core networks. This chapter aims to show that SUA does not negatively affect an operator's network evolution.

### Scenario 1

An operator may choose to forgo Release 4 when upgrading a Release 99 core network to a Release 5 core network. In this case, the network operator will not have to worry about existing M3UA deployment with its network. It can directly deploy SUA for transport MAP and CAP. The operator should take steps to interwork with other operator's M3UA enabled core networks. This can be done via Signaling Gateways (via the SS7 network domain) or by deploying SGs which support both SCCP/M3UA and SUA.

### Scenario 2

An operator with an existing Release 4 core network may wish to add network nodes which support SUA. In this case, interworking can still be managed via the Signaling Gateway or via a Signaling Gateway which supports both SUA and SCCP/M3UA. SUA will interwork with SCCP layers at a SG seamless, irrespective if SCCP is over M3UA or MTP3. Via this SG, the SUA enabled nodes can communicate with all other nodes.

### Scenario 3

A Greenfield operator wishing to deploy a full VoIP enabled network may wish to deploy a network free of legacy protocols, as much as possible. By using a SIP-ISUP interworking gateway, and a Signaling Gateway for interworking with PSTN signalling, the operator can have its signalling needs met by SUA.

### Scenario 4

An operator with no need of IP signalling networks can be unaffected by SUA, as operators deploying IP signalling networks are required to interwork with SS7 networks via Signaling Gateways.

### Scenario 5

An operator who want to keep M3UA can be unaffected by SUA, as operators deploying SUA are required to interwork with M3UA based networks via Signaling Gateways.



---

## 11 Benefits and Drawbacks

### 11.1 Benefits:

#### 11.1.1 Benefits perceived by some companies:

One less protocol layer with elimination of SCCP reduces the complexity of the network node (implementation as well as management) therefore saves cost.

SUA allows the IP network to route the messages. This is an advantage of SUA (routed) over M3UA (Point to Point) in the all IP scenario as M3UA needs to be routed on point codes, while SUA messages can be routed using IP addresses.

SUA provides much better scalability and flexibility for signalling network implementation in all IP network compared to the SCCP/M3UA option. M3UA overlays a hop-by-hop, connectionless protocol mechanism over an end-to-end, connection-oriented protocol. The result of this leads to flexibility and scalability issues.

The powerful end-to-end addressing and routing capability of SUA can greatly reduce the signalling transfer latency.

The M3UA nodes need to be addressed by point codes at M3UA layer and by IP addresses at IP layer. Additionally, in the all IP network, the network operators are not required to allocate, assign and administer point codes to network nodes.

There are some function redundancies in SCCP/M3UA/SCTP stack mode e.g. message segmentation and reassembling mechanism are specified at both SCTP layer and SCCP layer. SUA removes some of the functional redundancies, thus better utilizing network and processor.

The capabilities of SUA make SCCP and M3UA unnecessary and SUA can be considered preferable in terms of efficiency and implementation complexity.

In future all IP network, SIP based all IP mechanism transported over SUA enabled GPRS networks would be advantages over an interim M3UA solution.

M3UA requires management of two mapping tables to find out the IP address of the peer signalling end point (Adds complexity).

M3UA requires two lookups, one to map the Global Title to the point code and another to map the point code to the IP address. This Adds processing delay.

M3UA requires SCCP node to be configured with both the point code and the IP address even in all IP case.

In all IP case, with SCCP sitting on top of M3UA plus widely deployed SCCP local lookup tables, it is not easy to use standard IP name services such as DNS/ENUM for managing the mapping tables (Mobile number to Point code and point code to IP address).

With M3UA, flexibility of IP routing cannot be easily utilised without maintaining large amounts of network wide data at each node. So messages are sent hop by hop when point codes addressing mechanism is used.

#### 11.1.2 Benefits agreed by all companies

When using SCCP over M3UA, different flavours of SCCP are needed to inter-operate with different national systems. This problem is reduced with SUA.

SUA allows the messages routing using Global Titles without involvement of point codes in IP-to-IP case.

With SUA each IP node may not consume point code resources in all IP case.

## 11.2 Drawbacks

### 11.2.1 Drawbacks outlined by some companies

Some networks and implementations are using SPC as a means to identify nodes in OA&M.

The introduction of SUA as an alternative to M3UA+SCCP will introduce options in implementations, which will sooner or later lead to increased cost.

SUA cannot cater for all needs for an operator.

The operator can apply similar principles for network planning, network management and network operation as for the MTP network.

The operator can reuse the GT analysis already provided by data builds in SCCP, which is proven to work in existing networks

In future all IP network, SIP based all IP mechanism would be advantages over an interim SUA solution .

### 11.2.2 Drawbacks agreed by all companies

SUA doesn't support MTP3-user protocols such as ISUP and BICC.

Interworking between SUA and SCCP/M3UA is introduced. Interworking between an operator who has deployed an M3UA only network and an operator who has deployed an SUA only network can be done via the Signaling Gateways used to interwork with the legacy SS7 network. Alternatively, the SUA operator should provide the means to interwork.

Some operators may wish to use common principles for network planning, network management and network operation as for the MTP network. However, it assumes that administering an M3UA would be similar to the administration of an MTP3 network.

In a node with Release 4 functionality the additions of a new protocol may impose additional cost for training, testing, new equipment (protocol analyser).

The introduction of SUA as an alternative to M3UA+SCCP will introduce options in the networks, and between networks.

An SUA message is longer than the corresponding combination of M3UA + SCCP messages.

## 11.3 Neutral Points agreed by all companies

IPSec can be used as a general mechanism to protect MAP and CAP messages. This applies to M3UA too.

For point-to-point links, M3UA allows for IP routing between the signalling endpoints, as does SUA.

The release 4 "SS 7 protocol" signalling transports cater for all signalling transport needs in Release 5.

When there is interworking between IP and SS7, nodes in the IP domain require signalling point codes.

---

## 12 Open Issues

For using IPSec to protect SUA, the following open issues need further study: whether both IPSec transport mode and IPSec tunnel mode are applicable to SUA or only one mode. It may depend on the version of IP protocol to be used and maybe other network configuration issues. This also applies to M3UA.

There might be a new version of SCTP due to checksum problem. This will create a backward compatibility problem of different SCTP versions. This issue applies to both SUA and M3UA.

---

## 13 Conclusion

Unfortunately it has not been possible to reach consensus in CN4 on whether or not to recommend that CN4 proceed with specifying the possible use of SUA for the transport of the BSSAP+, CAP and MAP protocols.

CN plenary are asked to decide how any further work should proceed.

---

## 14 Work Plan

CN4#8	May 14-18, 2001	Presentation of the TR to CN4 for approval.
CN#12	June 18-22, 2001	Presentation of the TR to CN for information.
CN4#9	July 9-13, 2001	Presentation of the TR to CN4 for discussion.
CN#14	Dec 12-14, 2001	Presentation of the TR to CN for approval.

---

## Annex A: Procedure for Message Routing with DNS/ENUM

### A.1 Routing Using Provided E.164 (MSISDN) Number

The following steps illustrate the process involved in routing the SUA messages using provided E.164 (MSISDN) number.

The SUA receives the E.164 number and SSN from its upper layers (In Called Party Address parameter) [MS: I am referring to destination address which will be called party rather than calling party]

The SUA with the AMF attempts to map the E.164 number + SSN to an IP address. Because the number is for the subscriber from a different PLMN, it cannot find a mapping IP address.

The SUA then constructs the domain name from the E.164 number and send a DNS query to the local ENUM server for the URIs associated with the constructed domain name. The ENUM server, by following the referrals, forwards the original query to the Authorised ENUM server (ENUM server in the target PLMN). The Authorised Name server either returns a list of IP addresses or URIs associated with the domain name (constructed from E.164 number) or an error code. The result is then be forwarded to the SUA. Recall that the returned IP address or URI is for the destination SUA node and not the SG (no need to go through the SG). URIs will be resolved with IP addresses.

From the list of IP address(es) returned, the SUA has to pick the IP address associated with the service represented by the SSN.

The SUA message is passed down to the SCTP layer and SCTP checks whether the association was established between two nodes. As stated before, the SCTP association should be up and available all the time. SCTP is responsible for setting up the association with destination IP address if the association is not already established. Therefore the SUA message is sent to the IP address found in Step 4. If the address returned in step 4 is of SG's, then the SG shall be responsible for routing the message to the destination SUA node. The destination SUA node routes the message to the application identified by the parameters in the Called Party Address.

Since DNS queries across PLMNs can sometimes take a while, the following enhancements are recommended to improve system performance:

Local ENUM servers or SUA nodes cache the information so subsequent queries need not cross PLMN boundaries. Caching remote DNS data is a standardised mechanism in DNS service. However, care should be taken to invalidate the cache after TTL expires (TTL is returned as part of DNS result). Applications should also be able to handle error conditions (Cache pointing to an invalid node) and re-request the data.

ENUM server lookup to be performed by the SG. In this case, if the originating SUA node cannot find an entry in its local lookup tables it has to forward the SUA message to a SG within the PLMN. Selection of the SG is implementation dependent.

---

### A.2 Routing Using Provided E.212 (IMSI) Number

In this section we will discuss two options; one based on E.164 addressing information and another based on E.212 addressing information.

#### A.2.1 Routing using E.214 addressing information

The following steps illustrate the process involved in routing the SUA messages using the provided E.212 (IMSI) number with conversion to E.214 (GMT) number.

The SUA receives E.212 number and SSN (Optional) from its upper layers (In Called Party Address parameter)

The SUA with the AMF attempts to map the E.212 number + SSN (Optional) to an IP address. Because the number is for the subscriber from a different PLMN, it may not find a mapping IP address if the data is not cached after ENUM request or the caching expired.

The SUA then extracts the *MCC* and *MNC* values from the E.212 number. In order to hide the IMSI structure, *CC* and *NDC* (Part of E.164 number) should be derived from *MCC* and *MNC* values.

The SUA will construct the domain name from the derived *CC* and *NDC* values. A DNS query will be sent to the local ENUM server to retrieve the URI, in the form of x@hostname or y@ipaddress, associated with the domain constructed above. URIs will be resolved with IP addresses.

If necessary, the ENUM server, by following the referrals, forwards the original query to the Authorised ENUM server. The Authorised ENUM server either returns a list of URIs associated with the domain name or an error code. The result is then forwarded to the SUA. Recall that the address returned by the ENUM server will be one of the following:

IP address of the SG of the target PLMN

Host name corresponding to a pool of SGs in case of multiple SGs in the target PLMN (for redundancy and load sharing).

The SUA message is passed down to the SCTP layer and SCTP checks whether the association was established between two nodes. As stated before, the SCTP association should be up and available all the time. SCTP is responsible for setting up the association with destination IP address if the association is not already established. Therefore the SUA message is sent to the IP address received in Step 5. The message will be sent with the following information:

Routing Indicator Set to Route on GT:

Address Parameter with Global Title (Converted from E.212 to E.214) and SSN

When the SG at the destination PLMN receives the message it will look up its internal table to derive the destination SUA node's IP address from the Global Title and SSN information of the SUA.

A message will be sent to the destination SUA node. The destination SUA node routes the message to the application identified by the SSN in the Called Party Address parameter.

Because DNS queries across PLMNs can sometimes take several seconds, the following options are available to improve system performance:

Local ENUM servers or SUA nodes cache the information so subsequent queries need not cross PLMN boundaries. Caching remote DNS data is a standardised mechanism in DNS service. However, care should be taken to invalidate the cache after TTL expires (TTL is returned as part of the DNS result). Applications should also be able to handle error conditions (Cache pointing to an invalid node) and re-request the data.

ENUM server lookup is to be performed by the SG. In this case, if the origination SUA node cannot find a matching entry in its local tables, it has to forward the SUA message to a SG within the PLMN. Selection of the SG is implementation dependent.

## A.2.2 Routing using E.212 addressing information

As mentioned earlier, this option requires IETF to define standards to store E.212 numbers in the ENUM server.

The following steps illustrate the process involved in routing the SUA messages using the provided E.212 (IMSI) number.

The SUA receives E.212 number and SSN (Optional) from its upper layers (In Called Party Address parameter)

The SUA with the AMF attempts to map the E.212 number + SSN (Optional) to an IP address. Because the number is for the subscriber from a different PLMN, it may not find a mapping IP address if the data is not cached after previous ENUM request or the caching expired.

The SUA then constructs the domain name from the E.212 number using a similar approach defined for E.164 numbers in RFC 2916. Assuming the name belongs to e212.arpa domain. A DNS query will then be sent to the local ENUM server to retrieve the URI, in the form of x@hostname or y@ipaddress, associated with the domain name constructed above. URIs will be resolved with IP addresses.

The ENUM server, by following the referrals, forwards the original query to the Authorised ENUM server. The Authorised ENUM server either returns a list of URIs associated with the domain name or an error code. The result is then forwarded to the SUA. Recall that the address returned by the ENUM server will be one of the following:

IP address/Host name of the SG of the target PLMN (For reasons such as security e.t.c)

IP Address/Host name of the target service node.

The SUA message is passed down to the SCTP layer and SCTP checks whether the association was established between two nodes. As stated before, the SCTP association should be up and available all the time. SCTP is responsible for setting up the association with destined IP address if not. Therefore the SUA message is sent with SSN to the IP address received in Step 5. If the address returned in step 5 is of SG's, then the SG shall be responsible for routing the message to the destination service node.`

---

## Annex B: Document History

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2001-03					Document created		0.0.1
2001-06					Document revised based on comments from CN4#8 meeting.	0.0.1	0.1.1
2001-07					Document revised based on comments from CN4#9 meeting.	0.1.1	0.2.0
2001-10					Document revised based on comments from CN4#10 meeting.	0.3.0	0.3.1
2001-11					Document rised to v.2.0.0 and sent to CN#14 for approval	0.3.1	2.0.0
2001-12					Approved at CN#14	2.0.0	5.0.0