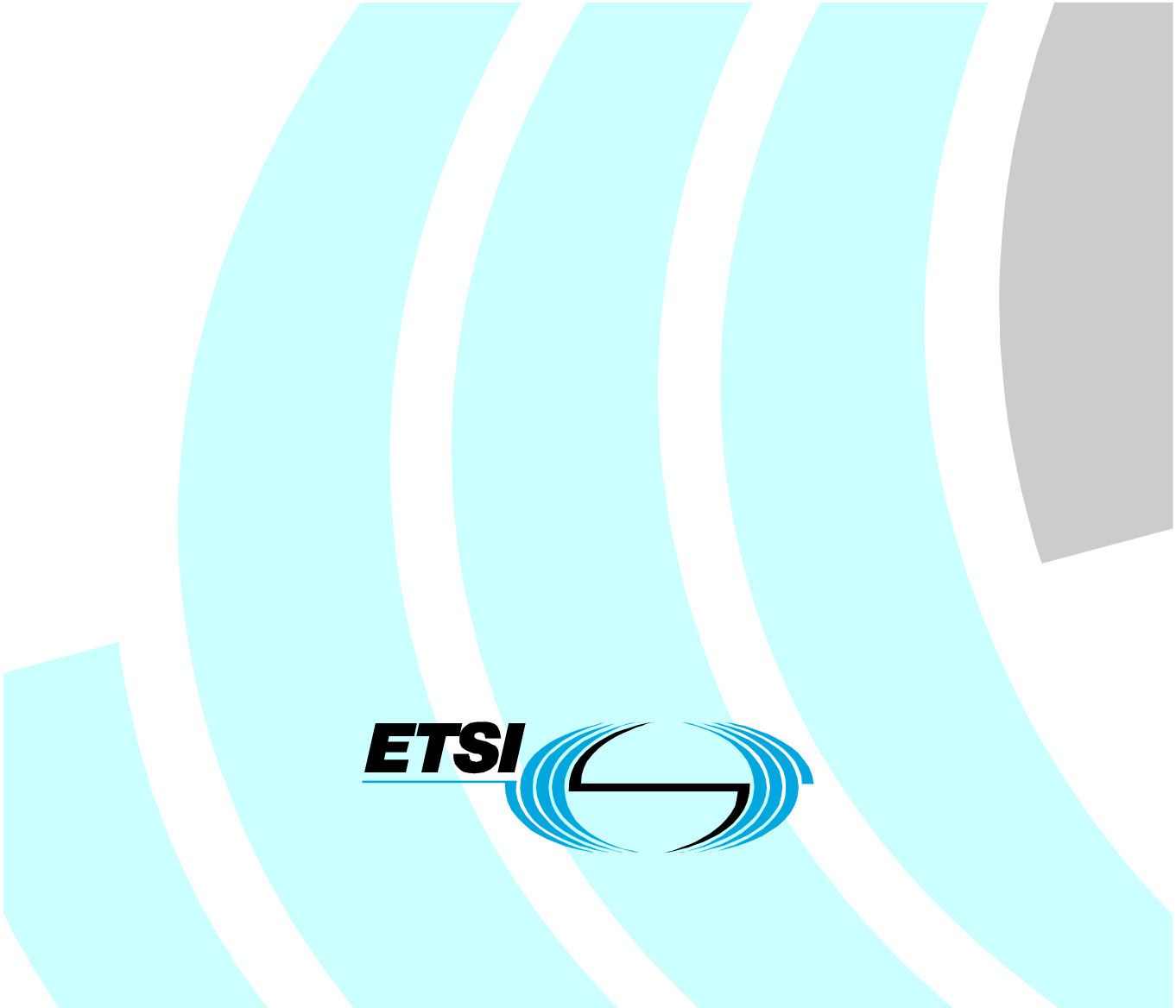
ETSI TR 183 032 V1.1.1 (2006-05)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study into mechanisms for the support of encapsulated ISUP information in IMS



Reference
DTR/TISPAN-03059-NGN-R1

Keywords
IMS, ISUP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

The present document (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document addresses issues for the support of ISUP information between IMS entities when used in an NGN, i.e. MGCF to MGCF, MGCF to AS, AS to MGCF, AGCF to AS, and possibly AS to AS.

The present document provides a home for text for incorporation into other deliverables once the documentation structure has been decided.

A number of potential use cases exist for such a mechanism, e.g. PSTN to PSTN bridging using IMS, support of service information to AS from MGCF in simulation services, support of the IMS based PSTN/ISDN emulation subsystem, but it is not in the scope of the present document to provide information relating to use of this mechanism to support such use cases. Such use of this mechanism will be dealt with by other work items.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ETSI TS 181 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Multimedia Telephony with PSTN/ISDN simulation services".

[2] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements".

[3] ETSI TS 183 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Conference (CONF); Protocol specification".

[4] ETSI TS 183 016 : "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol specification".

[5] ETSI TS 183 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

[6] ETSI TS 183 042: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN IMS Supplementary Services; Call Completion on Busy Subscriber (CCBS), Call Completion No Reply (CCNR)".

[7] ETSI ES 201 296: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP); Signalling aspects of charging".

[8] ETSI EN 383 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control (BICC) Protocol or ISDN User Part (ISUP) [ITU-T Recommendation Q.1912.5, modified]".

[9] ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

[10] ITU-T Recommendation Q.1912.5: "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part".

[11] ITU-T Recommendation Q.1980.1: "The Narrowband Signalling Syntax (NSS) - Syntax definition".

[12] ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Subsystem; Functional architecture".

[13] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[14] ETSI TS 124 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.228 Release 5)".

[15] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 Release 7)".

[16] ETSI TS 129 163: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks (3GPP TS 29.163 Release 7)".

[17] IETF RFC 2976: "The SIP INFO Method".

[18] IETF RFC 3204: "MIME media types for ISUP and QSIG Objects".

[19] ETSI ES 283 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking SIP-ISUP for TISPAN-IMS".

[20] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 6)" for NGN Release 1".

[21] ITU-T Recommendations Q.764: "Signalling System No. 7 - ISDN User Part".

[22] IETF RFC 3261: "SIP: Session Initiation Protocol".

[23] ETSI TS 183 043: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);. IMS-based PSTN/ISDN Emulation Stage 3 specification".

[24] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 Release 7)".

[25] IETF RFC 3966: "The tel URI for Telephone Numbers".

[26] ETSI TS 183 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication DIVersion (CDIV); Protocol specification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

SIP endpoint: any SIP UA within the IM CN subsystem

NOTE: For the purposes of handling included ISUP information, such a SIP endpoint will be a AS or an MGCF or an IBCF, and the entity that contains the SIP endpoint is inclusive of ISUP functionality which will allow the processing of the encapsulated ISUP information.

3.2 Abbreviations

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

3PTY	Three-ParTY
ACM	Address Complete Message
ACR	Anonymous Call Rejection
AGCF	Access Gateway Control Function
AS	Application Server
ASF	Application Server Function
B2BUA	Back to Back User Agent
BGCF	Border Gateway Control Function
BICC	Bearer Independent Call Control
CCBS	Call Completion to Busy Subscriber
CCNR	Call Completion on No Response
CD	Call Deflection
CFB	Call Forwarding on Busy
CFNR	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restriction
CONF	CONFerence Calling, Add-On
CPG	Call Progress Message
CS	Circuit Switched
CSCF	Call Session Control Function
CUG	Closed User Group
CW	Call Waiting
DDI	Direct Dialling In
ECT	Explicit Call Transfer
GVNS	Global Virtual Network Service
HOLD	Call HOLD
IBCF	Interconnection Border Control Function
IMS	IP Multimedia core network Subsystem
IMS-ALG	IMS Application Layer Gateway
IP	Internet Protocol
ISC	IP multimedia Service Control
ISDN	Integrated Services Digital Network
ISUP	ISDN Signalling User Part
IWF	InterWorking Function
LOP	LOop Prevention message
MCID	Malicious Call IDentification
MG	Media Gateway
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
MLPP	MultiLevel Precedence and Preemption
MRFC	Media Resource Function Controller
NGN	Next Generation Network
NNI	Network Network Interface
NSS	Narrowband Signalling Syntax
P-CSCF	Proxy-CSCF
PES	PSTN/ISDN Emulation Subsystem
PSTN	Public Switched Telecommunications Network
REV	REVerse Charging
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Server Local Function
SUB	SUBaddressing

TCAP	Transaction CAPabilities
TLS	Transport Layer Security
TP	Terminal Portability
UA	User Agent
UE	User Equipment
UNI	User Network Interface
UPSF	User Proxy Server Function
UUS	User-to-User Signalling
VGW	Virtual GateWay

4 Introduction and potential use cases

4.1 Introduction

It is the responsibility of the TISPAN stage 2 documents to define the functional architecture for the use of various capabilities defined at stage 1. This clause identifies the various functional architectures defined at stage 2 that are either required to make use of encapsulated ISUP, or could make use of the advantages of encapsulated ISUP.

By bringing these use cases together in the present document, it is also hoped that a common solution can be devised that meets all the use cases.

As the fundamental basis for the service layer in NGN is the IMS defined by 3GPP, it is understood that the use cases and the solutions must be able to coexist with, and be compatible with, the existing 3GPP IMS architecture and 3GPP IMS usage.

Throughout this text, reference is made to the ISUP protocol. In general this can also be assumed to refer to the use of the BICC protocol as well, unless otherwise explicitly stated.

4.2 Use of IMS as a transit network

Clause 6.9.1 of TS 181 005 [2] specifies:

- "The NGN shall support the ability for the interconnection between two PSTN/ISDN and/or emulation networks to remain unchanged from the legacy case."

The ability to support this bridging between two networks (i.e. by bridging between two MGCFs) by using IMS and the transit network has been discussed and endorsed within stage 2 discussions, with open issues still existing on which entities are responsible for performing the routeing between the two MGCFs.

From the above requirement for "the interconnection between two PSTN/ISDN to remain unchanged from the legacy case" two options exist:

- to transfer the signalling unchanged between the two networks (i.e. to encapsulate the ISUP signalling that is the NNI signalling of the PSTN/ISDN);

- to provide a mapping between the ISUP signalling in the PSTN/ISDN and the SIP signalling such that mapping in one direction followed by mapping in the other direction provides exactly the same content as existed originally.

While the protocol solution in to the above stage 1 requirement has yet to be decided, the difficulty in supporting the mapping approach above led to the decision in ITU-T to specify the SIP-I approach in ITU-T Recommendation Q.1912.5 [10] profile C.

4.3 Emulation services

Clause 5.9.2 of TS 181 005 [2] specifies:

- "The TISPAN IMS shall provide at least the same level of interoperability with an emulation network as achieved with legacy PSTN/ISDN networks."

Clause 6.9.1 of TS 181 005 [2] specifies:

- "PSTN/ISDN emulation networks shall provide interfaces to PSTN/ISDN networks."

and:

- "PSTN/ISDN Emulation shall provide a high level of interoperability with the services in the PSTN/ISDN being emulated. The degree to which service interoperability is provided is a matter for operators of Public Electronic Communications Networks and, in some cases, national regulators."

Figure 4.1 is taken from TS 182 012 [12] (figure 3). TS 182 012 [12] specifies a number of functional entities are required to support ISUP encapsulation, and that a number of interfaces are required to carry encapsulated ISUP in order to provide full ISDN transparency. These functional entities and interfaces are:

- MGCF.
- AS.
- AGCF.
- Mg reference point (MGCF - CSCF).
- Mw reference point (CSCF - CSCF).
- Mi reference point (CSCF - BGCF).
- Mj reference point (BGCF - MGCF).
- Mk reference point (BGCF - BGCF).

Not directly specified, but assumed to be included in this list are:

- ISC reference point (CSCF - ASF).
- P2 reference point (AGCF - CSCF).

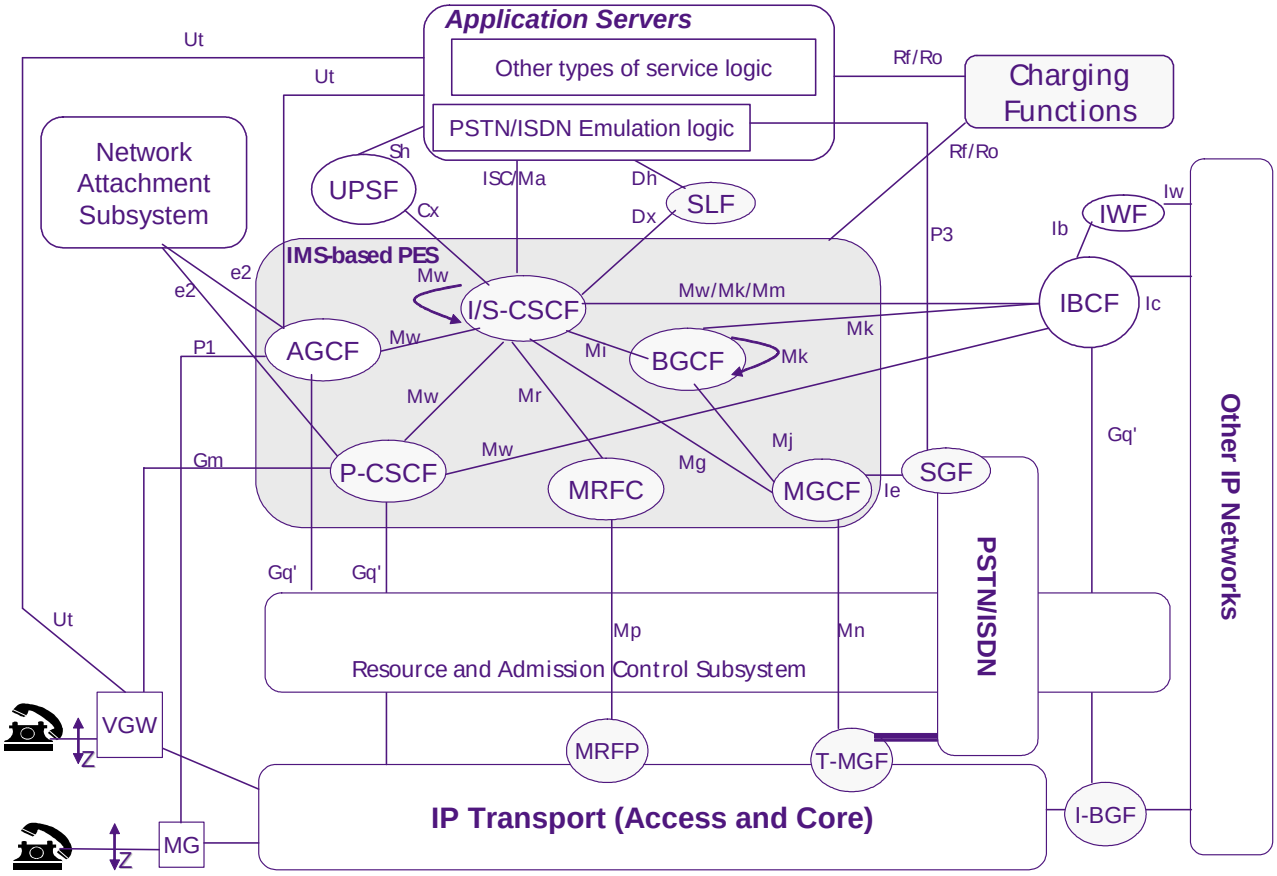


Figure 4.1: PSTN/ISDN emulation subsystem - functional architecture

MRFC A role for encapsulated ISUP is therefore clearly identified in the IMS based PSTN/ISDN emulation.

IMS based PES needs to support both analogue and ISDN users and the use of encapsulated ISUP may vary depending on the type of user supported. ISDN services require more information to be transferred than analogue services.

4.4 Simulation services

It is not possible to build the use case for simulation services on existing stage 2 documents, as no stage 2 document exists.

A key requirement of TS 181 002 [1] clause 5.1 specifies:

- The PSTN/ISDN Simulation services shall support interworking with existing fixed and mobile voice and IP data networks, including PSTN, ISDN, Mobile and Internet.

- It shall be possible to have PSTN/ISDN Simulation communications between IMS users and users in PSTN/PLMN-CS networks. When an PSTN/ISDN Simulation session originates or terminates in a Circuit-switched telephony call, the experience of the CS telephony network user should not substantially differ from that of a communication between two CS telephony network users in terms of aspects such as the delay to set-up communications and the total permissible delay in transporting speech between the end users. The PSTN/ISDN Simulation service does not necessarily have to support all services offered by the CS telephony network.

The capabilities that exist in the ISUP on the PSTN side of the MGCF therefore need to be represented in the SIP protocol on the IMS side of the MGCF.

In order to interwork the ISUP into SIP specific parameters, some knowledge of the individual services may be required, as it is not possible to achieve a totally transparent mapping between ISUP parameters and SIP specific parameters. Whenever possible, ISUP information should be mapped into available SIP headers, but when a fully transparent mapping is not possible, the use of ISUP encapsulation may be required to support the service. When using encapsulated ISUP in support of a service, the MGCF only needs to support generic capabilities, making it straightforward to support existing PSTN services until and unless equivalent SIP mechanisms are available.

The same considerations apply to the potential use of ISUP encapsulation between ASs in support of NNI aspects of a simulation service.

Possible solution for NNI capabilities is potentially quicker than IETF defining new SIP parameters, which in any case only map directly to the equivalent ISUP parameters.

Current simulation services that could benefit from use of encapsulated ISUP are as follows:

- TS 183 005 [3]: Conferencing simulation service.
- TS 183 016 [4]: Malicious Call Identification simulation service.
- TS 183 042 [6]: Completion of Calls to Busy Subscriber simulation service and Completion of Calls on No Reply simulation service.

Contributions have been made proposing the support of encapsulated ISUP in the support of the above simulation services and those contributions were deferred until the results of the present document are complete.

There is ongoing debate in ETSI TISPAN as to whether the NNI portions of the simulation services, particularly when interworking, and the NNI portions of the emulation services, particularly when supported by IMS and when interworking, can and should be one and the same functionality, and therefore lead to the same protocol solution.

Additionally, ES 201 296 [7] provides for the support of charging information within an ISUP APM, and some contributions have seen the need for the support of this information within the IMS environment. This is not a simulation service, but may need to operate in the IMS in a similar manner.

4.5 Recursion

In both SIP, and in the usage of SIP for IMS specified in TS 123 228 [13], TS 124 228 [14] and TS 124 229 [15], redirection by both forward switching at the detecting UA, and by sending a 3xx response back on the path and recursing at an originating UA are allowed.

When an incoming call is received from the PSTN/ISDN, destined for an IMS user, and is forwarded back out to the PSTN/ISDN by either mechanism, similar configurations are created to the bridging use cases described elsewhere.

Similarly when an IMS user with an incoming call from the PSTN sends a REFER to the MGCF with a Refer-To header indicating a user in the PSTN, a similar bridging situation in the IMS can occur.

While in these cases, a user does exist in the IMS for whom services are being provided, if they occur as a result of provision of the ISDN simulation services then the ISDN service descriptions and the ISDN simulation services provide for the ability to obtain services between the two resultant end users. Examples include:

- TS 181 002 [1] clause 8.1.5.2.1: "The MCID simulation service can be invoked for a diverted communication. In addition to the normal operation of the MCID simulation service, the identity of the first diverting user shall be registered and, as a network option, the last diverting user can be registered". As a result, portions of the MCID service, such as the request for identity, need to be providing across the bridge between the two MGCFs.

5 Requirements

R1: The MGCF shall provide a fully conformant ISUP implementation to the PSTN/ISDN when interworking with IMS.

R2: IMS shall support the optional transport of ISUP information within SIP messages using existing SIP mechanisms if possible, or with additions that require only IANA registration based on external specifications.

R3: It must be possible to realize IMS application servers that are capable of supporting selected subsets of PSTN services associated with ISUP information within SIP messages. The supported subsets shall include at least those needed for a) all simulation services and b) all emulation services.

R4: The MGCF shall be capable of interworking between IMS and PSTN using ISUP information within SIP messages as needed for the supported subsets of PSTN services.

R5: It must be possible to secure ISUP information so that endpoints unauthorized to access the ISUP information either never receive any encapsulated ISUP information or are unable to interpret the contents of any encapsulated ISUP information they receive.

R6: SIP endpoints conformant to the SIP profile defined in the present document must be able to interoperate whether or not they can decode, recognize, or generate encapsulated ISUP information.

R7: If it is possible for encapsulated ISUP information to reach the P-CSCF on the way to a UE, it should be possible for the P-CSCF to recognize and remove the encapsulated ISUP information.

R8: The I-CSCF, S-CSCF and BGCF shall be fully transparent to attachments such as encapsulated ISUP information.

R9: It shall be possible to remove some or all encapsulated ISUP information when signalling between SIP networks, e.g. at a IBCF.

R10: The encapsulated ISUP information shall take precedence over SIP signalling.

R11: It must be possible to identify situations in which feature control information is included in encapsulated ISUP information associated with SIP session management procedures and assure that the call is properly handled (e.g. proceed or release) if the feature control information cannot be communicated between peer SIP signalling entities. Proper handling is determined by the procedures for "interworking with other networks" documented in the stage 3 description for the impacted service for the MGCF and is determined by service logic for Application Servers.

R12: It must be possible to identify when a peer SIP signalling entity is unable to process ISUP information not associated with SIP session management procedures and back off to the corresponding failure handling procedures.

R13: It must be possible to determine at a node originating a SIP session whether to:

1) pass in-band call progress from the terminating network towards the call originator (requiring backward cut-through);

2) pass no media towards the call originator; or

3) locally generate in-band ringing tone toward the originating side.

R14: It must be possible to identify the presence of authorized early media carrying in-band call progress information from the terminating network and allow backward cut-through only for authorized early media.

NOTE: R12 and R13 are being addressed under the WI on basic call and are included here only to identify their relevance to the problem.

R15: In the absence of a clear indication from the peer SIP signalling entity of the status of echo suppression in its portion of the bearer path, a signalling node will assure that its portion of the network suppresses any potential echo towards the peer network.

R16: A SIP signalling node shall perform backward cut-through in the presence of authorized early media. A SIP signalling node locally generating in-band call progress shall perform backward cut-through either when presented with authorized early media or on answer.

R17: A SIP signalling node shall perform forward cut-through no later than at answer.

6 Protocol design issues

6.1 Introduction

This clause identifies a number of issues that have been studied in preparation to making the protocol decisions documented in clause 6.11. Those protocol decisions are then implemented in clause 6.3 as proposals for amendments for a number of TISPAN stage 3 specifications.

6.2 ISUP confidentiality

This clause addresses two security aspects of encapsulated ISUP information:

- Confidentiality of encapsulated ISUP information to keep the information in ISUP from unauthorized entities.
- Integrity/authenticity of encapsulated ISUP information to protect the ISUP information from unauthorized manipulation.

When encapsulation of ISUP information is used with the SIP network in support of services, it is essential that only trusted entities be permitted to understand the ISUP contents. Security sensitive information within ISUP primarily pertains to keeping called/calling party numbers/identity information private.

It should be noted that all transfer within NGN is subject to network domain security, as specified in TS 133 210 [24], and this applies to any transfer of SIP messages that may contain encapsulated ISUP information.

Several mechanisms are possible to ensure that encapsulated ISUP information can only be read by entities permitted to receive such information:

1) Require absolute knowledge of the trustworthiness of the endpoint of each request.
2) Encrypt the data so that it can be read only by entities with the appropriate key.
3) Withhold the ISUP information until a proven relationship exists with a peer SIP signalling entity.
4) Remove ISUP information destined toward an untrusted entity or network.

Mechanism 1 has the following concerns, which may render it unworkable:

- IMS does not mandate the inclusion of application servers in the path of every session, so the UNI and NNI may not be distinguishable.
- It is not possible to know in advance if a particular IMS user in a separate IMS will include an application server that is capable of handling ISUP information and performing as a B2BUA to isolate the UNI and NNI.
- When an AS sends a SIP request to an arbitrary target, the AS cannot determine whether or not the target is capable of handling ISUP information since the AS does not perform any routeing function.
- It is not possible to know in advance if a particular IMS user in a separate IMS will include an application server operating as a SIP proxy that performs retargeting of SIP requests (for example, call diversion), making the UNI indistinguishable from the NNI.
- It is not possible to know in advance if an application server will perform retargeting of a SIP request.
- It is difficult to track the ISUP capabilities of all entities within connected SIP networks.

Mechanism 2 has the following characteristics:

- The SIP procedures will differ from ITU-T Recommendation Q.1912.5 [10] profile C (SIP-I) since the disposition of encapsulated ISUP information will usually be marked as optional. Clause 6.3 includes a high level proposal for the modified procedures.

- ISUP information must be secured with S/MIME or other encryption scheme.
- For achieving end-to-end security, ISUP information attachments must be secured with S/MIME or other encryption scheme. An ISUP information attachment shall be integrity protected and authenticated by the source by applying an S/MIME digital signature. The ISUP information attachment should be encrypted using S/MIME if the security policy of the originating and terminating ISUP information encapsulating entity both require this. It is left as for further study how two SIP entities encapsulating ISUP information can determine if encryption is supported.
- S/MIME requires certificates and private keys to be used. Lack of a prevalent public key infrastructure will create serious problems. If self-signed certificates are used, the key exchange mechanisms are susceptible to man-in-the-middle attacks whereby an attacker can potentially inspect and modify S/MIME bodies. The attacker needs to intercept the first exchange of keys between the two parties in a dialog, remove the existing signatures from the request and response, and insert a different signature containing a certificate supplied by the attacker. Each party will think they have exchanged keys with the other, when in fact each has the public key of the attacker (see RFC 3261 [22]). It is not known if this PKI infrastructure will be available if the transit network is untrusted.
- The headers of the encapsulating SIP messages carrying the ISUP messages need to be protected. SIP headers are not protected by the normal usage of S/MIME with SIP. The only way to protect it is by tunnelling the SIP header in the MIME bodies. This SIP tunnelling for protection of SIP header will create additional overhead.
- If SIP tunnelling is used, the usage of TCP is recommended because of the larger message size. This reduces our choice for transport protocol.
- Peer IMS either need to share a common key for encrypting encapsulated ISUP information, or the IBCF may need to decrypt and re-encrypt encapsulated ISUP information according to the encryption keys used by the peer networks.
- When SIP message size is of concern, such as on a wireless air interface, the P-CSCF should be able to determine the presence of S/MIME that is private to the network and unreadable by a UE so that it can be compressed to minimum size.
- Instead of deploying S/MIME for securing ISUP, the most obvious ECS mechanism is TLS. RFC 3261 [22] mandates the usage of TLS for proxies, redirect servers and registrars. Methods for use of TLS are already defined in IETF.
- Instead of deploying S/MIME for securing ISUP, the most obvious ECN mechanism to apply is IPsec, and in 3GPP the SEG function covers the requirement. The calling party domain and the called party domain may deploy SEG at the edge of their networks.
- TLS and IPsec do not provide full end-to-end security protection of encapsulated ISUP information among the originating and terminating ISUPencapsulating entity. TLS or IPsec however support a hop-by-hop trust relation among multiple trustworthy networks.
- Without additional procedures, the ciphered ISUP may be shared with untrusted networks, which is undesirable. SIP messages remain larger with ISUP S/MIME compared to simple removal of ISUP MIME.

Mechanism 3 will typically require the use of a preliminary SIP transaction such as the OPTIONS request to determine peer capabilities before actual session establishment can proceed.

Mechanism 3 is possible but requires more signalling than the other mechanisms, so should be considered only if the other mechanisms have significant limitations.

Mechanism 4 has the following characteristics:

- The SIP procedures will differ from ITU-T Recommendation Q.1912.5 [10] profile C (SIP-I) since the disposition of encapsulated ISUP information will usually be marked as optional. Clause 6.3 includes a high level proposal for the modified procedures.

- A B2BUA is required on the path towards any peer network for which local policy prohibits the forwarding of encapsulated ISUP information to or from the peer network, since the IETF does not allow a proxy to remove or alter MIME attachments. This peer network is considered untrusted with respect to the encapsulated ISUP information. This B2BUA removes any ISUP information marked with optional disposition before forwarding the encapsulating SIP information to or from an untrusted network. This B2BUA returns a 415 (Unsupported Media Type) response to any SIP request to or from an untrusted network where the SIP request contains an encapsulated ISUP information marked for mandatory disposition, and forwards nothing. The B2BUA also removes any indication of support for ISUP information in the Accept header of any SIP message to or from an untrusted network. The IBCF provides a B2BUA at the network boundary that can provide this function in TISPAN networks. IMS as specified by 3GPP has an IMS-ALG acting as a B2BUA that is inserted when interworking between networks using different versions of IP, but is not otherwise used.

- A B2BUA is required on the path towards a UE to remove optional encapsulated ISUP information to or from the UE. This B2BUA returns a 415 (Unsupported Media Type) response to any SIP request to or from the UE where the SIP request contains an encapsulated ISUP information marked for mandatory disposition, and forwards nothing. The B2BUA also removes any indication of support for ISUP attachments in the Accept header of any SIP message to or from a UE. In the current architecture this function would be performed by an AS allocated to the subscriber. The function may alternately be performed by the S-CSCF assigned to the subscriber.

The present document recommends the use of mechanism 4 (ISUP information removal). The mechanisms for provisioning and implementing local policy decisions needed to realize mechanism 4 are not described in the present document.

The present document includes no detailed procedures to support the use of ISUP information S/MIME.

6.3 Relationship between ISUP information and SIP call control

6.3.1 Introduction

NOTE: The analysis of ISUP encapsulation in this clause is applicable to all interfaces listed in the scope of the present document except for AGCF-to-AS signalling.

The potential applicability of encapsulating ISUP information for AGCF-to-AS signalling can be addressed in the future if a clear requirement is identified. Clause 6.2 describes two basic strategies for augmenting IMS to support ISUP semantics when transiting or bridging between endpoints that support encapsulated ISUP information. When it is possible to determine that the terminating UA supports ITU-T Recommendation Q.1912.5 [10] Profile C (SIP-I), the originating UA can use Profile C (SIP-I) procedures. When either or both are known not to support encapsulated ISUP information, the endpoints can use Profile A procedures. As discussed in the clause 6.2, it is not always possible to know in advance which scenario applies when routeing functions are separate from the originating endpoint, as they are with the AS and MGCF in IMS. There are some cases when an IMS may be configured such that an MGCF performs a sufficient portion of the routeing function necessary to determine which profile is appropriate for a given destination. For example, the MGCF may have sufficient routeing capability to determine that the next hop is a SIP-I network endpoint, in which case it would be appropriate for the MGCF to behave according to Profile C (SIP-I) of ITU-T Recommendation Q.1912.5 [10]. This is not possible when originating from an AS which has no routeing capability in an IMS. MGCF conforming to Profile C (SIP-I) is treated as out of scope within the present document. Rather this scenario is considered as if a SIP-I IWU is co-located with the MGCF.

An alternative consistent with IMS entities is to describe a new profile that allows the endpoints to dynamically determine which ISUP services and procedures are common to both endpoints so they can effectively interoperate regardless of their degree of support for ISUP services. The remainder of this clause 6.3 focuses on this approach to supporting endpoints that are able to accept encapsulated ISUP information within IMS.

For most basic calls, the information available in encapsulated ISUP information is redundant with the information available in the SIP headers and SDP bodies. In this case, any processing of encapsulated ISUP information is unnecessary for any endpoint.

It is desirable for a SIP endpoint to selectively support any fraction of the additional services enabled by encapsulated ISUP information, from none of them to all of them.

6.3.2 Transport of ISUP information

Clause 6.6 provides a discussion of manner to transport ISUP information. Since the decision was made to use NSS messages bodies to carry the ISUP information, the remainder of the document reflects the use of NSS.

6.3.3 Determining support for NSS message bodies

The following procedures provide the mechanism for SIP endpoints to determine whether they should interoperate according to ES 283 027 [19] or according to a new profile that supports a range of PSTN services.

1) An originating SIP endpoint capable of handling NSS message bodies in support of any subset of the possible services shall include within the initial SIP INVITE request an Accept header indicating support for NSS ("application/nss"). A terminating SIP endpoint capable of handling NSS message bodies in support of any subset of the possible services shall include an indication of support for NSS message bodies in the first backward SIP message when the originating SIP endpoint is also capable of supporting NSS message bodies. This indication will be an Accept header, if allowed in the SIP message being sent, or an NSS message body.

2) A SIP endpoint not capable of handling NSS message bodies or not receiving indication from its peer of support for NSS message bodies (via the Accept header or inclusion of NSS message body) shall perform procedures according to ES 283 027 [19].

3) A SIP endpoint capable of handling NSS message bodies and receiving an indication from its peer of support for NSS message bodies (via the Accept header or inclusion of NSS message bodies) shall exchange ISUP information according to service logic and local configuration controls.

6.3.4 Categories of ISUP information

The use of encapsulated ISUP information can be categorized as follows:

- Category 1: ISUP information that provides feature control information that augments existing SIP session management procedures.

- Category 2: ISUP information that is not associated with existing SIP session management procedures.

Category one information includes the ISUP IAM, ACM, CPG (usually), ANM and REL. This information is typically encapsulated within the SIP INVITE request, 180 (Ringing) response, 183 (Session Progress) response, 200 (OK) response and BYE request, respectively. Information carried within ISUP CPG message may also be encapsulated in the reINVITE request and UPDATE request when interworking the Call Hold supplementary service. This new SIP profile does not call for the processing of the ISUP state machine on a SIP interface for these ISUP messages, since SIP itself has the necessary state machine and associated timers needed for the interface, although implementations may choose to implement some additional timers when interoperating with ISUP networks. The encapsulated ISUP information in these cases augments the SIP signalling when the information cannot be reflected by the SIP signalling.

6.3.5 Handling ISUP information within SIP session management messages

6.3.5.1 Determining ISUP compatibility for the INVITE request

The following procedures allow for peer signalling endpoints to determine whether or not they support a mutually compatible set of PSTN-based services according on the contents of the INVITE request.

1) A MGCF sending an initial INVITE request shall mark the encapsulated ISUP information with mandatory disposition if the ISUP preference indicator is set to "ISUP required all the way". If the parameter compatibility parameter associated with any parameter indicates "release call" when pass on is not possible, the message shall be marked as mandatory. The message may be marked as mandatory handling under other circumstances as a matter of local policy. Otherwise the UAC shall mark the encapsulated ISUP information with optional disposition. An Application Server shall determine the disposition based on service logic.

2) A SIP endpoint receiving an initial INVITE request with encapsulated ISUP information marked with optional disposition may ignore any unrecognized or unsupported ISUP information.

3) When a SIP endpoint receives an initial INVITE request that includes encapsulated ISUP information with mandatory disposition, and the endpoint cannot decode or recognize the encapsulated ISUP information, the endpoint shall reject the INVITE request with a 415 (Unsupported Media Type) response.

4) A SIP endpoint receiving an initial INVITE request with encapsulated ISUP information marked with mandatory disposition should reject the INVITE request with a 603 (Decline) response if the encapsulated ISUP information includes an ISUP parameter unrecognized or unsupported by the endpoint where the parameter requires call release according to ISUP procedures when unsupported or unrecognized. This may occur for CUG and UUS, and for any parameter with compatibility information requiring release when pass on is not possible.

6.3.5.2 Retry on failure of ISUP compatibility for the INVITE request

The following procedure allows for retry to an alternative destination when the initial terminating endpoint is incapable of supporting a required service.

1) A SIP endpoint or proxy receiving a 415 or 603 (Decline) response message in response to having sent or forwarded a SIP INVITE request may wish to attempt an alternate route in the hope that that a route supporting encapsulation is found. Otherwise the call must be failed backwards.

6.3.5.3 Supporting a consistent set of ISUP procedures

The following procedure ensures that each SIP endpoint supports a consistent set of ISUP procedures determined by the supported ISUP services.

1) A SIP endpoint that sends or receives a SIP message containing encapsulated ISUP information for a supported service shall construct or process the encapsulated ISUP information message according to the relevant service specification. It should be possible to support multiple services simultaneouslywithin a given SIP message, although this does not occur for ETSI services. Sending of encapsulated ISUP information related to ISUP information compatibility procedures when handling an unrecognized or unsupported parameter or message is optional.

6.3.5.4 ISUP in other SIP session management procedures

The following procedures describe additional handling of encapsulated ISUP information in all SIP messages other than the INVITE request and the INFO request. The minimum level of support for ISUP information in these messages is already determined by ISUP information in the INVITE request for the dialog, as previously described.

1) A SIP endpoint shall mark with optional disposition all NSS message bodies it sends in messages other than the initial SIP INVITE request and the SIP INFO request. This includes, for example, the ACM, ANM and REL messages.

2) A SIP endpoint indicating support for NSS message bodies may ignore unsupported or unrecognized ISUP information encapsulated in any SIP message it receives in messages other than the initial INVITE request and the INFO request.

6.3.6 Handling transparent ISUP messages

6.3.6.1 General

Category two messages include all other ISUP messages that are not local to the ISUP interface, and sometimes the CPG message. ITU-T Recommendation Q.1912.5 [10] describes category two messages as transparent messages in clause 5.4.3.2, and lists the ISUP messages in this category. SIP-I (ITU-T Recommendation Q.1912.5 [10] profile C) carries these messages in either the first 183 response or in the SIP INFO request, but the procedures below only use the INFO request to carry category two messages.

6.3.6.2 Sending transparent ISUP messages

The following procedure describes how a peer SIP signalling endpoint sends a transparent ISUP message within a dialog.

1) When sending a category two encapsulated ISUP information that would be marked with optional disposition is to be sent before an established dialog, it may be sent in a reliable 183.

2) If the category two ISUP information would be marked with required disposition, the sender shall always include it in a SIP INFO request. The sender shall wait for acknowledgment of the first reliable response before sending the INFO request. A UAS may need to send a reliable provisional response if an INFO request is pending and the UAS has not previously sent and received acknowledgment for a provisional response.

6.3.6.3 Receiving transparent ISUP messages

The following procedures describe the handling of transparent ISUP information at the receiver, allowing for a wide range of PSTN services at the receiver. This mechanism, in conjunction with the corresponding backoff procedures at the sender described below, allows the receiver to selectively choose which PSTN services to support. For example, an IMS AS may choose to support call transfer notifications, but not support the IDR/IDS exchange. This flexibility allows development of an AS with support for only those parts of ISUP necessary to provide a given service and no more, thus significantly reducing the amount of ISUP processing needed within such an AS compared to the use of SIP-I (ITU-T Recommendation Q.1912.5 [10] profile C).

1) When a SIP endpoint receives a SIP INFO request that includes encapsulated ISUP information and the endpoint cannot decode or recognize the encapsulated ISUP information, the endpoint shall reject the INFO request with a 415 (Unsupported Media Type) response.

2) When a SIP endpoint receives a SIP INFO request marked with required disposition that includes encapsulated ISUP information with ISUP information that is unrecognized or unsupported by the endpoint, and any of the unrecognized or unsupported information does not have included compatibility indicates or has compatibility indicators requiring call release if it cannot be processed or forwarded, the endpoint shall reject the SIP INFO request with a 603 (Decline) response.

3) When a SIP endpoint receives a SIP INFO request that includes ISUP information marked as optional disposition that is unrecognized or unsupported by the endpoint, and none of the unrecognized or unsupported information has compatibility indicators requiring call release if it cannot be processed or forwarded, the endpoint may reject the SIP INFO request with a 603 (Decline) response, invoke the procedures appropriated for unrecognized ISUP information, (e.g. return an encapsulated ISUP information Confusion message), or ignore the ISUP information.

4) When a SIP endpoint receives a SIP INFO request that includes encapsulated ISUP information with ISUP information for a supported service, the endpoint shall process the encapsulated ISUP information message according to the relevant PSTN service.

6.3.6.4 Handling responses to INFO request

6.3.6.4.1 General

The following procedures determine the handling at the sender of an INFO request with encapsulated ISUP information when receiving the SIP response to the request. When a SIP endpoint receives a failure response to an INFO request it backs off to the procedure normally performed in a Profile A endpoint.

1) When a SIP endpoint receives a 415 or 603 (Decline) response message in response to having sent a SIP INFO request with encapsulated ISUP information, the endpoint shall abort the procedure associated with the encapsulated ISUP information and back off to the corresponding failure procedure defined for service. This may be based on service logic. At and MGCF, if the encapsulated ISUP information contained compatibility information, these failure procedures may include the SIP endpoint performing the procedures appropriate for pass on not possible. Failure of the transaction related to the INFO request does not impact the state of the ongoing dialog, which will continue according to RFC 2976 [17], but the service failure procedures may impact the dialog state.

2) When a SIP endpoint receives a 200 (OK) response message in response to having sent a SIP INFO request with encapsulated ISUP information, the endpoint shall continue service procedures related to the transmitted ISUP information according to the relevant PSTN service specification.

6.3.6.4.2 Special cases of handling responses to INFO request

The set of procedures below are special backoff cases not covered by the previous set of procedures. These cases provide special handling associated with certain ISUP timers and compatibility procedures.

1) A SIP endpoint receiving a 415 (Unsupported Media Type) or 603 (Decline) in response to sending an encapsulated information interworked from an INR shall behave as if it received an INF indicating that the requested information is not available.

2) A SIP endpoint receiving a 415 (Unsupported Media Type) or 603 (Decline) in response to sending an encapsulated SUS (network) information shall assume the role of the controlling exchange in respect to re-answer timing. If the SIP endpoint subsequently receives the equivalent of a RES indication, it shall stop the reanswer timer.

3) A SIP endpoint receiving a 415 (Unsupported Media Type) or 603 (Decline) in response to sending an encapsulated Confusion information or an encapsulated Forward Transfer information shall ignore the event.

The procedures described above provide for dynamic adaptation between two SIP endpoints supporting varying subsets of PSTN services.

6.4 Applicability of ISUP timers to SIP with encapsulated ISUP information

Any procedures related to ISUP timers would be realized via the service logic in an application server.

ITU-T Recommendation Q.764 defines a number of timers that indicate that an ISUP message is expected in response to a sent message or a follow-up message is expected to a received message. Many of these timers are associated with circuit maintenance supervisory messages or ISUP status and do not apply across a SIP network. Some timers apply to establishing a basic call while others apply to clearing circuits. Another group applies to ISUP supplementary services.

Clause 5.3.2 of ITU-T Recommendation Q.1912.5 [10] provides the only reference to ISUP timers throughout the document:

> In the case of Profile C (SIP-I) of ITU-T Recommendation Q.1912.5 [10], the following ISUP timers defined in Q.764 shall not be supported by ISUP procedures on the SIP side of the IWU: T1, T4, T5, T10, T12 through T32, T36 and T37.

There is no reason to consider any of these excluded timers for a new SIP profile since they are considered irrelevant to Profile C (SIP-I).

Table 6.1 summarizes the remaining timers and their functions. There is no requirement in ITU-T Recommendation Q.1912.5 [10] to implement these timers for Profile C (SIP-I), but only an implication that they may be relevant.

Table 6.1: Applicability of ISUP timers to SIP

Timer	Send/Rec	Expect	Action at Timeout	Comment
T2	/SUS user	RES	Send REL	Applicable at the initiating exchange (not IMS)
T3	/TTB	timeout	resume normal service	"temporary trunk blocking" (national use) is not relevant to SIP
T6	/SUS net	RES	Send REL	May be applicable at the controlling exchange
T7	IAM	ACM/CON	Send REL	May be applicable to the equivalent SIP messages
T8	/IAM w/cont	COT	Send REL	May be applicable to the equivalent SIP messages
T9	ACM	ANM	Send REL	May be applicable to the equivalent SIP messages
T11	IAM-SAM	SAM	Send ACM	Not applicable to terminating UA in TISPAN - assume INVITE request includes all digits
T33	INR	INF	Send REL, alert	Applicable at the initiating exchange (not IMS)
T34	Indicate SGM	SGM	continue call but lose service information	Not relevant to SIP since segmented ISUP messages not carried in SIP
T35	IAM, SAM	SAM	Send REL - too few digits	Not applicable to terminating UA in TISPAN - assume INVITE request includes all digits
T38	SUS net	RES	Send REL	May be applicable at an international exchange
T39	MCID req IDR	MCID resp IRS	Call continues	Applicable at the initiating exchange

The more darkly shaded rows in table 6.3 are either not needed or are not applicable to SIP with encapsulated ISUP information for the reasons described in the table. The remaining rows are described below. The lightly shaded rows in table 6.3 are not applicable to any of the simulation services.

T2 is run at the initiating exchange during terminal portability procedures. This is not applicable to the simulation architecture but may be applicable to a SIP-capable exchange supporting terminal portability.

T6 is run at the controlling exchange to perform re-answer timing. If an ISUP exchange is not the controlling exchange but cannot forward an ISUP SUS message that it receives to the next exchange, it should typically perform re-answer timing. If an IMS entity performs the role of the controlling exchange and is capable of handling the ISUP SUS message, it may run T6. If an IMS entity is not the controlling exchange, is capable of handling the ISUP SUS message, but cannot forward the message, it may also run T6.

T7, T8 and T9 are associated with ISUP call establishment messages that have direct SIP counterparts. Implementations should consider whether any of these timers should be used with the SIP messages, in addition to the SIP timers.

T33 is run at the initiating exchange during the information request procedure, but no ETSI service uses the procedure.

T38 may be used at an international exchange as a backup to T6.

T39 is run at the initiating exchange during the MCID procedure.

6.5 Usage of INFO request in SIP

There is some ambiguity regarding the usage of the INFO request in ITU-T Recommendation Q.1912.5 [10] and RFC 2976 [17]. Recent communication on the IETF SIP exploder has reached the following consensus regarding the usage of the INFO request.

The INFO request may be used to convey encapsulated ISUP information in the forward direction as soon as a reliable provisional or final response is received, and additionally in the backward direction after a reliable provisional or final response is acknowledged. SIP entities intending to support encapsulated ISUP information should indicate support for 100rel.

6.6 Method of ISUP information encapsulation

RFC 3204 [18] defines the binary ISUP encapsulation mechanism used by profile C (SIP-I) in ITU-T Recommendation Q.1912.5 [10]. ITU-T Recommendation Q.1980.1 [11] (Narrowband Signalling Syntax - NSS) defines an alternate ISUP encapsulation method using text encoding. These are the only ISUP encapsulation mechanisms available today and the only ones under consideration at this time. While RFC 3204 [18] is efficient and extensively deployed today, ITU-T Recommendation Q.1980.1 [11] has several advantages worth considering for application to TISPAN networks.

ISUP information may be transported in either binary, as described by Q.1912.5 for SIP Profile C (SIP-I), or text format, as accommodated by the use of Narrowband Signalling Syntax (NSS) as described in ITU-T Recommendation Q.1980.1 [11]. The binary format requires that the entire binary ISUP message body be included in the SIP message, even in the event that much of the information is redundant with SIP signalling.

Given the text format of all ISUP information encoded by ITU-T Recommendation Q.1980.1 [11], this should be more acceptable to SIP servers already parsing ASCII-based SIP.

Furthermore, clause 5.2.1 of ITU-T Recommendation Q.1980.1 [11] expects that encapsulated NSS messages will not include parameter lines that have been successfully mapped to the encapsulating protocol - SIP. This also simplifies the handling of NSS messages since they contain little or no redundant information.

To avoid conflict within the NGN a single format will be used - NSS.

6.7 Interoperation between ISUP interworking profiles

The present document is primarily focused on augmenting IMS SIP with optional encapsulated ISUP information in an interoperable manner with non-encapsulating IMS endpoints. Since SIP-I (ITU-T Recommendation Q.1912.5 [10] profile C) and IMS SIP are not meant to interoperate, it is recommended to provide interworking (rather than interoperability) between SIP-I and IMS SIP via the IBCF/IWF or other means.

The IMS may choose to support a regional ISUP variant internal to the network when using encapsulated ISUP information to support various local ISUP services according to procedures in the present document. This raises the issue of interoperation between networks supporting different ISUP variants based on the SIP profile in the present document.

Based on the network configuration, the MGCF may provide interworking between the ISUP variant used within the IMS and the ISUP variant used in the connected CS network. The TR already allows for interworking to support this configuration.

The IMS and its peer SIP networks can independently choose whether to support ISUP information encapsulation, and which ISUP variant to use in providing services. It is not practical to support interoperation between all possible variants of ISUP. Three practical alternatives exist for interoperation of ISUP variants between peer SIP networks:

1) Remove ISUP information from any SIP messages to or from the peer network.

2) Agree to interoperate with the same regional ISUP variant used within the respective networks (for compatible networks).

3) Agree that each network will interwork between their internal ISUP variant and the international ISUP variant defined by the present document when interoperating.

The IBCF/IWF provides a candidate network element to provide interworking, according to local policy, between the regional ISUP variant used within the network, and one of the following SIP profiles associated with the interface to the peer network:

1) No ISUP information.

2) The same regional ISUP variant used within the IMS.

3) The ISUP variant in the present document (if different from the one used within the IMS).

The present document includes no detailed procedures in support of this strategy for interoperating between networks supporting different ISUP variants, although the IWF is potentially available in the architecture for this purpose. The architecture and detailed procedures needed to interwork between different ISUP variants remains for further study.

6.8 ISUP precedence over SIP headers in ITU-T Recommendation Q.1912.5

When encapsulating a binary ISUP message in a SIP message, SIP header information normally takes precedence over corresponding information in the ISUP message. There are a few exceptions to this rule for profile C (SIP-I) of ITU-T Recommendation Q.1912.5 [10] that are of concern in the case where an ISUP message is marked with optional disposition and discarded. What is the impact on a call when binary ISUP information that normally takes precedence over corresponding SIP information is discarded? This question becomes even more important when considering that application servers may modify SIP headers when performing value-added services, and these modifications may not be reflected in the corresponding encapsulated ISUP information parameters.

Case 1: Clause 6.1.3.6 of ITU-T Recommendation Q.1912.5 [10] indicates that in the event that the P-Asserted-Identity and the Calling Party Number of the encapsulated IAM are the same, the stronger of the two privacy indications shall be used. This may result in the privacy information in APRI of the Calling Party Number taking precedence over the Privacy header in the SIP INVITE request. If the Calling Party Number from the encapsulated ISUP information is not available because the encapsulated ISUP information message is discarded, then only the Privacy header is available for use. Version 7.1.0 of TS 129 163 [16] provides a network option to map the Privacy header to "presentation restricted by network" as needed to address this case.

NOTE: TS 129 163 [16] extends ITU-T Recommendation Q.1912.5 [10] for the COLP service, which will provide the Connected Party Number in a backward P-Asserted-Identity and associated Privacy header. In this case, a similar condition and solutions as case 1 above may apply.

Case 2: Clauses 6.1.3.9 of ITU-T Recommendation Q.1912.5 [10] indicate that the information in the Hop Counter of an encapsulated ISUP information IAM takes precedence over the Max-Forwards header in SIP messages. The SIP Max-Forwards header will only influence the ISUP Hop Counter when the encapsulated ISUP information is not present, or when it is present, but the encapsulated IAM does not include the optional Hop Counter parameter. As a result, the ISUP Hop Counter will be generated based on the received SIP Max-Forwards (after scaling and decrementing). The difference is not significant to the network.

Case 3: Clauses 7.3.1 and 7.3.2 of ITU-T Recommendation Q.1912.5 [10] indicate that the information in encapsulated ISUP information ACM and CPG messages takes precedence over the normal interpretation of the SIP 18x response. In the event that the ACM/CPG is discarded any information carried in the optional parameters will be lost and only the default values for the Backward Call Indictors will be applied. As backward messages, the ACM and CPG will only be sent if the originating side already indicates willingness to receive encapsulated ISUP information, so this is not an issue as long as the profile A defaults are acceptable.

Care should be taken when using a 18x response as the ACM could be indicating a "early" ACM so that announcements, etc., can be generated typically from IN. The CPG generated in the backward direction is usually deployed to carry specific service information.

Case 4: Clause 6.11.1 of ITU-T Recommendation Q.1912.5 [10] indicates that the ISUP cause value takes precedence over the SIP 4xx-6xx response. In many cases, multiple ISUP cause values map to the same SIP response, so this rule primarily serves to retain the meaning of the original ISUP cause value. If the ISUP cause value is not available, the SIP response still has valid meaning but is perhaps less specific. The use of the Reason header, which can include the ISUP cause value according to ITU-T Recommendation Q.850 [9], can be used to retain the full semantics of the ISUP cause value. It may not be available from some endpoints, in which case the less specific SIP reason code should be adequate.

In addition to these cases described in ITU-T Recommendation Q.1912.5 [10], the ETSI endorsement of ITU-T Recommendation Q.1912.5 (EN 383 001 [8]) also calls for the Calling Party number to take priority over the P-Asserted-Identity header. Care must be taken to assure that the P-Asserted-Identity header always contains the proper Calling Party information.

These cases demonstrate that when proper precautions are taken in the handling of key SIP header information, it is safe to ignore ISUP information that when present might take precedence over the corresponding SIP header information.

When the encapsulated ISUP information in a SIP message is carried in an NSS message body the precedence is changed because the NSS should only carry information that cannot be reflected by SIP headers. An NSS message body will not be present unless the SIP signalling in the encapsulating message cannot represent the information, or the information is different from the default values defined in ES 283 027 [19]. On receipt of a SIP message containing an NSS message body, the AS should use the encapsulated ISUP information in preference to any value determined by interworking procedures and default values.

6.9 Service analysis

6.9.1 General

This clause 6.9 presents an analysis of the defined ETSI ISDN supplementary services and their support by ISUP transparency. For each service, the messages and parameters related to the service are enumerated. A discussion is provided to describe the potential impacts to the call if the service related information cannot be delivered either because the peer SIP server does not accept encapsulated ISUP information or it only accepts ISUP messages related to specific services and rejects all others. Annex A includes a summary table of the messages and parameters used by the supplementary services.

This clause 6.9 does not describe all SIP extensions under consideration within TISPAN and the IETF as alternatives to encapsulated ISUP information. As SIP extensions are developed for the NNI to signal information equivalent to information currently only available within ISUP messages, those SIP extensions are expected to be used in preference to encapsulated ISUP information.

6.9.2 Direct Dialling In (DDI)

The DDI digits to support the DDI service are carried as part of the Called Party Number in the ISUP IAM.

Table 6.2: Direct dialling in

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Called Party Number	INVITE request	Request-URI

Since this parameter is completely mapped into the SIP Request-URI, there is no additional information carried by the encapsulated ISUP information that is not also available in the SIP headers. Therefore, this service would be unaffected if it is not possible to deliver the encapsulated IAM information.

Overlap sending of the Called Party Number information element can also result from the presence of the DDI supplementary service in the PSTN/ISDN or within an AGCF supporting DDI.

6.9.3 Calling LIne Presentation/Restriction (CLIP/CLIR)

This clause identifies the parameters carried in support of the CLIP/CLIR services provided to the end user.

Table 6.3: Calling Line Presentation/Restriction

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Access Transport	INVITE request	*Encapsulated*
	Calling Party Number		P-Asserted-Identity Privacy
	Generic Number (additional calling party number)		From

The Access Transport parameter carries information related to the subaddress in an identical manner to the subaddressing service; see SUB service for details.

The Calling Party Number of Generic Number (additional calling party number) are mapped to SIP headers, therefore no service functionality would be lost if the encapsulated is not delivered, with one exception. The Calling Party Number APRI (presentation restricted by network) is currently not uniquely mapped into SIP. The Privacy header will carry the fact that the information is restricted, but not the source of the restriction. The loss of this information should not significantly affect the call.

6.9.4 COnnected Line Presentation/Restriction (COLP/COLR)

This clause identifies the parameters carried in support of the COLP/COLR services provided to the end user.

Table 6.4: Connected Line Presentation/Restriction

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Optional Forward Call Indicators	INVITE request	Encapsulated
ANM, CON	Access Transport	200 (OK) response (to INVITE request) or previously received provisional response	*Encapsulated*
	Connected Number		P-Asserted-Identity Privacy
	Generic Number (additional connected number)		*Encapsulated*

The Access Transport parameter carries information related to the subaddress in an identical manner to the subaddressing service; see SUB service for details.

SIP does not carry the Connected line identification request indicator in the INVITE request. However if an AS wishes to request the service per subscriber it may provide the indicator within an encapsulated ISUP information message. If the encapsulated ISUP information is not delivered, then the request indicator would be lost. When mapping the SIP INVITE request to the ISUP IAM, this indicator may be set as an operator option (TS 129 163 [16] extension to ITU-T Recommendation Q.1912.5 [10]). For SIP terminations, the information could be returned, based on a network options. This would allow the service information to always be provided to the originating AS, instead of upon request. The AS could then decide when to deliver the connected line identity to the user.

The mapping into SIP headers will only provide the Connected Number information and its associated restriction. The Access Transport (see subaddressing) and Generic Number (additional connected number) information would be lost if the encapsulated ANM/CON were not be to be delivered. However, this would not significantly affect the call. The most significant service information will still be delivered.

6.9.5 Malicious Call IDentification (MCID)

Table 6.5: Malicious Call Identification

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IDR	MCID Request Indicators	INFO request	Encapsulated
IRS	MCID Response Indicators	INFO request	*Encapsulated*
	Calling Party Number		
	Access Transport		
	Generic Number		

The MCID information is not mapped into existing SIP headers. Therefore if the IDR message cannot be delivered, the service as defined cannot be provided. Since the requesting exchange will not fail the call if the requested information is not provided, there is no significant impact to the call. (Also see service description "Interactions with Other Networks".) The only side effect is that the termination is held until the MCID request timer expires. This impact can be mitigated by having the interworking node return an IRS upon being informed that the encapsulated ISUP information was not delivered (based on the fact the IDR would be sent in an INFO request with mandatory handling a 415 (Unsupported Media Type) or 603 (Decline) response would be returned). This IRS would indicate that no information is available, or may provide partial information if available, as a network option.

6.9.6 SUBaddressing (SUB)

Table 6.6: Subaddressing

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Access Transport	INVITE request	*Encapsulated*

The subaddressing information carried in the Access Transport is not mapped into a SIP header. Therefore this information is lost if the encapsulated IAM information is not delivered. However, per the service description "Interactions with Other Networks", the call is continued without this information, so there is no significant impact to the call.

NOTE: RFC 3966 [25] provides a mechanism for providing subaddresses within a tel URI parameter but this mechanism is not supported by any of the current interworking specifications, e.g. ES 283 027 [19].

6.9.7 Call Diversion Services - CFB/CFNR/CFU/CD

Table 6.7: Call Diversion Services

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Original Called Number	INVITE request	History
			Privacy
	Redirection information		Privacy
			Reason
	Redirecting Number		History
			Privacy
ACM, CPG	Call Diversion Information	180/181 response (to INVITE request)	History
			Privacy
	Generic Notification Indicators		SIP response type (i.e. 181)
	Optional backward call indicators		*Encapsulated*
	Redirection Number		History
			Privacy
	Redirection Number Restriction Indicator		History
CPG	Event Indicator	180/181 response (to INVITE request)	*Encapsulated*
ANM, CON	Redirection Number	200 (OK) response (to INVITE request)	History
			Privacy
	Redirection Number Restriction Indicator		Privacy

NOTE: The above mapping is based on current draft of TS 183 004 [26].

The most significant portions of the call diversion service related information is mapped to the History and Privacy headers. Only two pieces of service related information is not mapped: Optional backward call indicators and Event Indicator. These pieces of information are for informational purposes. No significant service impacts will occur if these are not delivered.

6.9.8 Explicit Call Transfer (ECT)

Table 6.8: Explicit Call Transfer

ISUP Information		SIP Information	
Message	Parameter	Message	Header
CPG	Call Transfer Number	INFO request	*Encapsulated*
	Generic Notification		*Encapsulated*
FAC	Access Transport	INFO request	*Encapsulated*
	Call Transfer Number		*Encapsulated*
	Generic Notification		*Encapsulated*
	Service Activation		*Encapsulated*
LOP	Call Transfer Number	INFO request	*Encapsulated*
	Loop Prevention Indicators		*Encapsulated*

None of the service information related to ECT is mapped to SIP headers. Since the information carried in the CPG and FAC messages are informational in nature, the transfer can still complete without significant loss of service should the encapsulated ISUP information messages not be delivered (per service description "Interactions of other networks"). If the interworking node learns that the LOP request message is not delivered, then it should return a LOP response with an indication of "insufficient information". Should the transferring node receive a LOP response with "insufficient information" or the T_{ECT} timer expires, it will decide if the transfer should continue when loop detection is attempted.

6.9.9 Call Waiting (CW)

Table 6.9: Call Waiting

ISUP Information		SIP Information	
Message	Parameter	Message	Header
ACM, CPG	Generic Notification	18x response (to INVITE request)	*Encapsulated*

The CW service information is not mapped to SIP headers. However, since this information is only for the purpose of notification, the call may continue, per service description "Interactions with Other Networks". Therefore there is no significant impact to the call.

6.9.10 Call HOLD (HOLD)

Table 6.10: Call HOLD

ISUP Information		SIP Information	
Message	Parameter	Message	Header
CPG	Generic Notification	INVITE request, reINVITE request, UPDATE request	*Encapsulated*
			SDP parameters

The ISUP Generic Notification is not mapped to SIP headers. However, since the call hold action (held or retrieved) is mapped to a SDP level parameter (e.g. a=sendonly), the service actions are not lost. Therefore, no service functionality is lost if the encapsulated CPG is not delivered.

6.9.11 Terminal Portability (TP)

Table 6.11: Terminal Portability

ISUP Information		SIP Information	
Message	Parameter	Message	Header
SUS	Suspend Indicators	INFO request	*Encapsulated*
RES	Resume Indicators	INFO request	*Encapsulated*

The TP service information is not mapped to SIP headers. However, since this information is only for the purpose of notification, the call may continue, per service description "Interactions with Other Networks". Therefore there is no significant impact to the call.

6.9.12 Call Completion to Busy Subscriber (CCBS)

Table 6.12: Call Completion to Busy Subscriber

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	CCSS	INVITE request	*Encapsulated*
	Forward Call Indicators		*Encapsulated*
REL (diagnostic)	Cause Indicator	4XX response (to INVITE request)	*Encapsulated (see note)*
NOTE: Use of Allow-events header to carry indicator is currently under study.			

This service is invoked after a failed termination attempt due to the called subscriber being busy. The REL (diagnostic) field indicates that the terminating node is able to support CCBS. If the encapsulated REL is not delivered, then the CCBS service cannot be invoked. But this does not affect the current call, it is already terminating. If the REL is successfully delivered to the originator, then there is high probability that subsequent exchanges with encapsulated ISUP information will also be successful.

NOTE: Interworking with TCAP capabilities is also required to support this service, but such considerations are outside the scope of the present document.

6.9.13 Call Completion on No Response (CCNR)

Table 6.13: Call Completion on No Response

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	CCSS	INVITE request	*Encapsulated*
	Forward Call Indicators		*Encapsulated*
ACM, CPG	CCNR Possible	18x response (to INVITE request)	*Encapsulated (see note)*
NOTE: Use of Allow-events header to carry indicator is currently under study.			

This service is invoked after a failed termination attempt due to the called subscriber not answering. The REL (diagnostic) field indicates that the terminating node is able to support CCNR. If the encapsulated REL is not delivered, then the CCNR service cannot be invoked. But this does not affect the current call, it is already terminating. If the REL is successfully delivered to the originator, then there is high probability that subsequent exchanges with encapsulated ISUP information will also be successful.

NOTE: Interworking with TCAP capabilities is also required to support this service, but such considerations are outside the scope of the present document.

6.9.14 CONFerence Calling (CONF)

Table 6.14: Conference Calling

ISUP Information		SIP Information	
Message	Parameter	Message	Header
CPG	Generic Notification	INVITE request, UPDATE request	*Encapsulated*
			SDP parameters

The CONF service information is not mapped to SIP headers. This information is only for the purpose of notification, the call may continue, per service description "Interactions with Other Networks". Therefore there is no significant impact to the call.

The Generic Notification value will also be used to drive the SDP directionality parameters in the SIP network.

6.9.15 Three-ParTY (3PTY)

Table 6.15: Three-Party

ISUP Information		SIP Information	
Message	Parameter	Message	Header
CPG	Generic Notification	INVITE request, UPDATE request	*Encapsulated*
			SDP parameters

The 3PTY service information is not mapped to SIP headers. This information is only for the purpose of notification, the call may continue, per service description "Interactions with Other Networks". Therefore there is no adverse impact to the call. The Generic Notification value will also be used to drive the SDP directionality parameters in the SIP network.

6.9.16 Closed User Group (CUG)

Table 6.16: Closed User Group

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	CUG Interlock Code	INVITE request	*Encapsulated*
	Forward Call Indicators		*Encapsulated*
	Optional forward call indicator		*Encapsulated*

The CUG relation information is not mapped into SIP headers. If the ISUP IAM is not delivered then in most cases the call can continue, but without user group services. There is one exception for consideration - if the call is marked as "CUG without outgoing access" then the call should not be allowed to complete. But in this case the IAM will be marked as "ISUP required" and therefore the encapsulated ISUP information will have a disposition of mandatory. This will result in the SIP INVITE request being failed if the terminating end does not accept the encapsulated ISUP information. Ideally, the interworking node should specify the cause value as #29 in this case, instead of the default interworking.

6.9.17 MultiLevel Precedence and Preemption (MLPP)

Table 6.17: Multilevel Precedence and Preemption

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Precedence	INVITE request	*Encapsulated*
ACM, CPG	Generic Notification	18x response (to INVITE request)	*Encapsulated*
	Optional Backward Call Indicators		*Encapsulated*
REL (cause value)	Cause Indicator	4xx-6xx response (to INVITE request)	Reason

The only service information that can be mapped to SIP headers is the cause value, which get mapped to the Reason header. All other information will be encapsulated. If the encapsulated information cannot be delivered then the call shall continue per service specification "Interworking with Other Networks". In this case the call will continue as a normal call.

6.9.18 Global Virtual Network Service (GVNS)

Table 6.18: Global Virtual Network Service

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Forward Call Indicators	INVITE request	*Encapsulated*
ANM, CON	Backward GVNS	200 (OK) response (to INVITE request)	*Encapsulated*

All service information will be encapsulated. If the encapsulated information cannot be delivered then the call shall continue per service specification "Interworking with Other Networks". The terminating node will make the determination if it is still possible to complete the call.

6.9.19 REVerse Charging (REV)

Table 6.19: Reverse Charging

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Remote Operations	INVITE request	*Encapsulated*
ANM, CON	Remote Operations	200 (OK) response (to INVITE request)	*Encapsulated*
FAC	Remote Operations	INFO request	*Encapsulated*

All service information will be encapsulated. If the encapsulated information cannot be delivered then the call shall continue per service specification "Interworking with Other Networks". In this case, the service will not be allowed, but the call may be otherwise unaffected.

6.9.20 User-to-User Signalling (UUS)

Table 6.20: User-to-User Signalling

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Forward Call Indicators	INVITE request	*Encapsulated*
	User to User Indicators		*Encapsulated*
	User to User Information		*Encapsulated*
ACM, CPG	User to User Indicators	18x response (to INVITE request)	*Encapsulated*
	User to user Information		*Encapsulated*
ANM, CON	User to User Indicators	18x response (to INVITE request)	*Encapsulated*
	User to user Information		*Encapsulated*
SGM	User to User Information	INVITE request, 18x response (to INVITE request), 200 (OK) response (to INVITE request) (see note)	*Encapsulated*
FAC, FAA, FRJ	Facility Indicator	INFO request	*Encapsulated*
USR	User to User Information	INFO request	*Encapsulated*
REL	User to User Indicators	4XX-6XX response (to INVITE request), BYE request	*Encapsulated*
	User to User Information		*Encapsulated*
NOTE: The ISUP message is reassembled prior to sending the corresponding SIP message. The SGM message is never sent across SIP.			

All service related information is encapsulated. The call will be allowed to continue in the case that the UUS service is marked as non-essential and the ISUP message is not delivered. However, the service will not be allowed. Per the service specification "Interworking with Other Networks" the service request will assume to be rejected if no explicit response is provided. However, to provide more explicit failure information, the following handling procedures may be invoked as a network option:

- If the interworking node has knowledge that the encapsulated ISUP information IAM message explicitly requesting the non-essential service was not delivered (based on the Accept header returned from the far node) it can mark the returned ACM as "service not provided".
- If the interworking node has knowledge that the terminating node supports ISUP, but that the ISUP IAM message requesting an implicit service (UUS1) was not delivered, then the returned ACM can be marked as "UUI discarded".
- If the interworking node has knowledge that the ISUP IAM message for an essential UUS is not delivered, then the interworking node should return a REL with cause #29.

6.9.21 Anonymous Call Rejection (ACR)

Table 6.21: Anonymous Call Rejection

ISUP Information		SIP Information	
Message	Parameter	Message	Header
IAM	Calling Party Number	INVITE request	P-Asserted-Identity
REL (cause value)	Cause Indicators	4xx-6xx response (to INVITE request), BYE request	Reason

All service related information is be mapped into SIP headers. Therefore, if the encapsulated ISUP message is not delivered, the service will be unaffected.

6.10 Interfaces to the AGCF

Study of the protocol requirements for interface to the AGCF within the IMS-based PES indicate that the information transfer need is for the use of particular parameters that could be coded within ISUP. However clause 5.3.3 of TS 182 012 [12] now states:

- "The protocol used for the Mw reference point is SIP. SIP messages exchanged over the Mw reference point may contain encapsulated ISUP information, except between the AGCF and a CSCF."

Discussion has identified the Calling Party Category parameter as a particularly useful piece of information to encode. However discussions are currently in progress in IETF that may result in the ability to encode this information within SIP itself, and therefore it is concluded that any solution for carriage of information to the AGCF need not be provided by carriage of the ISUP parameter.

The proposed solution in the present document therefore need not cover interfaces to the AGCF.

6.11 Summary of protocol decisions

The following conclusions are drawn from the contents of clauses 6.2 through 6.10.

1) **Supported interfaces:** The proposed solution in the present document need not cover interfaces to the AGCF. Information transfer is covered between MGCFs, between ASs, and between an MGCF and an AS, inclusive of intermediate IMS entities.

2) **Security:** Confidentiality of encapsulated ISUP information will be met by removing ISUP information destined toward an untrusted entity or network. This function may be performed variously by an IBCF, a P-CSCF or an AS provided to the subscriber.

3) **New profile:** A new interworking profile to those defined in ITU-T Recommendation Q.1912.5 [10] should be defined. The new interworking profile will be substantially based on the existing interworking profile C (SIP-I) but will differ in the key characteristics identified by the remaining conclusions.

4) A SIP endpoint that sends or receives a SIP message containing encapsulated ISUP information for a supported service may construct or process the encapsulated ISUP information message according to the relevant service specification. Sending of an encapsulated ISUP information Confusion message when handling an unrecognized or unsupported parameter or message is optional.

5) **Compatibility of initial INVITE request:** New rules for ISUP compatibility are defined such that a SIP endpoint sending an initial INVITE request with an encapsulated IAM information shall mark it with mandatory disposition if the ISUP preference indicator is set to "ISUP required all the way". A SIP endpoint receiving an initial INVITE request with encapsulated ISUP information marked with optional disposition may ignore any unrecognized or unsupported ISUP information. When a SIP endpoint receives an initial INVITE request that includes encapsulated ISUP information with mandatory disposition, and the endpoint cannot decode or recognize the encapsulated ISUP information, the endpoint shall reject the INVITE request with a 415 (Unsupported Media Type) response. A SIP endpoint receiving an initial INVITE request with encapsulated ISUP information marked with mandatory disposition should reject the INVITE request with a 603 (Decline) response if the encapsulated ISUP information includes an ISUP parameter unrecognized or unsupported by the endpoint where the parameter requires call release according to ISUP procedures when unsupported or unrecognized.

6) **Compatibility of transparent ISUP information:** When sending category two encapsulated ISUP information, the sender shall always include it in a 183 Session Progress or SIP INFO request message. Encapsulated information in a 183 may only be marked as optional disposition. Encapsulated information in an INFO may be marked as either optional or mandatory disposition. The sender shall wait for acknowledgment of the first reliable response before sending the INFO request. A UAS may need to send a reliable provisional response if an INFO request is pending and the UAS has not previously sent and received acknowledgment for a provisional response. When a SIP endpoint receives a SIP INFO request that includes encapsulated ISUP information with required disposition and the endpoint cannot decode or recognize the encapsulated ISUP information, the endpoint shall reject the INFO request with a 415 (Unsupported Media Type) response. When a SIP endpoint receives a SIP INFO request that includes encapsulated ISUP information with required disposition with that is unrecognized or unsupported by the endpoint, and any of the unrecognized or unsupported information has either no compatibility indicators or compatibility indicators requiring call release if it cannot be processed or forwarded, the endpoint shall reject the SIP INFO request with a 603 (Decline) response. When a SIP endpoint receives a SIP INFO request that includes encapsulated ISUP information with ISUP information for a supported service, the endpoint shall process the encapsulated ISUP information message according to the relevant ISUP specification. When a SIP endpoint received encapsulated ISUP information marked with optional disposition that is unrecognized or unsupported, the endpoint may either ignore the information or act upon any compatibility indicators that may be present. When a SIP endpoint receives a 415 or 603 (Decline) response message in response to having sent a SIP INFO request with encapsulated ISUP information, the endpoint shall abort the ISUP procedure associated with the encapsulated ISUP information message and back off to the corresponding ISUP procedure defined for interworking the service with other networks. If the encapsulated ISUP information contains message and/or parameter compatibility parameters, the SIP endpoint shall perform the procedures appropriate for pass on not possible. Failure of the INFO transaction does not impact the state of the ongoing dialog, which will continue according to RFC 2976 [17]. When a SIP endpoint receives a 200 (OK) response message in response to having sent a SIP INFO request with encapsulated ISUP information, the endpoint shall continue ISUP procedures related to the transmitted ISUP message according to the relevant ISUP specification.

7) **Compatibility of messages other than INVITE request and INFO request:** A SIP endpoint shall mark with optional disposition all NSS message bodies it sends in messages other than the initial SIP INVITE request and the SIP INFO request. A SIP endpoint indicating support for ISUP may ignore unsupported or unrecognized ISUP information encapsulated in any SIP message it receives in messages other than the initial INVITE request and the INFO request.

8) **Method of ISUP encapsulation:** NSS message bodies shall be used to encapsulate ISUP information.

9) **Interworking with other profiles:** The procedures defined by this new SIP profile provide interoperability with the existing IMS SIP profile.

Furthermore, TISPAN has agreed to limit the scope of the NSS procedures described in the present document for TISPAN Release 1 to IMS PES. More general applicability to IMS is for further study outside Release 1.

7 Proposed amendments to TISPAN NGN specifications

7.1 Introduction and key

The proposals in clause 7 represent proposed amendments to a number of TISPAN NGN specifications.

Clause numbering within these amendments is in accordance with the addressed specification. Where the clause is entirely new, no textual markings are made. Where an existing clause is modified, proposed new text is marked by underline, and proposed deleted text by strikeout.

7.2 Proposed amendments to TS 183 043 - application server procedures

Start of proposed new clause

5.3.3.5 Transport of ISUP information

5.3.3.5.1 General

Clause 5.3.3.5 describes the general behaviour of the PES application server in the case the PES application server is capable of exchanging ISUP information, as defined in ITU-T Recommendation Q.763, carried within Narrowband Signalling Syntax (NSS) message bodies with its SIP signalling peers to perform service related signalling that is capable of interworking with PSTN services. Clause C.1.4 lists examples of services some of which may require the use of encapsulated ISUP information. The sending or receiving of ISUP information in NSS message bodies is applicable to any of the following roles of the Application Server:

- PES application server acting as terminating UA or redirect server.
- PES application server acting as originating UA.
- PES application server performing 3rd party call control.

The procedures defined in the following clauses allow a PES application server to discover whether or not its peer SIP signalling entity (i.e. the next UA along the signalling path, which may be a B2BUA, and therefore excluding any intermediate proxies) is capable of supporting NSS message bodies within SIP messages, and to successfully support the additional exchange of ISUP information needed for those services supported in common by endpoints supporting potentially different sets of services. Each IMS PES must assure that NSS message bodies are not forwarded to UEs and are not forwarded to untrusted SIP networks according to local policy. Clause 5.3.3.5.2.4 describes the role of the PES application server in maintaining NSS security.

NOTE: Services that require manipulation of the ISUP information within NSS message bodies cannot be implemented on application servers acting as a SIP proxy.

The PES application server shall support parameter translations and defaults defined in ES 283 027 for the ISUP information needed for supported services. The PES application server shall also send each piece of ISUP information in the appropriate SIP message so as to allow the valid interworking with the corresponding PSTN services according to ES 283 027. The PES application server shall not include in NSS message bodies any ISUP information that is already represented by SIP signalling.

The handling of forked requests with NSS message bodies is for further study.

5.3.3.5.2 Sending NSS message bodies to a peer SIP signalling entity

5.3.3.5.2.1 General

The PES application server shall send an NSS message body with encapsulated ISUP information in the appropriate SIP message to a peer SIP signalling entity according to the clauses 5.3.3.5.2.2 through 5.3.3.5.2.7, when all the following conditions are satisfied.

- The PES application server is capable of performing service related signalling using ISUP information for one or more of the services it supports.
- An event associated with one of the supported services occurs that requires that ISUP information be sent to the peer SIP signalling entity. This event may be the receipt of signalling information from another SIP interface to the PES application server, or a service event internal to the PES application server.
- Either the encapsulating message is the initial INVITE request, or the peer SIP signalling entity has previously indicated support for NSS message bodies within the associated dialog (see clause 5.3.3.5.2.2).
- The SIP signalling in the encapsulating message cannot represent the information, and the information is different from the default values defined in ES 283 027.

5.3.3.5.2.2 Determining support for NSS message bodies

When constructing an initial INVITE request, an originating PES application server that supports any services that require encapsulated ISUP information shall include an indication of support for NSS by including an Accept header in the initial INVITE request that indicates support for NSS ("application/nss") according to clause 5.3.3.5.2.3. Until the originating PES application server receives an indication of support for NSS message bodies from its peer SIP signalling entity (by receipt of a SIP message that either includes an Accept header indicating support for NSS or an NSS message body), the originating PES application server shall not send any further NSS message bodies within the dialog.

If a terminating PES application server receives an initial INVITE request that does not include an Accept header indicating support for NSS, the terminating PES application server shall not send NSS message bodies within the dialog. If a terminating PES application server supporting any services that require the signalling of ISUP information receives an initial INVITE request that includes an Accept header indicating support for NSS, the terminating PES application server shall indicate support of NSS in the first SIP message to its SIP signalling peer. The terminating PES application server indicates support of NSS using the Accept header if allowed in the SIP message. Otherwise, the terminating PES application server does this by including an NSS message body in the SIP message. In the later case, if there is no need to send ISUP information to the SIP signalling peer in the first SIP message, the terminating PES application server shall send a Generic Parameter List (GPL) NSS message with no parameters.

A terminating PES application server not supporting NSS will follow procedures in clause 5.3.3.5.3.1.

5.3.3.5.2.3 NSS message bodies

The PES application server shall format the NSS message body according to ITU-T Recommendation Q.1980.1. The Content-Type header field associated with the NSS message body shall be included as follows:

- Content-Type: application/nss.

The Content-Disposition header field associated with the NSS message body shall be set in one of the following two ways (see clause 5.3.3.5.2.7):

- Content-Disposition: signal; handling = required; or
- Content-Disposition: signal; handling = optional.

5.3.3.5.2.4 ISUP information security

If network entities in the IMS PES cannot be relied on to provide ISUP information confidentiality and integrity, then the PES application server shall not send NSS message bodies or process received NSS message bodies (other than ignoring or rejecting any NSS message bodies).

A PES application server acting as routeing B2BUA shall remove NSS message bodies and indications of NSS support (e.g. an NSS entry in the Accept header) from SIP messages being forwarded towards each UE. If a PES application server is assigned to remove the NSS message bodies from SIP messages being forwarded to a UE, then the PES application server shall be configured within the terminating filter criteria for its UE.

5.3.3.5.2.5 Determining in which message to encapsulate ISUP information

If a service logic event coincides with one of the SIP basic call control messages, i.e. INVITE request, re-INVITE request, BYE request, UPDATE request, or responses to these messages, any required ISUP information shall be encapsulated in the corresponding SIP message.

If a service logic event requiring the sending of ISUP information occurs that does not coincide with one of the SIP basic call control messages, the PES application server shall send the ISUP information encapsulated in an INFO request or a 183 (Session Progress) response, as described below.

An originating PES application server cannot send an INFO request until it receives a reliable provisional response or final response.

A terminating PES application server cannot send an INFO request until a reliable provisional response or final response has been sent by the PES application server and the response has been acknowledged. If service logic requires an NSS message body marked with optional handling (see clause 5.3.3.5.2.7) to be sent before an INFO request can be sent, the terminating PES application server may send the NSS message body in a 183 (Session Progress) reliable response. If the service logic requires an NSS message body marked with required handling to be sent before an INFO request can be sent, the terminating PES application server shall first send a 183 (Session Progress) reliable response without an NSS message body and wait for acknowledgment of the response before sending the NSS message body in the INFO request.

5.3.3.5.2.6 Determining the NSS message identifier code

If the ISUP information included in the NSS message body uniquely identify the ISUP message needed to interwork the ISUP information to an ISUP interface, or if the interworking with ISUP is unambiguously identified by the SIP signalling and/or the encapsulated ISUP information, the PES application server shall include the ISUP information in an NSS GPL message. Otherwise, the PES application server shall include an explicit ISUP message name in the NSS message body.

5.3.3.5.2.7 Determining the content disposition handling

5.3.3.5.2.7.1 Content disposition for the initial INVITE request

A PES application server sending an INVITE request with an NSS message body shall mark it for required handling (see clause 5.3.3.5.2.3) if the service logic requires the peer SIP signalling entity to understand the ISUP information.

Otherwise, the PES application server shall mark the NSS message body in the initial INVITE request for optional handling.

If the peer SIP signalling entity is unable to process an NSS message body marked for required handling in an initial INVITE request, it will reject the INVITE request with a failure response, allowing the originating PES application server, or perhaps a proxy on the path, to optionally retry the request to an alternate destination that may be capable of handling the NSS message body.

5.3.3.5.2.7.2 Content disposition for the INFO request

A PES application server sending an INFO request with an NSS message body shall mark it for required handling if the service logic requires the peer SIP signalling entity to understand the ISUP information.

Otherwise, the PES application server shall mark the NSS message body in the INFO request for optional handling.

If the peer SIP signalling entity rejects an NSS message body in an INFO request by returning a failure response, the PES application server performs the service procedure that applies when unable to signal ISUP information, if such a procedure exists, and continues the call associated with the parent dialog. The PES application server shall release the call if the INFO request fails and there is any ISUP information in the INFO request that requires call release if it cannot be processed or forwarded.

5.3.3.5.2.7.3 Content disposition for other SIP messages

If the previous clauses do not apply, the PES application server shall mark the NSS message body in the SIP message for optional handling.

NOTE: A PES application server sending an NSS message body in any SIP response message will mark it for optional handling, since the peer SIP signalling entity cannot reject the message.

5.3.3.5.3 Receiving an NSS message body from a peer SIP signalling entity

5.3.3.5.3.1 General

On receipt of a SIP message containing an NSS message body, a PES application server supporting services that require encapsulated ISUP information shall de-encapsulate the ISUP information from the NSS message body, perform the processing described in the clause 5.3.3.5.3.2, and trigger the relevant service logic.

If the PES application server does not receive ISUP information required by the service logic, the service logic defines the PES application server behaviour, e.g. by assuming default values defined by the service logic.

5.3.3.5.3.2 ISUP compatibility procedures

A PES application server shall reject with a SIP 603 (Decline) response a SIP request that includes an NSS message body that is marked for required handling, that includes ISUP information that the PES application server does not support, and that either includes no compatibility parameter for the unsupported information, or includes a compatibility parameter for the unsupported information that requires release when the parameter is unsupported. Otherwise, the PES application server shall ignore any unsupported ISUP information.

The PES application server may ignore any unsupported ISUP information it receives in an NSS message body marked for optional handling or perform any other behaviour determined by the service logic.

End of proposed new clause

7.3 Proposed amendments to TS 183 043 - MGCF procedures

Start of proposed new clause

5.3.5.4 Transport of ISUP information

5.3.5.4.1 General

The procedures in the clause 5.3.5.4 allow the PES interworking application to discover whether or not its peer SIP signalling entity is capable of supporting the encapsulation of ISUP information in Narrowband Signalling Syntax (NSS) message bodies within SIP messages, and to successfully support the additional exchange of ISUP information needed for those services supported in common by endpoints supporting potentially different sets of services. These procedures are based on ES 283 027 with the extended capabilities described in the present document. When signalling ISUP information within a SIP dialog, the PES interworking application shall act as either a Type A or Type B exchange depending on the role (e.g. gateway between operators, transit) the PES interworking application is performing for that particular call and the ability to exchange ISUP information during the call. Clause C.1.4 lists examples of services some of them may require the use of encapsulated ISUP information. Each IMS PES must assure that ISUP information is not shared with UEs and untrusted SIP networks according to local policy. Clause 5.3.5.4.2.4 describes the PES interworking application's role in maintaining NSS security.

The PES interworking application shall support parameter translations and defaults defined in ES 283 027 for the ISUP information needed for supported services. The PES interworking application shall also send each piece of ISUP information in the appropriate SIP message so as to allow valid interworking with the corresponding PSTN services according to ES 283 027. The PES interworking application shall not include in NSS message bodies any ISUP information that is already represented by SIP signalling.

The handling of forked requests with NSS message bodies is for further study.

5.3.5.4.2 Sending ISUP information to a peer SIP signalling entity

5.3.5.4.2.1 General

The PES interworking application shall send an NSS message body with encapsulated ISUP information in the appropriate SIP message to a peer SIP signalling entity according to the clauses 5.3.5.4.2.2 through 5.3.5.4.2.7, when all the following conditions are satisfied.

- Either the encapsulating message is the initial INVITE request, or the peer SIP signalling entity has previously indicated support for NSS message bodies within the associated dialog (see clause 5.3.5.4.2.2).
- An event occurs requiring signalling to the peer SIP signalling entity. This event may be the receipt of an ISUP message from the PSTN, or an event internal to the MGCF.
- According to local configuration, selected ISUP information shall be encapsulated and sent towards the peer SIP signalling entity.

- The SIP signalling in the encapsulating message cannot represent the information, and the information is different from the default values defined in ES 283 027.

5.3.5.4.2.2 Determining support for NSS message bodies

When constructing an initial INVITE request, the O-MGCF supporting NSS message bodies shall include an indication of support for NSS by including an Accept header in the initial INVITE request that indicates support for NSS ("application/nss") according to clause 5.3.5.4.2.3. Until the O-MGCF receives an indication of support for NSS message bodies from its peer SIP signalling entity (by receipt of a SIP message that either includes an Accept header indicating support for NSS or an NSS message body), the O-MGCF shall not send any further NSS message bodies within the dialog.

If an I-MGCF receives an initial INVITE request that does not include an Accept header indicating support for NSS, the I-MGCF shall not send NSS message bodies within the dialog. If an I-MGCF supporting NSS receives an initial INVITE request that includes an Accept header indicating support for NSS, the I-MGCF shall indicate support of NSS in the first SIP message to its SIP signalling peer. The I-MGCF indicates support of NSS using the Accept header if allowed in the SIP message. Otherwise, the I-MGCF does this by including an NSS message body in the SIP message. In the later case, if there is no need to send ISUP information to the SIP signalling peer in the first SIP message, the I-MGCF shall send a generic parameter list (GPL) NSS message with no parameters.

5.3.5.4.2.3 NSS message bodies

The PES interworking application shall format the NSS message body according to ITU-T Recommendation Q.1980.1. The Content-Type header field associated with the NSS message body shall be included as follows:

Content-Type: application/nss

The Content-Disposition header field associated with the NSS message body shall be set in one of the following two ways (see clause 5.3.5.4.2.7):

- Content-Disposition: signal; handling = required; or
- Content-Disposition: signal; handling = optional.

5.3.5.4.2.4 ISUP information security

If network entities in the IMS PES cannot be relied on to provide NSS confidentiality and integrity, then the PES interworking application shall not send NSS message bodies or process received NSS message bodies (other than ignoring or rejecting any NSS message bodies).

5.3.5.4.2.5 Determining in which SIP message to encapsulate ISUP information

If an event requiring the sending of ISUP information coincides with one of the SIP basic call control messages, i.e. INVITE request, re-INVITE request, BYE request, UPDATE request, or responses to these messages, any required ISUP information shall be encapsulated in the corresponding SIP message.

If an event requiring the sending of ISUP information occurs that does not coincide with one of the SIP basic call control messages, the AS shall send the ISUP information encapsulated in an INFO request or a 183 (Session Progress) response, as described below. Clause 5.3.5.4.4 describes events unrelated to SIP basic call control messages that may require the sending of ISUP information.

An O-MGCF cannot send an INFO request until it receives a reliable provisional response or final response.

An I-MGCF cannot send an INFO request until a reliable provisional response or final response has been sent by the I-MGCF and the response has been acknowledged. If an event requires an NSS message body marked with optional handling (see clause 5.3.5.4.2.7) to be sent before an INFO request can be sent, the I-MGCF may send the NSS message body in a 183 (Session Progress) reliable response. If an event requires an NSS message body marked with required handling to be sent before an INFO request can be sent, the I-MGCF shall first send a 183 (Session Progress) reliable response without an NSS message body and wait for acknowledgment of the response before sending the NSS message body in the INFO request.

5.3.5.4.2.6 Determining the NSS message identifier code

If the ISUP information included in the NSS message body uniquely identify the ISUP message needed to interwork the ISUP information to an ISUP interface, or if the interworking with ISUP is unambiguously identified by the SIP signalling and/or the encapsulated ISUP information, the PES interworking application shall include the ISUP information in an NSS GPL message. Otherwise, the PES interworking application shall include an explicit ISUP message name in the NSS message body.

5.3.5.4.2.7 Determining the content disposition handling

5.3.5.4.2.7.1 Content disposition for the initial INVITE request

An O-MGCF sending an initial INVITE request with an NSS message body shall mark it for required handling (see clause 5.3.5.4.2.3) in any of the following cases:

- The ISUP preference indicator received from the PSTN is set to "ISUP required all the way".
- The parameter compatibility parameter associated with any ISUP parameter in the NSS message body indicates "release call" or "discard message" when pass on is not possible.
- As a matter of local policy.

Otherwise, the O-MGCF shall mark the NSS message body in the initial INVITE request for optional handling.

If the peer SIP signalling entity is unable to process an NSS message body marked for required handling in an initial INVITE request, it will reject the INVITE request with a failure response, allowing the O-MGCF, or perhaps a proxy on the path, to optionally retry the request to an alternate destination that may be capable of handling the NSS message body.

5.3.5.4.2.7.2 Content disposition for the INFO request

If an event occurs requiring the sending of an NSS message body, the event does not coincide with one of the SIP basic call control messages (see table 1 in clause 5.3.5.4.4.1), and any failure procedures are defined when unable to pass on ISUP information in the NSS message body to the peer SIP signalling entity, the PES interworking application shall mark the NSS for required handling. For example, the "Interactions with other networks" clause of each relevant supplementary service specification (see Table C.1.4) specifies the PES interworking application procedures when unable to pass on ISUP information. Otherwise, the PES interworking application shall mark the NSS message body for optional handling.

Otherwise, the O-MGCF shall mark the NSS message body in the INFO request for optional handling.

If the peer SIP signalling entity rejects an NSS message body in an INFO request by returning a failure response, the PES interworking application performs the service procedure for failing to pass on the ISUP information, if such a procedure exists, and continues the call associated with the parent dialog. The PES interworking application shall release the call if the INFO request fails and there is any ISUP information in the INFO request that requires call release if it cannot be processed or forwarded.

5.3.5.4.2.7.3 Content disposition for other SIP messages

A PES interworking application sending an NSS message body in any SIP message other than the INVITE request and the INFO request shall mark it for optional handling.

NOTE: A PES interworking application sending an NSS message body in any SIP response message will mark it for optional handling, since the peer SIP signalling entity cannot reject the message.

5.3.5.4.3 Receiving an NSS message body from a peer SIP signalling entity

5.3.5.4.3.1 General

On receipt of a SIP message containing an NSS message body, the PES interworking application supporting NSS shall de-encapsulate the ISUP information from the NSS message body, perform the processing described in clauses 5.3.5.4.3.2 and 5.3.5.4.3.3, and pass the ISUP information to the relevant ISUP procedures.

5.3.5.4.3.2 ISUP compatibility procedures (local policy options)

A PES interworking application shall reject with a SIP 603 (Decline) response a SIP request that includes an NSS message body that is marked for required handling, that includes ISUP information that the PES interworking application does not support, and that requires release according to ISUP procedures when unsupported. Otherwise, the PES interworking application shall ignore any unsupported ISUP information.

The PES interworking application may ignore any unsupported ISUP information it receives in an NSS message body marked for optional handling or perform any other behaviour determined by the ISUP procedures.

5.3.5.4.3.3 Alignment of SIP signalling and NSS message body contents

On receipt of a SIP message containing an NSS message body, the PES interworking application shall use the encapsulated ISUP information in preference to any value determined by interworking procedures and default values defined in ES 283 027.

5.3.5.4.4 ISUP messages for special consideration

5.3.5.4.4.1 General

Table 7.1 below lists the PES interworking application behaviour upon receipt of ISUP messages that have no counterparts in basic SIP call control messages.

Table 7.1: ISUP messages for special consideration

ISUP message	Reference
Subsequent address message	5.3.5.4.4.6
Reset circuit	5.3.5.4.4.2
Call progress	5.3.5.4.4.3 (see note 1)
Circuit group blocking	5.3.5.4.4.2
Circuit group blocking acknowledgement	5.3.5.4.4.2
Circuit group query (national use)	5.3.5.4.4.2
Circuit group query response (national use)	5.3.5.4.4.2
Group reset	5.3.5.4.4.2
Circuit group reset acknowledgement	5.3.5.4.4.2
Confusion	5.3.5.4.4.2 or 5.3.5.4.4.3 (see note 2)
Facility reject	5.3.5.4.4.2 or 5.3.5.4.4.3 (see note 2)
User-to-user information	5.3.5.4.4.3
Forward transfer	5.3.5.4.4.3
Subsequent directory number (national use)	5.3.5.4.4.3
Suspend	5.3.5.4.4.3 or 5.3.5.4.4.5
Resume	5.3.5.4.4.3 or 5.3.5.4.4.5
Blocking	5.3.5.4.4.2
Blocking acknowledgement	5.3.5.4.4.2
Continuity check request	5.3.5.4.4.2
Continuity	5.3.5.4.4.2
Unblocking	5.3.5.4.4.2
Unblocking acknowledgement	5.3.5.4.4.2
Unequipped CIC (national use)	5.3.5.4.4.2
Circuit group unblocking	5.3.5.4.4.2
Circuit group unblocking acknowledgement	5.3.5.4.4.2
Charging information (national use)	5.3.5.4.4.3
Facility accepted	5.3.5.4.4.3
Facility request	5.3.5.4.4.3
User part test	5.3.5.4.4.2
User part available	5.3.5.4.4.2
Facility	5.3.5.4.4.3
Network resource management	5.3.5.4.4.3
Identification request	5.3.5.4.4.3
Identification response	5.3.5.4.4.3
Information (national use)	5.3.5.4.4.3
Information request (national use)	5.3.5.4.4.3
Segmentation	5.3.5.4.4.4
Loop back acknowledgment (national use)	5.3.5.4.4.3
Loop prevention	5.3.5.4.4.3
Overload (national use)	5.3.5.4.4.2
Pass-along (national use)	5.3.5.4.4.3
Application transport	5.3.5.4.4.2 or 5.3.5.4.4.3 (see note 2)
Pre-release information	5.3.5.4.4.3
Release complete	5.3.5.4.4.2
NOTE 1: This is the default handling of the ISUP information associated with the Call Progress (CPG) message when other clauses in the specification do not apply. The ISUP information associated with a CPG message may be encapsulated in a 18X response, an UPDATE request, a reINVITE request, or an INFO request. NOTE 2: The ISUP information in the these messages is either locally terminated or sent transparently depending on whether it is destined for the PES interworking application or for another exchange.	

5.3.5.4.4.2 ISUP side procedures only

ISUP information from these messages is not encapsulated within SIP messages since they relate to procedures that are relevant only for the ISUP interface. Typically these messages are related to maintenance of ISUP circuits. If ISUP information associated with these ISUP messages is received within an NSS message body, the ISUP information shall be discarded.

5.3.5.4.4.3 Transparent messages

If the PES interworking application is configured to forward ISUP information meant for end-to-end service transparency, the PES interworking application shall send the ISUP information through the SIP network as described in clause 5.3.5.4.2.5.

5.3.5.4.4.4 ISUP segmentation

ISUP information from the Segmentation message itself is not encapsulated within SIP. Instead the PES interworking application will reassemble the original message received from the PSTN with its segmented part and encapsulate any relevant information in accordance with other procedures in the present document.

5.3.5.4.4.5 Receipt of network initiated SUS and RES

If the I-MGCF is not the controlling exchange for network initiated Suspend procedures and NSS message bodies are supported by the peer SIP signalling entity, then the I-MGCF shall forward ISUP information from received SUS and RES in NSS message bodies.

If the I-MGCF is the controlling exchange for network initiated Suspend procedures or is unable to forward SUS information to the peer SIP signalling entity, the I-MGCF shall invoke the procedures described in ITU-T Recommendation Q.764 clause 2.4.1c on the ISUP interface and shall not forward ISUP information from either SUS or RES.

5.3.5.4.4.6 Subsequent address message

When receiving overlap signalling on the ISUP interface, the PES interworking application shall include the current values of all encapsulated ISUP information in each INVITE request.

End of proposed new clause

7.4 Proposed amendments to TS 183 043 - IBCF procedures

Start of proposed new clause

5.3.6.2 Procedures related to NSS message bodies

Depending on local policy, the PES interconnection application in an IMS PES supporting NSS, acting as a B2BUA, may perform any reasonable combination of the following functions related to an NSS message body within a received SIP message, where the message is to be forwarded either into or outside of the IMS PES:

- Removal of an Accept header list entry for NSS ("application/nss");
- Removal of an NSS message body marked for optional handling;
- Filtering of NSS message body parameters (e.g. removal of ISUP information associated with a service not supported by the network); and
- Rejection of a SIP request that includes an NSS message body marked for required handling by returning a SIP 415 (Unsupported Media Type) response.

A PES interconnection application shall only forward NSS message bodies to or from trusted networks supporting NSS.

End of proposed new clauses

7.5 Proposed amendments to TS 183 043 - list of supplementary services

Start of proposed new clause

C.1.4 Supplementary services using ISUP information

Full support of supplementary services may be realized by exchanging service information between peer SIP signalling entities via SIP signalling and/or encapsulated ISUP information. The ISUP information necessary to support each individual service is specified by the corresponding ETSI or ITU-T supplementary service specification; see table 1.

Table C.1: Supplementary Service References

Supplementary Service	ETSI/ITU-T Reference
Calling Line Identification Presentation (CLIP)	EN 300 356-3
Calling Line Identification Restriction (CLIR)	EN 300 356-4
COnnected Line Identification Presentation (COLP)	EN 300 356-5
COnnected Line Identification Restriction (COLR)	EN 300 356-6
Terminal Portability (TP)	EN 300 356-7
User-to-User Signalling (UUS)	EN 300 356-8
Closed User Group (CUG)	EN 300 356-9
SUBaddressing (SUB)	EN 300 356-10
Malicious Call Identification (MCID)	EN 300 356-11
CONFerence Call (CONF)	EN 300 356-12
Explicit Call Transfer (ECT)	EN 300 356-14
Call Forwarding Busy (CFB)	EN 300 356-15
Call Forwarding No Reply (CFNR)	EN 300 356-15
Call Forwarding Unconditional (CFU)	EN 300 356-15
Call Deflection (CD)	EN 300 356-15
Call HOLD (HOLD)	EN 300 356-16
Call Waiting (CW)	EN 300 356-17
Completion of Calls to Busy Subscriber (CCBS)	EN 300 356-18
Three-PartY (3PTY)	EN 300 356-19
Completion of Calls on No Reply (CCNR)	EN 300 356-20
Anonymous Communication Rejection (ACR)	TS 183 011
Multi-Level Precedence and Pre-emption (MLPP)	ITU-T Q.735.3
Global Virtual Network Service (GVNS)	ITU-T Q.735.6
REVerse charging (REV)	ITU-T Q.736.3

End of proposed new clause

Annex A: Messages and parameters used by the supplementary services

Table A.1: Messages and parameters used by the supplementary services

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Initial Address Message	■	■	■		■	■					■	■			■	■	■	■	■	
Access transport		◈			◈															
Called party number	✓																			
Calling party category																				
Calling party number		✓																		✓
CCSS											×	×								
CUG interlock code															◈					
Forward call indicators											× (3)	× (3)			× (3)				× (3)	
Forward GVNS																	◈			
Generic number		✓ (1)																		
Original called number						✓ (2)														
Optional forward call indicator			◈												◈					
Precedence																◈				
Redirection information						✓ (2)														
Redirecting number						✓ (2)														

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Remote operations																		◈		
User to user indications																			◈ × (4)	
User to user information																			◈	
Address Complete						■		■				■				■				
Call diversion information						✓ (2)														
CCNR possible												◈								
Generic notification indicators						✓ (2)		●								●				
Optional backward call indicators						◈										◈				
Redirection number						✓ (2)														
Redirection number restriction indicator						✓ (2)														
User to user indications																			◈ × (4)	
User to user information																			◈	
Call Progress						■	■	■	■			■	■	■		■			■	
CCNR possible												◈								

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Call diversion information						✓ (2)														
Call Transfer Number							●													
Event indicator						✓ (2)														
Generic notification indicator						✓ (2)	●	●	●				●	●		●				
Optional backward call indicators						◈										◈				
Redirection number						✓ (2)														
Redirection number restriction indicator						✓ (2)														
User to user indications																			◈ ✕ (4)	
User to user information																			◈	
Answer			■			■											■	■	■	
Access Transport			◈																	
Backward GVNS																	◈			
Connected Number			✓																	
Generic Number			◈																	
Redirection number						✓ (2)														

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Redirection number restriction indicator						✓ (2)														
Remote Operations																		◈		
User to user indications																			◈ ✕ (4)	
User to user information																			◈	
Connect			■			■											■	■		
Access Transport			◈																	

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Backward GVNS																	◈			
Connected Number			✓																	
Generic Number			◈																	
Redirection number						✓ (2)														
Restriction indicator						✓ (2)														
Remote operations																		◈		
User to user indicators																			◈ × (4)	
User to user information																			◈	
Segmentation																			■	
User to user information																			◈	

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Identification Request				■																
MCID Request Indicators				◈																
Identification Response				■																
MCID Response indicators				◈																
Calling party number				◈																
Access Transport				◈																
Generic Number				◈																
Facility							■											■		
Access Transport							●													
Call transfer number							●													
Generic notification indicators							●													
Remote operations																		◈		
Service Activation							●													
Facility Request																			■	
Facility indicator																			◈	

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Facility Accepted																			■	
Facility indicator																			◈	
Facility Reject																			■	
Facility indicator																			◈	
User to User Information																			■	
User-to-user information																			◈	
Loop Prevention							■													
Call Transfer Reference							◈													
Loop prevention indicators							◈													
Suspend										■										
Suspend Indicators										●										
Resume										■										
Resume Indicators										●										

	DDI	CLIP/ CLIR	COLP/ COLR	MCID	SUB	CFB/ CFNR/ CFU/ CD	ECT	CW	HOLD	TP	CCBS	CCNR	CONF	3PTY	CUG	MLPP	GVNS	REV	UUS	ACR
Release											■					■		■	■	
Cause indicators											×					◈				●
Remote operations																		◈		
User to user indications																			◈ × (4)	
User to user information																			◈	

History

Document history		
V1.1.1	May 2006	Publication