



SOCIETY OF CABLE
TELECOMMUNICATIONS
ENGINEERS, INC.

ENGINEERING COMMITTEE
Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-18 2004
(formerly DSS 02-17)

IPCablecom CMS to CMS Signaling

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the Standards. Such adopting party assumes all risks associated with adoption of these Standards, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this standard have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc.
140 Philips Road
Exton, PA 19341

Contents

1	INTRODUCTION	6
1.1	SCOPE	6
1.2	SPECIFICATION LANGUAGE.....	6
2	REFERENCES	7
2.1	NORMATIVE REFERENCES	7
2.2	INFORMATIVE REFERENCES	8
2.3	REFERENCE ACQUISITION.....	8
3	TERMS AND DEFINITIONS.....	8
4	ABBREVIATIONS AND ACRONYMS.....	9
5	BACKGROUND AND MOTIVATION	10
5.1	REQUIREMENTS AND DESIGN PRINCIPLES	10
5.2	IPCABLECOM ARCHITECTURE.....	11
5.3	CMSS TRUST MODEL	12
5.4	CMS TO CMS ARCHITECTURAL MODEL	13
5.5	OVERVIEW OF CMS BEHAVIOR	15
5.6	BASIC TELEPHONY CALL FLOW	15
5.7	CMS-MGC BASIC TELEPHONY CALL FLOW.....	17
6	SIP PROFILE	19
6.1	INTRODUCTION	20
6.2	OVERVIEW OF SIP FUNCTIONALITY	20
6.3	TERMINOLOGY.....	20
6.4	OVERVIEW OF OPERATION.....	20
6.5	STRUCTURE OF THE PROTOCOL.....	20
6.6	DEFINITIONS.....	20
6.7	SIP MESSAGES	20
6.7.1	Requests	20
6.7.2	Responses	21
6.7.3	Header Fields	21
6.7.4	Bodies	21
6.7.5	Framing SIP Messages	21
6.8	GENERAL USER AGENT BEHAVIOR	21
6.8.1	UAC Behavior.....	21
6.8.2	UAS Behavior.....	22
6.8.3	Redirect Servers.....	22
6.9	CANCELING A REQUEST.....	22
6.10	REGISTRATIONS	22

6.11	QUERYING FOR CAPABILITIES	22
6.12	DIALOGS	22
6.12.1	Creation of a Dialog.....	22
6.12.2	Requests within a Dialog.....	23
6.12.3	Termination of a Dialog	23
6.13	INITIATING A SESSION	23
6.14	MODIFYING AN EXISTING SESSION	23
6.15	TERMINATING A SESSION	23
6.16	PROXY BEHAVIOR	23
6.17	TRANSACTIONS	23
6.18	TRANSPORT	23
6.19	COMMON MESSAGE COMPONENTS	24
6.19.1	SIP and SIPS URI Component.....	24
6.20	HEADER FIELDS	24
6.20.1	Accept	24
6.20.2	Accept-Encoding	24
6.20.3	Accept-Language	25
6.20.4	Alert-Info.....	25
6.20.5	Allow	25
6.20.6	Authentication-Info	25
6.20.7	Authorization	25
6.20.8	Call-ID	25
6.20.9	Call-Info	25
6.20.10	Contact	25
6.20.11	Content-Disposition	26
6.20.12	Content-Encoding.....	26
6.20.13	Content-Language.....	26
6.20.14	Content-Length.....	26
6.20.15	Content-Type.....	26
6.20.16	CSeq	26
6.20.17	Date.....	26
6.20.18	Error-Info	26
6.20.19	Expires	26
6.20.20	From	27
6.20.21	In-Reply-To.....	27
6.20.22	Max-Forwards	27
6.20.23	Min-Expires	27
6.20.24	MIME-Version.....	27
6.20.25	Organization	27
6.20.26	Priority	27
6.20.27	Proxy-Authenticate	27
6.20.28	Proxy-Authorization	27
6.20.29	Proxy-Require	28
6.20.30	Record-Route	28
6.20.31	Reply-To.....	28
6.20.32	Require.....	28
6.20.33	Retry-After	28
6.20.34	Route.....	28
6.20.35	Server.....	28
6.20.36	Subject	28

6.20.37 Supported.....	28
6.20.38 Timestamp.....	28
6.20.39 To	28
6.20.40 Unsupported.....	29
6.20.41 User-Agent	29
6.20.42 Via	29
6.20.43 Warning	29
6.20.44 WWW-Authenticate	29
6.21 RESPONSE CODES.	29
6.22 USAGE OF HTTP AUTHENTICATION	29
6.23 S/MIME	30
6.24 EXAMPLES	30
6.25 AUGMENTED BNF FOR THE SIP PROTOCOL.....	30
6.26 SECURITY CONSIDERATIONS: THREAT MODEL AND SECURITY USAGE RECOMMENDATIONS	30
6.27 TABLE OF TIMER VALUES	30
7 SIP EXTENSIONS.....	30
7.1 URIS FOR TELEPHONE CALLS	31
7.1.1 Syntax	31
7.1.2 Procedures at an Originating CMS.....	34
7.1.3 Procedures at a Terminating CMS	35
7.1.4 Procedures at Proxy.....	35
7.2 RELIABILITY OF PROVISIONAL RESPONSES	35
7.3 SIP UPDATE METHOD	35
7.4 INTEGRATION OF RESOURCE MANAGEMENT AND SIP	35
7.4.1 Procedures at an Originating CMS.....	35
7.4.2 Procedures at a Terminating CMS	35
7.5 SIP-SPECIFIC EVENT NOTIFICATION.....	36
7.6 THE REFER METHOD	36
7.6.1 Procedures at an Originating CMS.....	36
7.6.2 Procedures at a Terminating CMS	36
7.7 SIP PROXY TO PROXY EXTENSIONS FOR SUPPORTING DCS.....	36
7.7.1 P-DCS-Trace-Party-ID	36
7.7.2 P-DCS-Gate	36
7.7.3 P-DCS Option Tag	36
7.8 THE SIP "REPLACES" HEADER	36
7.9 PRIVATE EXTENSIONS TO THE SIP PROTOCOL FOR ASSERTED IDENTITY WITHIN TRUSTED NETWORKS	36
7.10 A MESSAGE SUMMARY AND MESSAGE WAITING INDICATION EVENT PACKAGE FOR THE SESSION INITIATION PROTOCOL (SIP).....	37
7.10.1 Background and Appropriateness	37
7.10.2 Event Package Formal Definition	38
7.10.3 Formal Syntax	40
8 CMS-CMS SIGNALING.....	42
8.1 CMS INTERFACES	42

8.1.1	Overview of CMS Behavior	44
8.1.2	Overview of Tandem Proxy	48
8.2	CMS RETRANSMISSION, RELIABILITY, AND RECOVERY STRATEGIES	49
8.3	CMS TO CMS ROUTING	49
8.3.1	Forming a SIP-URI from a tel-URI.....	49
8.3.2	Routing a SIP-URI at Tandem CMSeS	50
8.3.3	Routing based on tel-URI	50
8.4	CMS PROCEDURES.....	50
8.4.1	CMS Messages and Procedures for Basic Call Setup	50
8.4.2	Initiating an Emergency Call.....	76
8.4.3	CMS Procedures for REFER.....	76
8.4.4	CMS handling of Mid-Call Changes	81
8.4.5	CMS handling of Call Teardown.....	91
8.4.6	Sample Implementation of Call Transfer	92
8.4.7	Sample Implementation of Ad-hoc Conference.....	98
8.4.8	Automatic Callback.....	98
8.4.9	Message Waiting Indicator	100
9	APPLICATION LAYER ANONYMIZER	102
9.1	SIGNALING CONTENT PRIVACY	103
9.2	IP ADDRESS PRIVACY	103
APPENDIX I - TIMER SUMMARY		106
APPENDIX II - CMSS MESSAGE AND HEADER OVERVIEW		106
APPENDIX III - THE SESSION INITIATION PROTOCOL (SIP) "REPLACES" HEADER.....		110
APPENDIX IV - ACKNOWLEDGMENTS		117

Figures

Figure 1: System Architecture – Realm.....	Error! Bookmark not defined.
Figure 2: Trusted Domain of IPCablecom Service Provider	Error! Bookmark not defined.
Figure 3: CMS Signaling Model.....	Error! Bookmark not defined.
Figure 4: CMS – CMS Signaling Basic Call Flow.....	Error! Bookmark not defined.
Figure 5: CMS to MGC Signaling.....	Error! Bookmark not defined.
Figure 6: CMS to CMS Signaling.....	Error! Bookmark not defined.
Figure 7: Overview of Interdomain Telephony Call Flow.....	Error! Bookmark not defined.
Figure 8: Call Forwarding Support	Error! Bookmark not defined.
Figure 9: REFER Support	Error! Bookmark not defined.
Figure 10: CMS Messages for Basic Call Setup	Error! Bookmark not defined.
Figure 11: Initiation of Call Transfer/Ad Hoc Conference	Error! Bookmark not defined.
Figure 12: Failure ca– F1 – no free conference circuits.....	Error! Bookmark not defined.
Figure 13: Establishing the leg from Bridge Server to Party C	Error! Bookmark not defined.
Figure 14: Failure ca– F2 – Party C busy	Error! Bookmark not defined.
Figure 15: On-hook initiates transfer action.....	Error! Bookmark not defined.
Figure 16: Relocation of Party B to Bridge	Error! Bookmark not defined.
Figure 17: Transfer completed, CMS ₁ ends involvement in call.....	Error! Bookmark not defined.
Figure 18: End of transferred call	Error! Bookmark not defined.
Figure 19: Application Layer Anonymizer.....	Error! Bookmark not defined.
Figure 20: Anonymizer Functions.	Error! Bookmark not defined.
Figure 21: Privacy Issues.	Error! Bookmark not defined.

1 INTRODUCTION

1.1 Scope

This document describes the IPCablecom Call Management Server (CMS) to CMS Signaling protocol intended for use by a CMS to communicate with another CMS in order to support packet-based voice and other real-time multimedia applications. The protocol exchanges between a CMS and a Media Gateway Controller (MGC) are identical to those between CMSes, and so for purposes of this specification the MGC is considered identical to a CMS. CMSes currently support multimedia endpoints (within the IPCablecom infrastructure) that use the Network-based Call Signaling [5] (NCS) protocol and the PSTN Gateway Call Signaling Protocol [6] (TGCP) for communicating signaling information between the endpoint and the CMS. In the future, other protocols may be supported as well, and the CMS to CMS protocol is intended to be sufficiently general to accommodate such protocols without change.

The CMS to CMS protocol uses the Session Initiation Protocol 2.0 (SIP) specification with extensions and usage rules that support commonly available local and CLASSSM services. This protocol is referred to as the Call Management Server Signaling (CMSS) protocol.

The CMSS protocol takes into account the need to manage access to network resources and account for resource usage. The usage rules defined in this specification specifically address the coordination between CMS Signaling and IPCablecom Dynamic Quality of Service (QoS) mechanisms for managing resources over the cable access network. In addition, this specification defines the protocols and messages needed between Call Management Servers for supporting these services.

This document specifies the protocols and procedures to use between CMSes belonging to a single service provider as well as between CMSes that belong to different service providers. In the case that the CMSes are owned by multiple service providers, it is assumed that the service providers have a mutual trust relationship.

Other IPCablecom documents describe interfaces between other system elements. These documents cover areas such as: Event Message recording for billing and other back office functions [3]; Dynamic Quality of Service [4]; Operations and Provisioning [28]; Electronic Surveillance [24]; and Security [2]. These other specifications indirectly place requirements on the signaling protocol to ensure that it transports the correct data needed to implement a complete system. This document includes syntax and protocols for implementing these requirements. Currently, the document does not address interworking with non-IPcablecom-compliant devices.

1.2 Specification Language

It is understood that implementing this recommendation is optional. If this Recommendation is implemented, the key words “MUST” and “SHALL” as well as “REQUIRED” are to be interpreted as indicating a mandatory aspect of this specification. The key words indicating a certain level of significance of particular requirements that are used throughout this Recommendation are summarized in the table below:

“MUST”	This word or the adjective “REQUIRED” means that the item is an absolute requirement of this specification.
“MUST NOT”	This phrase means that the item is an absolute prohibition of this specification.
“SHOULD”	This word or the adjective “RECOMMENDED” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
“SHOULD NOT”	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
“MAY”	This word or the adjective “OPTIONAL” means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- [1] ANSI/SCTE 24-1 2001 (formerly DSS 00-02) – IPCablecom Part 1: Architectural Framework for the delivery of time critical services over cable television networks using cable modems.
- [2] ANSI/SCTE 24-10 2002 (formerly DSS 02-16) – IPCablecom Part 10: Security Specification.
- [3] ANSI/SCTE 24-9 2001 (formerly DSS 00-14) – IPCablecom Part 9: Event Message Requirements
- [4] ANSI/SCTE 24-4 2001 (formerly DSS 00-04) – IPCablecom Part 4: Dynamic quality of service for the provision of real-time services over cable television networks using data modems.
- [5] ANSI/SCTE 24-3 2001 (formerly DSS 00-03) – IPCablecom Part 3: Network call signaling protocol for the delivery of time critical services over cable television networks using data modems.
- [6] ANSI/SCTE 24-12 2001 (formerly DSS 00-17) – IPCablecom Part 12: Trunking Gateway Control Protocol (TGCP).
- [7] ANSI/SCTE 24-15 2002 (formerly DSS 02-12) - IPCablecom Interdomain Quality of Service.
- [8] IETF RFC 3261, Rosenberg, J., Schulzrinne, H. Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M, E. Schooler, SIP: Session Initiation Protocol, June 2002.
- [9] ITU-T Recommendation E.123 - Notation for national and international telephone numbers, e-mail addresses and Web addresses (02/01)
- [10] ITU-T Recommendation E.164 - The international public telecommunication numbering plan. (05/97)
- [11] IETF RFC 2327 - Handley, M, V. Jacobson, SDP: Session Description Protocol, April 1998.
- [12] IETF RFC 1890 - Schulzrinne, H, RTP Profile for Audio and Video Conferences with Minimal Control, January, 1996.
- [13] IETF RFC 768 - Postal, J, User Datagram Protocol, August 1980.
- [14] IETF RFC 3312 - Integration of Resource Management and SIP for IP Telephony, October, 2002.
- [15] IETF RFC 3262 - Reliability of Provisional Responses in SIP, June, 2002.
- [16] IETF RFC 3323 - J. Peterson, A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002.
- [17] IETF RFC 3325 - C. Jennings, J. Peterson, M. Watson; Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks; November 2002.
- [18] IETF RFC 3265 - Adam Roach, SIP-Specific Event Notification, June 2002.
- [19] IETF RFC 3311 - J. Rosenberg, "The SIP UPDATE Method", October, 2002
- [20] IETF RFC 3263 - J. Rosenberg, H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", June 2002.
- [21] IETF RFC 2234 - Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", November 1997.
- [22] IETF RFC 2397 - L. Masinter, "The "data" URL Scheme", August 1998.
- [23] IETF RFC 2396 - T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", August 1998.
- [24] ANSI/SCTE 24-13 2001 (formerly DSS 00-18) - IPCablecom Part 13: Electronic Surveillance Standard
- [25] IETF RFC 3420 - Robert Sparks, Internet Media Type message/sipfrag, November 2002.
- [26] IETF RFC 3603 – W. Marshall and F. Andreassen, Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture, October 2003.

- [27] IETF RFC 3515 – R.Sparks, The Session Initiation Protocol (SIP) Refer Method, April 2003.

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

- [28] ANSI/SCTE 24-5 2001 (formerly DSS 00-10) – IPCablecom Part 5: Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems.
- [29] ANSI/SCTE 24-2 2001 (formerly DSS 00-01) – IPCablecom Part 2: Audio Codec requirements for the provision of bidirectional audio service over cable television networks using cable modems.
- [30] ANSI/SCTE 24-17 2002 (formerly DSS 02-14) - IPCablecom Audio Server Protocol.
- [31] IETF RFC 791, Transmission Control Protocol, Postal, J., September 1981
- [32] W. Marshall, M.Osman, F.Andreasen, D.Evans, “Architectural Considerations for Providing Carrier Class Telephony Services Utilizing SIP-based Distributed Call Control Mechanisms”, work in progress, January 2003
- [33] IETF RFC 2806 - A. Vaha-Sipila, "URLs for Telephone Calls", April 2000
- [34] H. Schulzrinne, A. Vaha-Sipila, "The tel URI for Telephone Calls", work in progress, June 2002.
- [35] J. Yu, "Extensions to the "tel" URL to Support Number Portability and Freephone Service", work in progress, June 2002.
- [36] R. Mahy, “A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”, work in progress, May 2002
- [37] IETF RFC 3398, G. Camarillo, A. Roach, J. Peterson, L. Ong, “Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping”, December 2002
- [38] PacketCable 1.2 Architecture Framework, PKT-TR-ARCH1.2-V01-001229, December 29, 2000, www.packetcable.com/specifications

2.3 Reference Acquisition

ITU-T Recommendations available at: <http://www.itu.int/ITU-T>

IETF RFCs available at: <http://www.ietf.org/rfc/>

SCTE Standards available at: www.scte.org

3 TERMS AND DEFINITIONS

This Recommendation defines the following terms:

Active	A service flow is said to be “active” when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be “admitted” when the CMTS has reserved resources (e.g. bandwidth) for it on the DOCSIS network.
Announcement Server	An announcement server plays informational announcements in IPCablecom network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
CNAM	Calling Name
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU

Event Message	Message capturing a single portion of a connection
Gateway	Devices bridging between the IP/Cablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway which sends and receives circuit switched network signaling to the edge of the IP/Cablecom network.
Header	Protocol control information located at the beginning of a protocol data unit.
Key	A mathematical value input into the selected cryptographic algorithm.
LNP	Local Number Portability
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Off-Net Call	A communication connecting an IP/Cablecom subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the IP/Cablecom Network
Privacy	A way to ensure that information is not disclosed to any one other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key which can decrypt messages sent encrypted by the user's public key.
Trunk	An analog or digital connection from a circuit switch which carries user media content and may carry voice signaling (MF, R2, etc.).

4 ABBREVIATIONS AND ACRONYMS

This Recommendation defines the following abbreviations and acronyms.

BCID	Billing Correlation ID
BLV	Busy Line Verification
CA	Call Agent
CFNA	Call Forwarding No Answer
CLASS	Custom Local Area Signaling Services
CMTS	Cable Modem Termination System
CNAM	Calling Name
DCS	Distributed Call Signaling
EI	Emergency Interrupt
E.164	Telephone number standard of ITU
FQDN	Fully Qualified Domain Name
GC	Gate Controller
IP	Internet Protocol
LNP	Local Number Portability
LRN	Local Routing Number
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MTA	Multimedia Terminal Adapter
NCS	Network Call Signaling
OSPS	Operator Services Positioning System
RFC	Request for Comments (IETF standard)
SDP	Session Description Protocol

5 BACKGROUND AND MOTIVATION

The material contained in this section and its subsections is informative. The design of the Call Management Server Signaling (CMSS) architecture recognizes the trend towards use of packet networks as the underlying framework for communications. These networks will provide a broad range of services, including traditional best-effort data service, as well as enhanced value-added services such as telephony and gaming. The Network based Call Signaling (NCS) and PSTN Gateway Call Signaling (TGCP) protocols are used to communicate between limited-function multimedia end-points, such as standard telephone sets and trunking gateways, and Call Management Servers (CMS). However, the NCS and TGCP protocols do not address the need for communication between multiple CMSes residing in one or more service providers' networks. This document covers the signaling performed between CMSes. The initial real-time multimedia service that is supported by the NCS and TGCP function is that of interactive telephony. The NCS and TGCP protocols represent the same architecture and are largely similar. In the following, where a distinction is not important, they will sometimes be simply referred to as NCS.

It is recognized that packet based networks may also offer additional real-time multimedia services to endpoints that are IP capable. Also, improvements in silicon will reinforce the trend towards increased functionality and "intelligence" in endpoints. These intelligent endpoints will be addressed in a future document to take advantage of the widespread availability of packet networks to enable a rich set of applications and services for users.

A key element of the CMSS architecture is a recognition of the need for coordination between call signaling, which controls access to telephony specific services, and resource management, which controls access to network-layer resources. This coordination is designed to meet the user expectations and human factors associated with telephony. For example, in a telephony environment, the called party should not be alerted until the resources necessary to complete the call are available. If resources were not available when the called party picked up, the user would experience a call defect. In addition, PSTN users expect to be charged for service only after the called party answers the phone. As a result, it must be possible to track usage accounting in a way that allows customer billing to start once the called party picks up. Coordination between call signaling and resource management is also needed to prevent fraud. The coordination between call signaling and Dynamic QoS [4] protocols ensures that users are authenticated and authorized before receiving access to the enhanced QoS associated with the telephony service.

In the NCS and TGCP protocols, the functionality required of the multimedia endpoint is simple, and more of the functionality resides in the network in call management servers, where the state of a session is maintained. The CMS is responsible for establishing and managing session legs, and for requesting and obtaining network layer QoS for the session. The NCS and TGCP protocols specify the information and message exchanges between the multimedia endpoint and the CMS. When the session has to be routed through multiple CMSes, additional functionality is required in the protocol to communicate the information related to the session. This includes information provided by the endpoint to the network as well as information that may reside in the CMS or other entities within the network that relates to the session. Examples of such additional information that may reside in the network include billing and data that may otherwise be kept private from untrusted multimedia endpoints.

5.1 Requirements and Design Principles

This section briefly describes the application requirements that led to the set of CMSS design principles.

The need to support primary line telephony service requires enhanced bearer channel and signaling performance, including:

- *Low delay* – end-to-end packet delay must be sufficiently small that it does not interfere with normal multimedia sessions. The ITU recommends no greater than 300 ms roundtrip delay for a telephony service.
- *Low packet loss* – packet loss must be sufficiently small that it does not perceptibly impede session quality or, in the case of telephony, performance of fax and voice band modems.
- *Short post-dial delay* – the delay between dialing the last digit and receiving positive confirmation from the network must be sufficiently short to ensure that users do not perceive a difference from post-dial delays typically experienced in the circuit switched network; in particular, the delay must not be so long that the user is led to believe that the network has failed.
- *Short post-pickup delay* – the delay between a user picking up a ringing phone or acknowledging a multimedia session and the voice or media path being cut through must be sufficiently short to ensure that the initial talk-spurt, e.g., "hello", is not clipped.

A number of key design principles that arise from the requirements and philosophy above are identified:

- It is essential to provide network-layer Quality of Service while allowing the service provider to derive revenues from the use of such service.

- The CMSS architecture must allow for communication between CMSes in the network. At a high level, one may regard a CMS as performing complex signaling tasks on behalf of an endpoint. When the network includes multiple CMSes, CMSS should provide the call signaling function between the CMSes on an individual call basis. Within such a context, the CMSS architecture must allow the network to support limited-function multimedia endpoints, while allowing additional functions to be performed by the CMSes (including the maintaining call state in the CMSes).
- The architecture must ensure that the network is protected from fraud and theft of service. The service provider must be able to authenticate users requesting service and to ensure that only those authorized to receive a particular service are able to obtain it. Furthermore, the service provider must be able to track the usage of such services in order to support billing.
- The architecture must enable the service provider to add value by supporting the functions of a trusted intermediary. In the case of telephony, this includes protecting the privacy of calling and called party information, and ensuring the accuracy of the information that is provided in messages from the network.
- The architecture must be implementable, cost-effectively, at very large scale.

5.2 IPcablecom Architecture

The CMS to CMS Signaling (CMSS) Architecture follows the principles outlined above to support a robust multimedia service. Figure 1 introduces the key components in the architecture. In addition, the definitions of all IPcablecom elements (Domain, Realm, etc.) are provided in the IPcablecom Interdomain Architecture Technical Report [1].

Multimedia Terminal Adapters (MTAs) may either be embedded into the Cable Modem (CM) or they may be stand-alone. The cable access network interfaces to an IP backbone through a CMTS that is the first trusted element within the provider's network. The CMTS performs network resource management, acts as a policy enforcement point, and as a source of event messages that can be used for billing.

The CMS establishes and receives sessions on behalf of an endpoint by using the NCS protocol to communicate with the MTA. The CMS uses the protocol specified here to communicate with other CMSes. In addition, it may also perform the function of a Gate Controller (GC), which is responsible for authorizing the enhanced Quality of Service for the media stream. The CMS acts as a source of event messages that can be used for billing.

Media Service Nodes represent network-based components that operate on media flows to support the service. Media service nodes perform audio bridging, play announcements, provide interactive voice response services, etc. The protocol exchanges between a CMS and a Media Service Nodes are identical to those between CMSes, and so for purposes of this document a Media Service Node is considered identical to a CMS. Media Service Nodes may be decomposed into a controller and a player, in which case CMSS signaling is performed with the controller.

PSTN gateways interface to the Public Switched Telephone Network. The PSTN gateway may be decomposed into a Media Gateway Controller (MGC), a signaling gateway (SG), and a Media Gateway (MG). The TGCP protocol is used between the MGC and the MG. The protocol exchanges between a CMS and an MGC are identical to those between CMSes, and so for purposes of this document, the MGC is considered identical to a CMS.

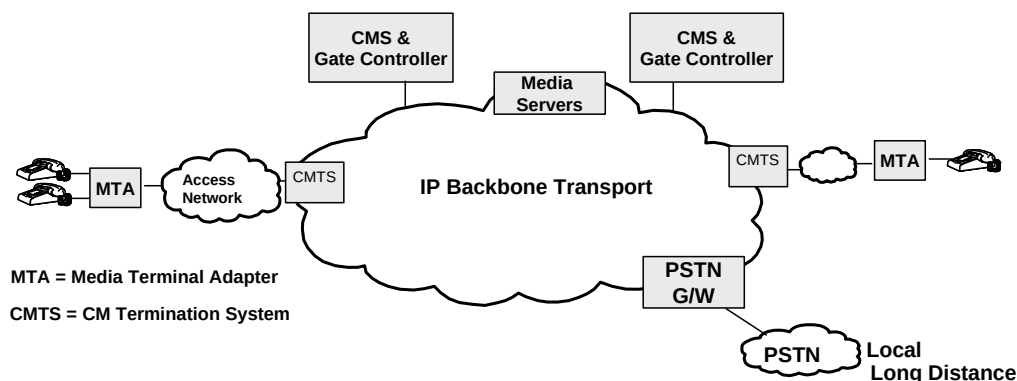


Figure 1: System Architecture – Realm

Access to network resources must be controlled by the service provider. The CMTS receives resource management requests from endpoints, and is responsible for ensuring that packets are provided the QoS they are authorized to receive (either through packet marking, or through routing and queuing the packets as a specific QoS-assured flow). The CMTS requires authorization from a Gate Controller (on a session by session basis for the multimedia service) before providing access to enhanced QoS for an end-to-end IP flow. Thus, the CMTS is able to ensure that enhanced QoS is provided only for end-to-end flows that have been authorized and for which usage accounting is being performed. Since the CMTS knows about the resource usage associated with individual IP flows, it generates the usage events that allow a user to be charged for service [3].

DQoS [4] introduces the concept of a “gate” in the CMTS. Conceptually, gates manage access to enhanced quality of service. The gate is a packet classifier and policer that ensures that only those IP flows that have been authorized by the CMS are granted access to enhanced QoS in the access and backbone networks. Gates are “admitted” selectively for a flow. For a multimedia service, gates are opened and controlled for individual sessions. Admitting a gate involves an admission control check that is performed when a resource reservation or commit request is received from the endpoint, and it may involve resource reservation in the backbone network if necessary. The packet filter in the gate allows a flow of packets to receive enhanced QoS for a session from a specific IP source address and port number to a specific IP destination address and port number.

CMSes implement a set of service-specific control functions required to support the telephony service:

- Authentication and authorization: Since services are only provided to authorized subscribers, CMSes authenticate signaling messages and authorize requests for service on a session-by-session basis.
- Name/number translation and call routing: CMSes translate dialed numbers or names to a terminating IP address based on call routing logic.
- Service-specific admission control: CMSes can implement a broad range of admission control policies for the telephony service. For example, CMSes may provide precedence to particular calls, *e.g.*, emergency calls initiated by dialing a special number such as 911. Admission control may also be used to implement overload control mechanisms, *e.g.*, to restrict the number of calls to a particular location or to restrict the frequency of call setup to avoid signaling overload.
- Signaling and service feature support: CMSes maintain and track all signaling activities to insure compliance and to manage subscriber features. For example, in the case of telephony, 3-way calling, caller ID, etc.

A CMS is responsible for a set of endpoints and the associated CMTSes. While endpoints are not trusted, there is a trust relationship between the CMTS and its associated CMSes, since the Gate Controllers in the CMSes play a role as a policy server that controls when the CMTS can provide enhanced QoS service. There is also a trust relationship among CMSes. Details of the security model and mechanisms are specified in [2].

CMSS supports inter-working with the circuit switched telephone network through PSTN gateways. A PSTN gateway may be realized as a combination of a Media Gateway Controller (MGC), Media Gateway (MG), and a Signaling Gateway (SG). A media gateway acts as the IP peer of an endpoint for media packets, converting between the data format used over the IP network and the format required for transmission over the PSTN, *e.g.*, PCMU. The signaling gateway acts as the IP peer of a PSTN endpoint for call signaling, providing signaling inter-working between the IP/Cablecom network and conventional telephony signaling protocols such as ISUP/SS7. The MGC uses the PSTN Gateway Call Signaling Protocol (TGCP) to control the operation of the media gateway.

There are additional system elements that may be involved in providing the multimedia service [1]. For example, in the case of telephony service, the CMS may interface with other servers that implement the authorization or translation functions. Similarly, announcements, voicemail, and three-way calling may be supported using media service nodes in the network. Management of security interfaces between system elements is explained in [2].

This document provides generic capabilities that can be used to implement additional features. Features that have an intra/inter-domain (CMS-CMS) impact are considered and specifically addressed below.

5.3 CMSS Trust Model

CMSS defines a trust boundary around the various systems and servers that are within a single domain. These trusted systems include the Internal and External Border Proxies¹, CMSes, CMTSes of the cable access network, and various servers such as bridge servers, voicemail servers, announcement servers, etc. Outside of the trust boundary are the customer premises equipment, *i.e.*, the MTAs, the Public Switched Telephone Network (PSTN)², and various media

¹ More generally referred to as tandem proxies or simply proxies.

² but not the PSTN GW.

service nodes operated by third-party service providers. At the boundary of the trusted domain are CMTSes/Edge Routers at the transport level and EBP/CMSes at the signaling level. The EBP interfaces to other IPCablecom domains. Although these other IPCablecom domains are outside the trust boundary, CMSS still trusts call signaling sent to and received from these other IPCablecom domains.

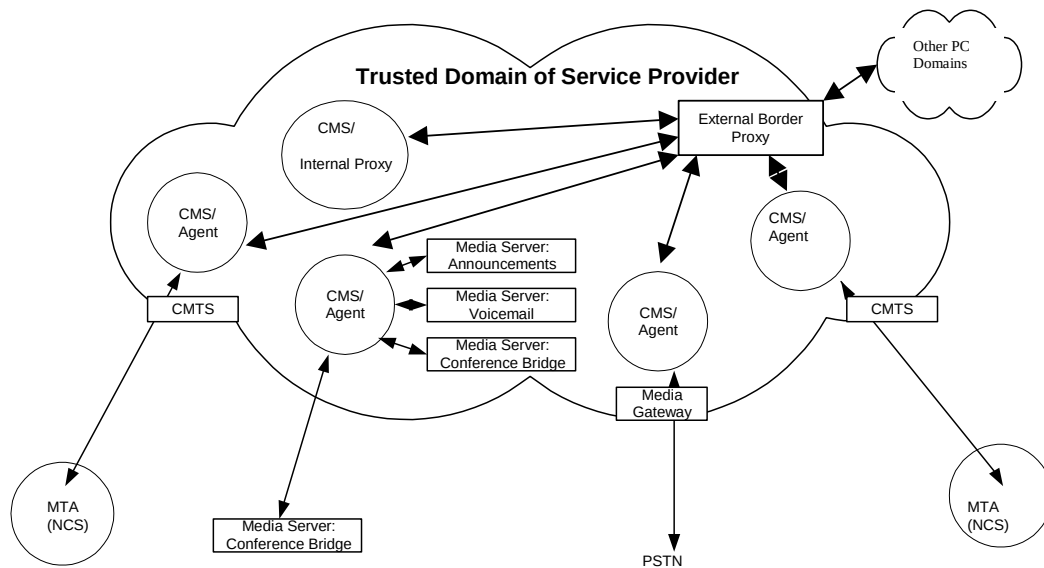


Figure 2: Trusted Domain of IPCablecom Service Provider

5.4 CMS to CMS Architectural Model

The Call Management Server (CMS) is an architectural entity that performs those services necessary to enable endpoints to establish IP multimedia sessions. The CMS is a complex of server functions that support session signaling, number translation, and feature support. In addition to processing signaling messages, the CMS provides functions for service and feature authorization, call routing, and service-specific admission control. As a trusted decision point, the CMS may also coordinate with Gate Controllers (which act as Policy Decision Points from a resource management point of view) to control when resource reservations are authorized for particular users and media flows.

This document describes the messages required to support IP Telephony between entities that support one or more of the roles indicated in the following table:

Role	Distinguishing function
Call Agent (CA) or CMS as defined above.	Support of endpoints implementing Network-Based Call Signaling (NCS) [5].
Media Gateway Controller (MGC)	Interworking with the PSTN. Use of PSTN Gateway Call Signaling (TGCP) [6] to control trunks.
Announcement Servers, Bridge Servers, or VoiceMail Servers	Provide various media services.
Tandem server within a domain, or a gateway server between service provider domains.	Routing functions only.

The list of roles may be expanded in the future. Although trust level varies between providers, the document assumes CMSEs within a REALM and across multiple domains trust each other. MTAs, however, are untrusted NCS endpoints. Note: where multiple roles are combined within a single node, the interface between them is hidden and untestable.

All of the various types of endpoint management systems currently fall into one of two different categories of CMSes. A CMS³ is a trusted entity that establishes calls on behalf of an untrusted endpoint, *e.g.*, an MTA, in the customer premise. The role of the CMS is to verify the signaling messages from the untrusted source, and provide various network services, such as translation, authentication and accounting. The second category is the Proxy. Proxies are

³ CMS/MGC and other types of centralized control CMSEs fall within this category as well.

classified into two types: proxies used within a domain, and proxies used between domains. The Interior Border Proxy (IBP) [38] is a proxy that can be used for inter-realm (intra-domain) signaling and the Exterior Border Proxy (EBP) [38] is required for inter-domain signaling. See the IPCablecom Inter-Domain Architecture Document [38] for further details. Where a distinction between the different types of proxy is either unimportant or is evident from the text, they will be simply referred to as proxies or tandem proxies.

A CMS is a SIP User Agent (UA). If the CMS controls NCS endpoints, the CMS furthermore contains a Gate Controller (GC) with a hidden and untestable interface between the UA and the GC as shown in Figure 3. The Tandem Proxy, EBP and IBP entities are SIP proxies. Specification of a GC-to-UA interface is left as for further study.

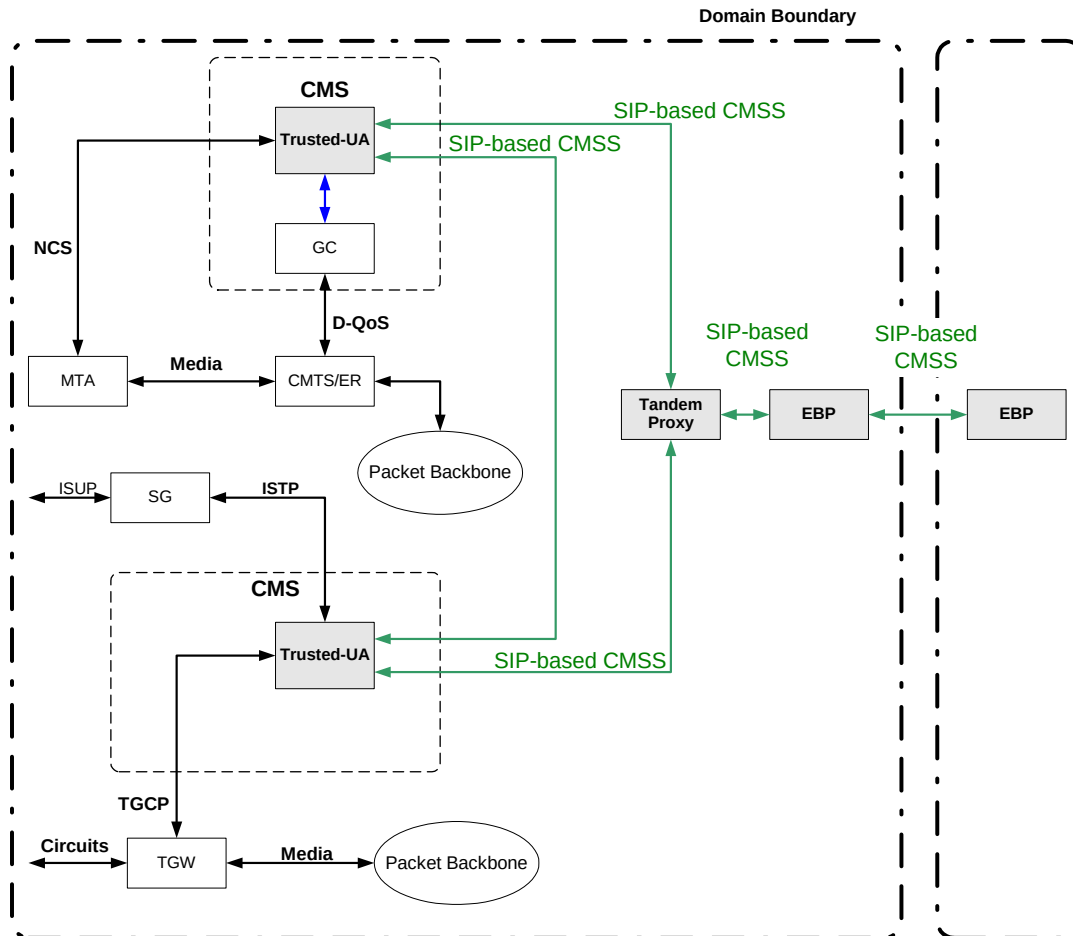


Figure 3: CMS Signaling Model

A CMS establishes connections either on its own behalf or on behalf of a non-SIP endpoint. Examples of the former are voicemail and conference bridge servers; in these cases the CMS is a trusted network entity that establishes connections on its own behalf. Examples of the latter are the Call Agent (CA) described in NCS [5], the Media-Gateway-Controller (MGC) described in [6], and the Announcement Controller (ANC) described in [30] in all of these cases there is centralized call control, protocol messages, *e.g.*, NCS, are exchanged between the CMS and the endpoint device, and the endpoint device does not participate in the SIP signaling exchanges directly.

The term CMS in this document refers to either of the above categories. Where only one category is being described, the term proxy⁴ or CMS will be used as a representative for the category being described.

Unless otherwise stated in this document, a CMS MUST follow the requirements given for SIP user agents in [8] and a proxy MUST follow the requirements given for SIP proxies and redirect servers in [8].

⁴ This may be further refined, *e.g.* into IBP and EBP. The term tandem proxy may also be used instead of just proxy.

Tandem proxies act as call routers and security association aggregation points. They may also provide additional functions such as signaling transformation gateways, signaling firewalls, etc. Depending on its role, a tandem proxy may remain in the call-signaling path for the duration of the call. More detailed tandem proxy information can be found in section 8.1.2.

5.5 Overview of CMS Behavior

IPCablecom defines the Call Management Server (CMS) as a complex of server functions which support call signaling, number translation, call routing, feature support and admission control. Within the CMS complex, the IPCablecom architecture allocates many of these responsibilities to the Proxy/CA/MGC and the Gate Controller (GC) function. In addition to processing session-signaling messages, a CMS provides functions for service and feature authorization, name/number translation, session routing, and service-specific admission control. As a trusted decision point, the CMS may also coordinate with Gate Controllers (which act as Policy Decision Points from a resource management point of view) to control when resource reservations are authorized for particular users. While the CMS is responsible for session control functions associated with proxying signaling requests, the Gate Controller is responsible for the policy decision regarding whether a requested QoS level should be admitted. Upon receipt of signaling information, a CMS instructs the Gate Controller to authorize a QoS level in advance of any resource reservation signaling (see [4] for more details).

The CMS associated with the endpoint originating a call is referred to as the originating CMS and is denoted by CMS_O. The CMS associated with the terminating endpoint is referred to as the terminating CMS and is denoted by CMS_T. The Gate Controllers (GC_O, GC_T) are the trusted policy decision points for controlling when and which resources are allowed to be reserved by endpoints; they coordinate with the CMTSes (CMTS_O, CMTS_T) through DQoS signaling. The CMTSes are the policy enforcement points, and ensure that the media path is provided the QoS it is authorized to receive.

The IPCablecom CMS-CMS architecture extends the use of the basic INVITE/200-OK/ACK SIP transaction. A provisional response, the 183-Session-Progress, and its acknowledgement, the PRACK/200-OK, are used with the initial INVITE to exchange capabilities and establish session state in the network prior to alerting the user. Following this exchange, the endpoints engage in resource reservations to obtain the resources they will need for the media streams. If the resource reservations are successful, the originating CMS performs an UPDATE/200-OK exchange. At this point the initial INVITE continues with a 180-Ringing or 183-Session-Progress, then a PRACK/200-OK followed by the final 200-OK response and ACK to the initial INVITE. In all cases, all provisional and final responses to an INVITE message traverse the path taken by the original INVITE through one or more CMSes and proxies; other messages, however, pass end-to-end directly between the originating CMS and the terminating CMS.

In support of billing functions, the originating CMS (CMS_O) includes information containing the account number of the caller and the Billing-Correlation-ID in the INVITE message that it sends.

Operator services such as Busy Line Verification (INVITE(BLV)) and Emergency Interrupt (INVITE(EI)) are initiated from a Media-Gateway-Controller type of CMS and sent to the number being verified/interrupted.

In call sequences associated with three-way calling, inter-domain call transfer, and inter-domain call forwarding, the CMS performs redirection. One possibility is that the CMS simply passes revised SDP to the other CMS, causing a redirection of media flow without changing the call topology. Alternatively, the CMS makes use of the REFER method to redirect the entire call. The REFER causes the receiver to initiate a new call using the information provided.

5.6 Basic Telephony Call Flow

Figure 4 presents a high-level overview of an example basic call that uses the CMSS protocol between the CMSes through a proxy while the end-points (MTAs) are using the NCS protocol.

In this example⁵, when the MTA goes off-hook and the user dials a telephone number, the originating MTA (MTA_O) collects the dialed digits and exchanges initial NCS messages with the originating CMS (CMS_O) to notify it of the dialed digits and create a (media) connection. As a result of creating the connection, MTA_O returns a session description using the Session Description Protocol (SDP), which will subsequently be passed to CMS_T. When CMS_O wishes to ensure that adequate resources are available in the network before users who wish to communicate are alerted, it includes additional information in the SDP. This additional information is a “Pre-Condition” (possibly a set of pre-conditions including both security and resource requirements) that needs to be satisfied before the terminating user is alerted. CMS_O verifies that MTA_O is a valid subscriber of the telephony service and determines that this subscriber is

⁵ Call flows throughout this document are examples only; IPCablecom does not mandate particular call flows.

authorized to place this call. CMS_O then translates the dialed number into the address of a terminating CMS (CMS_T) and sends the (1) INVITE message to it containing the SDP with the added pre-conditions.

It is assumed that the originating and terminating CMSes trust each other. CMS_O includes additional information, such as billing data containing the telephone number of the caller, in the INVITE message that it sends to CMS_T via the proxy. CMS_T then translates the dialed number into the address of the terminating MTA (MTA_T) and exchanges NCS signaling with MTA_T to create a (media) connection for the terminating endpoint. As part of the task of creating the connection, MTA_T selects the encoding and bandwidth requirements for the media streams and returns to CMS_T a session description containing a subset of the capabilities that were present in the NCS Create Connection request that are acceptable to MTA_T. CMS_T sends a GATE-SET message to the terminating CMTS (CMTS_T); this GATE-SET message conveys policy instructions allowing CMTS_T to create a gate for the IP flow associated with this phone call subsequent to the admission control that is performed following a resource reservation request. CMS_T may send information in the GATE-SET message to notify CMTS_T of billing-related information such as the IP address of the terminating RKS, the Billing Correlation ID (BCID) (see [3] for details) of the terminating event message stream, etc. (see [4] for further details). CMS_T then sends the (2) 183- Session-Progress response back to CMS_O via the proxy. Included in the 183-Session-Progress response is the SDP from MTA_T, with an indication added by CMS_T that the terminating side agrees to meet the preconditions specified in the INVITE before alerting the user. CMS_O then sends a GATE-SET message to the originating CMTS (CMTS_O) to indicate that it can admit a gate for the IP flow associated with the phone call. CMS_O then sends an NCS ModifyConnection request to MTA_O, enabling MTA_O to start reserving resources.

The initial INVITE request and the 183-Session-Progress response contain a SIP Contact header to indicate the IP address of the remote CMS to be used for subsequent end-to-end SIP signaling exchanges as well as the BCID and the Financial Entity ID (FEID) of the CMS sending the message. CMS_O acknowledges the 183-Session-Progress directly to CMS_T using the (3) Provisional Reliable Ack (PRACK) message. The terminating CMS_T acknowledges the PRACK message with the (4) 200-OK message. At this point, resource reservation has not yet completed, and thus the preconditions have not yet been met. CMS_T now issues a modify connection command to MTA_T instructing it to reserve network resources.

Once MTA_O has successfully completed its resource reservation thereby meeting its precondition, it sends an NCS signaling message to CMS_O which in turn sends the (5) UPDATE message directly to CMS_T. CMS_T acknowledges the UPDATE with the (6) 200-OK. When MTA_T has reserved its resources it exchanges NCS signaling with CMS_T. At this point in time, all preconditions have been met, and CMS_T can exchange NCS signaling with MTA_T instructing it to alert the user (ring the destination telephone). CMS_T then sends the (7) 180-Ringing message to CMS_O via the proxy indicating that the terminating phone is ringing, and that the calling party should be given a ringback call progress tone. CMS_O exchanges NCS signaling with MTA_O instructing it to provide ringback, and CMS_O sends another (8) Provisional ACK (PRACK) directly to CMS_T to acknowledge receipt of the (7) 180-Ringing message.

The terminating CMS_T acknowledges the PRACK with a (9) 200-OK. When the called party answers, by going off-hook, MTA_T exchanges NCS signaling with CMS_T to notify the off-hook and enable a full duplex connection. CMS_T also sends a (10) 200-OK final response to the (1) INVITE to CMS_O via the proxy. CMS_O acknowledges the 200-OK directly with the (11) ACK and exchanges NCS signaling with MTA_O instructing it to stop local ringback and enable a full duplex connection. At this point the resources that were previously reserved are committed, and the call is “cut through”

Either party can terminate the call. When CMS_O receives an on-hook notification from MTA_O, CMS_O sends a (12) BYE message directly to CMS_T, which is acknowledged with (13) 200-OK. Each CMS exchanges NCS signaling with its MTA to delete the connection and release the resources reserved.

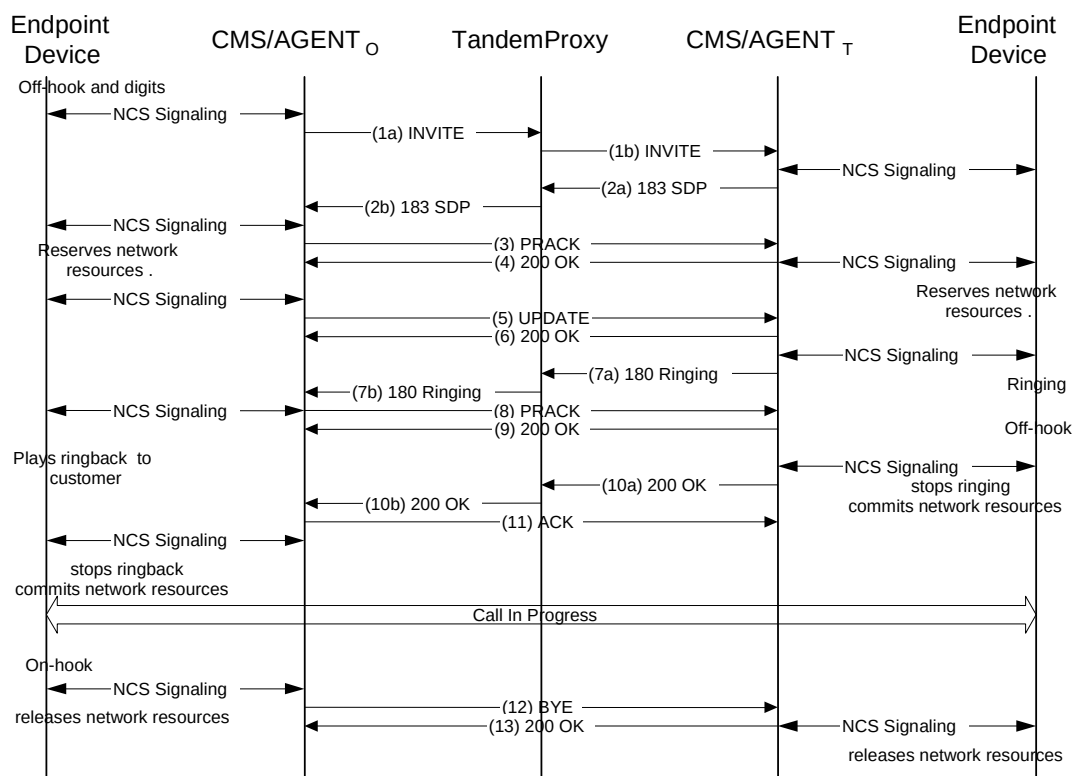


Figure 4: CMS – CMS Signaling Basic Call Flow

5.7 CMS-MGC Basic Telephony Call Flow

This section presents a high level overview of a basic call that uses the CMSS protocol between a CMS and an MGC to make an on-net to off-net call. The procedure shown follows the SIP to ISUP mapping recommendations provided in [37]. Note that CMSS in general is intended to be compatible with the interworking recommendations provided in [37].

The following procedure may be used to make a basic on-net to off-net call using CMSS as the protocol between a CMS and a MGC.

1. The subscriber goes off hook.
2. The MTA exchanges NCS signaling message with the CMS to notify the CMS that the subscriber went off hook.
3. The CMS instructs the MTA to start sending dial tone to the user by exchanging NCS signaling messages with the MTA.
4. The subscriber dials a valid telephone number.
5. The MTA collects the dialed digits and exchanges NCS messages with the CMS to notify the CMS of the dialed digits.
6. The CMS exchanges NCS messages with the MTA to create a (media) connection. As a result of creating the connection, the MTA returns a session description using the Session Description Protocol (SDP).
7. The CMS sends the MGC a (1) INVITE message containing the SDP.
8. The MGC exchanges TGCP signaling messages with the MG to create a (media) connection. During this exchange, session description information is also exchanged.
9. The MGC then sends a (2) 183-Session-Progress response back to the CMS with the SDP from the MG.
10. The CMS exchanges DQoS messages with the CMTS and NCS messages with the MTA so that the MTA will start reserving resources.
11. The CMS acknowledges the 183-Session-Progress using the (3) Provisional Reliable Ack (PRACK) message.
12. The MGC acknowledges the PRACK message with a (4) 200-OK message.

13. Once the MTA has successfully completed its resource reservation, the MTA exchanges NCS signaling messages with the CMS.
14. The CMS sends the (5) UPDATE message to the MGC.
15. The MGC sends an IAM message to the SG.
16. The MGC acknowledges the UPDATE message with a (6) 200-OK.
17. The MGC receives an ACM message from the SG.
18. If the ACM indicates, that the called party is being alerted, the MGC sends a (7) 180-Ringing message to the CMS. If the ACM instead indicated progress or in-band information available, the MGC would have sent a 183-Session-Progress instead (see [37] for details). In this latter case, the MGC would also exchange TGCP signaling with the MG instructing the MG to send packets to the MTA so in-band media provided by the PSTN can be heard by the subscriber.
19. The CMS exchanges NCS signaling with the MTA instructing it to play ringback to the subscriber.
20. The CMS sends another (8) Provisional ACK (PRACK) to the MGC to acknowledge the receipt of the 18x message.
21. The MGC acknowledges the PRACK with a (9) 200-OK.
22. The MGC receives an ANM message from the SG.
23. The MGC exchanges TGCP signaling with the MG instructing it to enable a full duplex connection.
24. The MGC sends a (10) 200-OK final response to the initial INVITE from the CMS.
25. The CMS exchanges NCS signaling with the MTA instructing it to enable a full duplex connection.
26. The CMS acknowledges the 200-OK with an (11) ACK message, the call is “cut through”.
27. The subscriber goes on hook.
28. The MTA exchanges NCS signaling with the CMS to notify the CMS of the on hook condition.
29. The CMS exchanges NCS signaling with the MTA instructing it to delete the connection and release resources.
30. The CMS sends the MGC a (12) BYE message.
31. The MGC sends the CMS a (13) 200-OK to acknowledge the BYE message.
32. The MGC sends a REL message to the SG.
33. The SG sends a RLC message to the MGC.
34. The MGC exchanges TGCP messages with the MG instructing the MG to delete the connection.

Figure 5 shows a basic on-net to off-net call flow, using CMSS as the protocol between the CMS and the MGC.

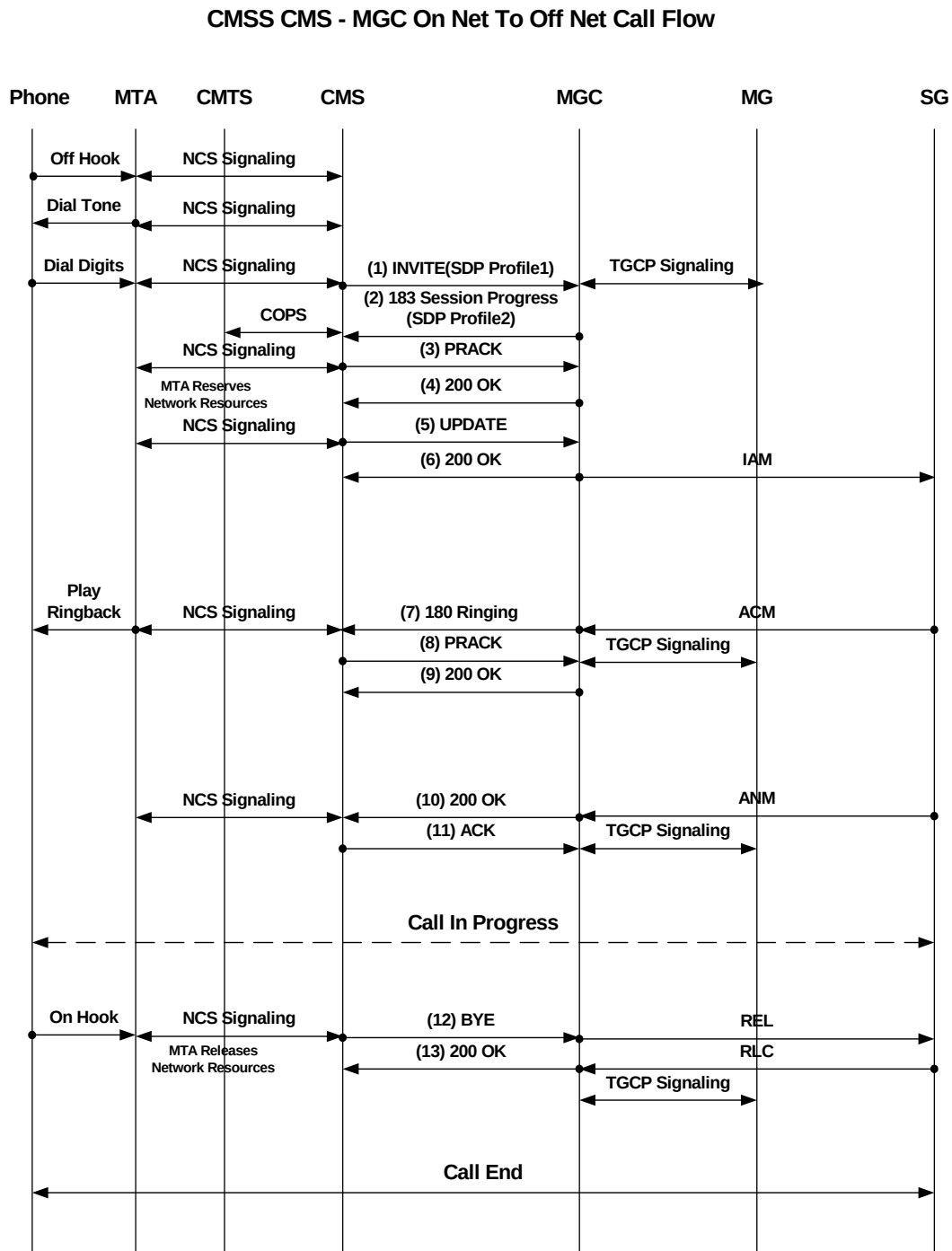


Figure 5: CMS to MGC Signaling

6 SIP PROFILE

This section defines a SIP [8] profile for usage in CMSS compliant systems. This section is structured to mirror the SIP document and its section numbering. The subsections of this section are numbered such that the second digit tracks the SIP section numbers of the SIP specification [8], and section titles at all header levels track the section titles of the SIP specification [8].

This section and section 7 define the nearly complete set of enhancements and restrictions to a standard SIP implementation based on [8]. However, not all details of the required behavior can be captured in these sections. Later sections provide details needed for certification and interoperability testing, which are generally not present in [8]. Sections 6 through 9 are considered normative. Informative call flow examples for the use of CMSS are provided in [28].

Unless otherwise stated in this document, a CMS MUST follow the requirements given for SIP user agents in [8] and a proxy MUST follow the requirements given for SIP proxies and redirect servers in [8].

6.1 Introduction

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 1.

Since there are no requirements in SIP/2.0 [8] section 1, CMSS implementations are automatically compliant with it.

6.2 Overview of SIP Functionality

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 2.

Since there are no requirements in SIP/2.0 [8] section 2, CMSS implementations are automatically compliant with it.

6.3 Terminology

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 3.

Since there are no requirements in SIP/2.0 [8] section 3, CMSS implementations are automatically compliant with it.

6.4 Overview of Operation

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 4.

Since there are no requirements in SIP/2.0 [8] section 4, CMSS implementations are automatically compliant with it.

6.5 Structure of the Protocol

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 5.

Since there are no requirements in SIP/2.0 [8] section 5, CMSS implementations are automatically compliant with it.

6.6 Definitions

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 6.

The reader should note that the term “client” in this section covers both UAs and proxies.

Since there are no requirements in SIP/2.0 [8] section 6, CMSS implementations are automatically compliant with it.

6.7 SIP Messages

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7, except as noted below.

6.7.1 Requests

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.1, except as defined in this section.

The INVITE, ACK, CANCEL, BYE, and OPTIONS methods MUST be supported. The REGISTER method MAY be supported.

The Request-URI MUST be a SIP URI, as defined in [8], or a tel URI as defined in Section 7.1. The SIPS URI format MAY be supported.

The Request-URI in an initial INVITE for a basic telephone call⁶ MUST identify the called party using a tel URI or by using the telephone-subscriber syntax (*i.e.*, the dialed phone number) in a SIP URI. Refer to Section 8.3 for details on forming the associated Request-URI. When with the Request-URI is a SIP URI, the host part MUST identify the CMS or entity to which the message is addressed.

The Request-URI for other requests associated with a basic telephone call MUST identify the targeted host using IPv4address or FQDN syntax, as given by the Contact header.

The host part of the Request-URI typically agrees with one of the host names of the receiving server. However, if the Request-URI of a received INVITE does not so agree, the server SHOULD proxy the request to another entity based on saved translation information or pre-provisioned policy information.

6.7.2 Responses

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.2.

6.7.3 Header Fields

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.3 and its subsections.

Furthermore, CMSS compliant applications MUST be able to both generate and accept short and long form header field names as defined in [8] section 7.3.3.

6.7.4 Bodies

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.4 and its subsections except as defined in this section.

6.7.4.1 Message Body Types

CMSS compliant applications MUST support the message body type "application/sdp".

The message body type "application/sdp" MUST be supported with the INVITE, UPDATE, and PRACK methods as well as any non-failure response to these methods.

Refer to Appendix II for a complete list of supported values.

6.7.4.2 Message Body Length

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.4.2.

6.7.5 Framing SIP Messages

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 7.5.

6.8 General User Agent Behavior

Behavior of CMSS User Agents (UA) MUST be in accordance with chapter 8 of this document and with [8] except as noted in this section.

Note that the behavior defined in this section applies only to requests and responses outside of a dialog. Behavior within a dialog is defined in 6.12.

6.8.1 UAC Behavior

Support for the REGISTER method and SIPS URIs is OPTIONAL, however if supported, it MUST be as specified in [8] section 8.1.

Support for multiple simultaneous media streams for a single call is OPTIONAL for an MTA. Consequently, UACs MUST NOT accept multiple dialogs for a given request, if such dialogs result in the establishment of multiple

⁶ This includes INVITEs generated as a result of forwarding.

simultaneous media streams, unless the MTA for which the dialog is being established supports multiple simultaneous media streams.

6.8.1.1 Generating the Request

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 8.1.1, except as noted below.

Request-URI in the request contains the address of the callee. This will normally be a telephone-number, but it may also be a general SIP-URI⁷. The From and To fields in the request might contain random strings that protect the Privacy of the session originator.

Refer to section 6.20 for further details of various header field values to be used.

The IETF allows option tags to be defined for their purpose only in standard-track RFCs. In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

6.8.1.2 Sending the Request

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 8.1.2 and its subsections.

6.8.1.3 Processing Responses

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 8.1.3 except as noted in this section.

When receiving a 401 (Unauthorized) or 407 (Proxy Authentication Required) response, it is OPTIONAL to follow the SIP authorization procedures.

When receiving a 420 (Bad Extension) response, it is OPTIONAL to follow the SIP retry procedures.

6.8.2 UAS Behavior

The CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 8.2 and its subsections.

6.8.3 Redirect Servers

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 8.3.

6.9 Canceling a Request

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 9 and its subsections.

6.10 Registrations

Proxies MUST, and UACs MAY, support the SIP REGISTER method in accordance with [8] section 10. Support for registrars is OPTIONAL; however if supported, it MUST be as specified in [8] Section 10.

6.11 Querying for Capabilities

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 11 and its subsections.

6.12 Dialogs

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 12 and its subsections, except as noted in the following subsections.

6.12.1 Creation of a Dialog

Support for SIPS URIs is OPTIONAL; however if supported, it MUST be as specified in [8] section 12.1 and its subsections. The IPCablecom security requirements [2] MUST still be honored⁸.

⁷ This can, for example, be used when forwarding to a an Interactive Voice Response (IVR) system.

6.12.2 Requests within a Dialog

Support for SIPS URIs is OPTIONAL, however if supported, it MUST be as specified in [8] section 12.2 and its subsections. The IPsec security requirements [2] MUST still be honored⁹.

6.12.3 Termination of a Dialog

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 12.3.

6.13 Initiating a Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 13 and its subsections, except as noted in this section.

The UAC MUST include a message body of type "application/sdp" with the initial INVITE.

To support codec selection, an SDP session description MUST be included in:

- the initial INVITE request (offer); and
- the first reliable non-failure response to the INVITE (e.g., 183-Session-Progress sent reliably).

6.14 Modifying an Existing Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 14 and its subsections, except as noted in this section.

If a re-INVITE is sent, it MUST include a message body of type "application/sdp" with a new offer. Furthermore, CMSS compliant applications MUST support the procedures for modifying an existing session described in Section 8.4.4.

6.15 Terminating a Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 15 and its subsections.

6.16 Proxy Behavior

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 16 and its subsections, except as noted in this section.

Support for multiple simultaneous media streams for a single call is OPTIONAL for an MTA. Since parallel forking may result in multiple simultaneous media streams for a single call, CMSS compliant implementations SHOULD NOT use parallel forking.

6.17 Transactions

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 17 and its subsections except as noted in this section.

Behavior of CMSS servers (proxies) MUST be in accordance with section 8 of this document, which takes precedence over [8] section 17 in case of any conflicts.

CMSS compliant User Agent Servers MAY return an error code 486 (Busy Here) to an INVITE request for a user if a dialog already exists for that user and the new INVITE is not part of that dialog.

6.18 Transport

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 18 and its subsections.

⁸ Thus, if IPsec is required by the PacketCable Security architecture, use of SIPS URIs will lead to using TLS over IPsec.

⁹ Thus, if IPsec is required by the PacketCable Security architecture, use of SIPS URIs will lead to using TLS over IPsec.

6.19 Common Message Components

6.19.1 SIP and SIPS URI Component

The definition of a SIP/SIPS-URI is as given in [8] section 19.1.1 and extended in Section 7.1.1 in this document.

6.20 Header Fields

CMSS compliant applications MUST be in accordance with SIP/2.0 [8] section 20 and its subsections, except as defined in this section.

In addition to the extensions listed in section 7, the following SIP headers MUST be supported by CMSS compliant applications.

- 1) Accept
- 2) Accept-Encoding
- 3) Accept-Language
- 4) Allow
- 5) Call-ID
- 6) Contact
- 7) Content-Disposition
- 8) Content-Encoding
- 9) Content-Length
- 10) Content-Type
- 11) CSeq
- 12) From
- 13) Max-Forwards
- 14) MIME-Version
- 15) Proxy-Require
- 16) Record-Route
- 17) Require
- 18) Route
- 19) Supported
- 20) Timestamp
- 21) To
- 22) Unsupported
- 23) Via

Other SIP headers MAY be supported by CMSS compliant applications. CMSS compliant applications SHOULD ignore unsupported optional headers.

Listed below is each SIP header defined in [8], and the requirements for supporting each in CMSS are identified.

6.20.1 Accept

The Accept header MUST be supported as specified in [8] section 20.1.

6.20.2 Accept-Encoding

The Accept-Encoding header MUST be supported as specified in [8] section 20.2, except as noted below.

The Accept-Encoding header MAY be used by CMSS compliant implementations. The "identity" encoding value MUST be supported; other encodings MAY be supported.

6.20.3 Accept-Language

The Accept-Language header MUST be supported as specified in [8] section 20.3, except as noted below.

The “Accept-Language” header SHOULD be present in requests with a value of “en” for English, which MUST be supported. Other values MAY be supported.

6.20.4 Alert-Info

Support for the Alert-Info header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.4.

It is noted that there are security risks associated with acting on the Alert-Info header as described in [8] section 20.4.

6.20.5 Allow

The Allow header field MUST be supported as specified in [8] section 20.5. The “Allow” header MUST be present in the initial INVITE and the 200-OK response to the initial INVITE.

Refer to Appendix II for a list of supported methods.

6.20.6 Authentication-Info

Support for the Authentication-Info is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.6.

See also Section 6.22.

6.20.7 Authorization

Support for the Authorization header field is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.7.

See also Section 6.22.

6.20.8 Call-ID

The Call-ID header MUST be supported as specified in [8] section 20.8, except as noted below.

CMSS restricts contents of the Call-ID header in order to support user Privacy.

When Privacy is requested by the session originator, the Call-ID MUST NOT contain the “@” sign and hence consists of a single “word” as defined in [8] section 25.1. The “word” MUST be a random identifier, and MUST be unique across all possible UAs with probability of greater than 0.999999. A suggested implementation is a text encoding (which does not contain an “@”) of a cryptographic hash of phone number, time, a random number, and a quantity provisioned or manufactured to be unique across UAs of otherwise identical manufacture. The last quantity is suggested to help prevent UAs of an otherwise identical manufacture from producing identical “random” Call-IDs when presented with identical stimuli.

6.20.9 Call-Info

Support for the Call-Info header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.9.

It is noted that there are security risks associated with acting on the Call-Info header as described in [8] section 20.9.

6.20.10 Contact

The Contact header MUST be supported as specified in [8] section 20.10, except as noted below.

CMSS compliant applications MUST populate the Contact header field in an INVITE request, and in a 2xx response to an INVITE request, with a SIP-URI. Support for any other type of URI is OPTIONAL.

When the user is requesting Privacy, the Contact header field SHOULD NOT contain any domain names; the IP address form SHOULD be used instead. It should be noted that, in systems with multiple network interfaces, use of the (single)

IP address form can reduce the overall system reliability. If multiple interfaces exist and reliability is a concern, it is considered a reasonable trade-off to refrain from using the IP address form.

CMSS compliant applications **MUST** populate the Contact header field in a 3xx response to an INVITE request with a valid SIP-URI or tel-URI. If the new destination is a telephone number, it **MUST** contain a tel URI with the number of the new destination as described in section 7.1. Support for any other type of URI is **OPTIONAL**.

6.20.11 Content-Disposition

The Content-Disposition header **MUST** be supported as specified in [8] section 20.11, except as noted below.

The Content-Disposition header **MAY** be used by CMSS compliant implementations. The value "session" **MUST** be supported; other values **MAY** be supported.

Note that the default value for message bodies of type "application/sdp" is "session", whereas the default value for all other message body types (*e.g.*, "message/sipfrag") is "render". If the default value is not desired, then the Content-Disposition header **MUST** be included.

6.20.12 Content-Encoding

The Content-Encoding header **MUST** be supported as specified in [8] section 20.12, except as noted below.

The Content-Encoding header **MAY** be used by CMSS compliant implementations. The "identity" encoding value **MUST** be supported; other encodings **MAY** be supported.

6.20.13 Content-Language

Support for the Content-Language header is **OPTIONAL**, however if supported, it **MUST** be as specified in [8] section 20.13.

6.20.14 Content-Length

This header **MUST** be supported as specified in [8] section 20.14.

6.20.15 Content-Type

The "Content-Type" header **MUST** be supported as specified in [8] section 20.15.

Refer to Appendix II for a list of supported values.

6.20.16 CSeq

The CSeq header **MUST** be supported as specified in [8] section 20.16.

6.20.17 Date

Support for the Date header is **OPTIONAL**; however, if supported, it **MUST** be as specified in [8] section 20.17.

6.20.18 Error-Info

Support for the Error-Info header is **OPTIONAL**; however, if supported, it **MUST** be as specified in [8] section 20.18.

It is noted that there are security risks associated with acting on the Error-Info header as described in [8] section 20.18.

6.20.19 Expires

Support for the Expires header in the methods and responses defined in [8] is **OPTIONAL**¹⁰; however, if supported, it **MUST** be as specified in [8] section 20.19.

¹⁰ Note that, per Section 7.5, support for the Expires header is required for the SUBSCRIBE method.

6.20.20 From

The From header MUST be supported as specified in [8] section 20.20, except as noted below.

In support of user Privacy, CMSS restricts the allowed contents of the SIP “From” header.

When the session originator requests Privacy, compliant applications MUST generate a From header according to the following rules:

- The display-name MUST be “Anonymous”.
- The addr-spec MUST contain the identifier “anonymous” for userinfo.
- The addr-spec MUST contain the non-identifying hostname “anonymous.invalid”.

6.20.21 In-Reply-To

Support for the In-Reply-To header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.21.

Note that use of this header is subject to security considerations as described in [8] section 20.21.

6.20.22 Max-Forwards

The Max-Forwards header MUST be supported as specified in [8] section 20.22, except as noted below.

When a CMSS compliant implementation of a back-to-back User Agent (B2BUA) forwards a request, it MUST use a Max-Forwards value equal to the incoming Max-Forwards value minus one.

6.20.23 Min-Expires

Support for the Min-Expires header is OPTIONAL (since support for the REGISTER method is optional); however, if supported, it MUST be as specified in [8] section 20.23.

6.20.24 MIME-Version

The MIME-Version header MUST be supported as specified in [8] section 20.24, except as noted below.

The MIME-Version header MAY be used by CMSS compliant implementations. The version "1.0" value MUST be supported; other values MAY be supported.

6.20.25 Organization

Support for the Organization header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.25.

6.20.26 Priority

Support for the Priority header is OPTIONAL; however if supported, it MUST be as specified in [8] section 20.26.

There are security ramifications for entities that act on this header.

6.20.27 Proxy-Authenticate

Support for the Proxy-Authenticate header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.27.

See also Section 6.22.

6.20.28 Proxy-Authorization

Support for the Proxy-Authorization header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.28.

See also Section 6.22.

6.20.29 Proxy-Require

The Proxy-Require header MUST be supported as specified in [8] section 20.29, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix II for a list of supported values.

6.20.30 Record-Route

The Record-Route header MUST be supported as specified in [8] section 20.30.

6.20.31 Reply-To

Support for the Reply-To header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.31.

6.20.32 Require

The "Require" header MUST be supported as specified in [8] section 20.32, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix II for a list of supported values.

6.20.33 Retry-After

Support for the Retry-After header is OPTIONAL; however, if supported, it MUST be as specified in [8] section 20.33.

6.20.34 Route

The Route header MUST be supported as specified in [8] section 20.34.

6.20.35 Server

Support for the Server header is OPTIONAL; however, if supported, it MUST be as specified [8] section 20.35.

6.20.36 Subject

Support for the Subject header is OPTIONAL, however if supported, it MUST be as specified [8] section 20.36.

6.20.37 Supported

The "Supported" header MUST be supported as specified in [8] section 20.37, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix II for a list of supported values.

6.20.38 Timestamp

The Timestamp header MUST be supported as specified in [8] section 20.38, except as noted below.

CMSS compliant implementations MAY send the Timestamp header in requests; if received, this header MUST be processed as described in [8] section 20.38.

6.20.39 To

The To header MUST be supported as specified in [8] section 20.39, except as noted below.

In support of user Privacy, CMSS restricts the allowable contents of the SIP “To” header. Typically, the “To” header indicates the dialed digits in a tel-URI (see section 7.1). This information is of end-to-end significance, and might reveal information about the caller’s location, *e.g.*, local, long-distance, PBX, or international.

When the call originator requests Privacy, CMSS compliant applications **MUST** generate a “To” header according to the following rules:

The display-name **MUST** be absent.

If a global telephone number is used, then the userinfo part of the addr-spec **MUST** contain a full E.164 number, including the country code.

The host part of the addr-spec **MUST** contain the non-identifying hostname “anonymous.invalid”.

If anonymity is not requested by the call originator and the user dialed a telephone number, then the To: header **SHOULD** contain a tel-URI with the dialed digits.

6.20.40 Unsupported

The Unsupported header **MUST** be supported as specified in [8] section 20.40.

6.20.41 User-Agent

Support for the User-Agent header is **OPTIONAL**; however, if supported, it **MUST** be as specified [8] section 20.41.

6.20.42 Via

The Via header **MUST** be supported as specified in [8] section 20.42, except as noted below.

When the user is requesting Privacy, the Via header field **SHOULD NOT** contain any domain names; the IP address form **SHOULD** be used instead. Support for IP address Privacy is described in more detail in Section 8.4.1.1.3. It should be noted that, in systems with multiple network interfaces, use of the (single) IP address form can reduce the overall system reliability. If multiple interfaces exists and reliability is a concern, it is considered a reasonable trade-off to refrain from using the IP address form.

A border proxy (EBP) which is passing a request outside of the trusted domain of the service provider **MAY** encrypt all “Via” headers except the topmost header (*i.e.*, the “Via” header of the terminating proxy) to a non-recognizable string. The proxy **MAY** include the encrypted string in the Via header, or it may cache the encrypted “Via” headers and include a local token string in the Via header.

6.20.43 Warning

Support for the Warning header is **OPTIONAL**; however, if supported, it **MUST** be as specified in [8] section 20.43.

6.20.44 WWW-Authenticate

Support for the WWW-Authenticate header is **OPTIONAL**; however, if supported, it **MUST** be as specified in [8] section 20.44.

See also Section 6.22.

6.21 Response Codes.

CMSS compliant applications **MUST** be in accordance with SIP/2.0 [8] section 21 and its subsections, except as specified below.

CMSS compliant applications **MUST NOT** issue a 401 or a 407 response; however, they **MUST** process any such received responses in accordance with section 6.8.1.2.

6.22 Usage of HTTP Authentication

Support of HTTP Authentication is **OPTIONAL**; however, if used, it **MUST** be as specified in [2] and [8] section 22. Where these documents conflict, [2] takes precedence.

See also Section 6.21.

6.23 S/MIME

Support of S/MIME is OPTIONAL; however, if used, it MUST be as specified in [2] and [8] section 23. Where these documents conflict, [2] takes precedence.

6.24 Examples

The examples provided in [8] Section 24 do not apply to CMSS compliant implementations. For equivalent examples, refer to Section 8 in this document.

6.25 Augmented BNF for the SIP Protocol

CMSS compliant applications MUST comply with SIP/2.0 [8] section 25.

6.26 Security Considerations: Threat Model and Security Usage Recommendations

CMSS compliant applications MUST comply with the IP-Cablecom Security specification [2].

Support for the SIP Security Considerations specified in [8] section 26 is considered OPTIONAL, unless they conflict with the IP-Cablecom Security specification [2], in which case they MUST NOT be used.

Note:

The IP-Cablecom Security specification may evolve to meet new architecture and security requirements and thus, may be subject for according changes. Therefore, it is not ruled out that consideration of further (SIP) security measures other than or in addition to the ones like IPSec currently specified in the IP-Cablecom Security specification might be considered in the future.

6.27 Table of Timer Values

CMSS compliant applications MUST comply with SIP/2.0 [8] Appendix A.

CMSS compliant applications MUST also support the timer values defined in Appendix I according to the procedures specified in 8.4.

7 SIP EXTENSIONS

SIP [8] has a flexible mechanism for adding extensions and new fields to the protocol for support of additional capabilities. This section defines a set of SIP extensions that enables IP-Cablecom CMSS-compliant systems to provide a robust multimedia service platform supporting basic telephony, CLASS, and custom calling features, while at the same time allowing the supported services to evolve to a multimedia environment. Many of the extensions have been documented in RFCs, to which this document provides cross-references. Several of these extensions have their base in the Distributed Call Signaling (DCS) framework, as described in [32].

This section describes procedures applicable to both NCS and SIP based endpoints; however, it should be noted that SIP based MTAs are out of scope of IP-Cablecom 1.2 and are described and listed in this section for reference purposes only. The term SIP User Agent (UA) in this section refers to an originator/terminator of SIP requests. The combination of a UA with its SIP Proxy is in many ways equivalent to a CMS; likewise a CMS may be decomposed into a UA and a SIP Proxy (with a hidden and untestable interface between them) as shown in Figure 3.

This section follows the naming convention of SIP [8], of User Agents, Clients, Servers, and Proxies. User Agent Clients initiate requests and in particular initiate sessions (*i.e.*, they are call originators), and User Agent Servers respond to requests and in particular accept session requests (*i.e.*, they are call terminators). A User Agent performs either role as required within the context of the call. The description of each extension in this section gives the specific procedures for CMSes and Proxies.

This specification extends SIP in several ways, which are summarized here. All these extensions MUST be supported:

- CMSS supports a resource reservation scheme in which network resources are reserved prior to alerting the user. This is done through specification of preconditions that must be met prior to continuing the session

establishment. Confirmation that the preconditions are met is indicated by an additional end-to-end message exchange (UPDATE/200-OK), which is nested within the normal INVITE/200-OK/ACK message exchange. This extension allows network resources to be reserved prior to alerting the user and also allows network resources to be committed after the user has accepted the invitation, *i.e.*, answered the call. This extension is described further in [14].

- CMSS supports Privacy extensions to SIP. These extensions enable users to make connections without identifying themselves or revealing location information. When Privacy is not requested by the originator, calling number delivery and calling name delivery is provided to the destination (*i.e.*, Caller-ID service) in a reliable manner. Entity identity is also provided to support regulatory features such as Customer Originated Trace, enabling a destination party to report a harassing session even if the originator requested anonymity. This extension is further described in [16] and [17].
- CMSS supports the DCS proxy-to-proxy extensions to SIP that allow proxies to pass additional information between them to perform service-provider functions such as accounting, authorization, billing, coordination of resources, electronic surveillance, etc. This extension is further described in RFC 3603 [26].
- CMSS supports the ability to send a reliable provisional response to a SIP request, ensuring the delivery of the provisional response to the initiating UA, with retransmissions as needed. This extension is further described in [15].
- CMSS supports the ability to send a request to another user agent to instruct that other user agent to initiate a new INVITE. Three extensions are defined for this, as described in RFC 3515 [27], [18] and Appendix III.
- CMSS supports the ability to send a request to another user agent to update that user agent with parameters of the session that do not impact the state of the session (*e.g.*, media parameters). This extension is further described in [19].

The remainder of this section defines further extensions to SIP required by a CMSS compliant application.

This section, and section 6, define the nearly complete set of enhancements and requirements to a standard SIP implementation based on [8]. However, not all details of the required behavior can be captured in these sections. Later sections provide details needed for certification and interoperability testing. Sections 6 through 9 of this document are normative.

7.1 URIs for Telephone Calls

CMSS compliant implementations MUST support URIs for telephone calls except as noted in this section.

The SIP URI can already contain a user part which reproduces the syntax of the tel URI [33] with characters other than those in the "unreserved" and "user-unreserved" sets escaped (see [8], Section 25.1). Such a user part is indicated by also including the "user=phone" parameter. CMSS defines extensions to the SIP URI to enable the use of telephone numbers as defined in [34] and [35]. These extensions relate to number portability and freephone service. At the time of writing, these extensions are works in progress, and hence the relevant parts to which CMSS compliant applications must adhere are included below.

7.1.1 Syntax

The "telephone-subscriber" production in [8] section 25 references the syntax of the tel URI [33]. The syntax is here modified and extended as suggested in [34] and [35]. Furthermore, a dial-around indicator is added to indicate when the user dialed a carrier access code. The resulting grammar is shown below.

The syntax definition follows RFC 2396 [23], indicating the actual characters contained in the URI. Note that the reserved characters "+", ";", "=", and "?" MUST NOT be escaped if shown in the grammar definitions below as they are delimiters for the "tel" URI scheme. These reserved characters MUST be escaped if they appear in parameter values.

Characters other than those in the "reserved" and "unsafe" sets (see [23]) are equivalent to their "% HEX HEX" encoding.

The "tel" URI has the following syntax:

```
telephone-uri    = "tel:" subscriber *param
subscriber      = global-number / local-number
global-number    = global-number-part [isdn-subaddress]
global-number-part = "+" 1*phonedigit
local-number     = local-number-part [isdn-subaddress] [context]
local-number-part = 1*phonedigit
```

```

isdn-subaddress    = ";isub=" 1*uric
context            = ";phone-context=" descriptor *(", " descriptor)
descriptor         = domainname / global-number-part
domainname         = *( domainlabel "." ) toplabel [ "." ]
domainlabel        = alphanum
                   / alphanum *( alphanum / "-" ) alphanum
toplabel           = ALPHA / ALPHA *( alphanum / "-" ) alphanum
param              = ";" (pname ["=" pvalue ] / yu-tel-param)
pname              = 1*uric
pvalue             = *uric
phonedigit         = HEXDIG / visual-separator
visual-separator   = "-" / "." / "(" / ")"
alphanum           = ALPHA / DIGIT

yu-tel-param       = *1(routing-number)
                   *1(npdi-dip-indicator)
                   *1(carrier-id-code)
                   *1(dial-around-indicator)

routing-number     = "rn=" global-rn / local-rn
global-rn          = "+" 1*phonedigit
local-rn           = 1*phonedigit [context]

npdi-dip-indicator = "npdi"
carrier-id-code    = "cic=" global-cic / local-cic
global-cic         = "+" 1*phonedigit
local-cic          = 1*phonedigit [context]
dial-around-indicator = "dai"

```

Production with missing non hash terminals can be found in [8] and RFC-2234 [21].

An example of a SIP URI that includes local-number-portability information is:

```
sip:+1-212-555-1212;rn=+1-212-234-8706;npdi@dcs-proxy;user=phone
```

7.1.1.1 Phone Numbers

The <subscriber> part of the URI indicates the number. The phone number can be represented in either global (E.164) or local notation. All phone numbers MUST use the global form unless they cannot be represented as such. Numbers from private numbering plans, emergency ("911", "112") and some directory assistance numbers (e.g., "411") and other "service codes" (numbers of the form N11 in the United States) cannot be represented in global (E.164) form, and need to be represented as a local number with a context. Local numbers MUST be tagged with a phone-context.

Implementations MUST NOT assume that telephone numbers have a maximum, minimum or fixed length, or that they always begin with a certain number.

7.1.1.1.1 Separators in Phone Numbers

Phone numbers MAY contain visual separators. Visual separators (<visual-separator>) merely aid readability and MUST be ignored by the CMSS compliant implementation.

Even though ITU-T E.123 [9] recommends the use of space characters as visual separators in printed telephone numbers, tel URIs MUST NOT use spaces.

7.1.1.1.2 Alphabetic Characters

In some countries, it is popular to write phone numbers using alphabetic characters which correspond to certain numbers on the telephone keypad. The URI format does not support this notation since the mapping from alphabetic characters to digits is not completely uniform internationally, although there are standards addressing this issue.

Since called and calling terminal numbers (TNs) are encoded in Binary Coded Decimal (BCD) in ISUP, this allows for six additional values per digit, sometimes represented as the hexadecimal characters A through F. However, in accordance with E.164, they may not be included in global numbers. Their use in local numbers is not defined, but is not prohibited.

7.1.1.1.3 Global and Local Numbers

Global (international) numbers are identified by the "+" character prefix. Global numbers MUST be composed with the country (CC) and national (NSN) numbers as specified in E.123 [9] and E.164 [10]. International numbers have the property of being context free everywhere in the world and are RECOMMENDED.

Local numbers only work within a certain geographical area or a certain part of the telephone network, *e.g.*, a private branch exchange (PBX) or a particular country. URIs with local phone numbers should appear only in environments where all local entities can successfully set up the call by passing the number to the dialing software. Digits needed for accessing an outside line, for example, are not included in local numbers.

The phone-context parameter can be used to identify unambiguously the local context where the local number is valid. The parameter value is defined by the "owner" of the local number. The parameter can contain a list of contexts that enumerate all the contexts where this number is valid. It does NOT in any way indicate a prefix that turns the local number into a global (E.164) number. The phone-context provides a unique identifier that lets a client know whether it can interpret the local number. It has no other meaning or function.

There are two ways to label the context: via a global number prefix (*e.g.*, "+33") and via a domain name, *e.g.*, "houston.example.com". The choice between the two is left to the "owner" of the local number and is governed by whether a global number prefix or a domain name is a valid identifier for a particular local number.

The two label types were chosen so that, in almost all cases, a local administrator can pick an identifier that is reasonably descriptive and does not require a new assigned number. It is left to the administrator to assign an appropriate identifier and to use it consistently. In many cases, an organization can choose many different identifiers.

The domain name does not have to resolve to any actual host, but it MUST be under the administrative control of the entity managing the local phone context.

For example, ";phone-context="+1,+49" indicates that the number is valid in country codes 1 (North America) and 49 (Germany). For a local number valid within a PBX, the organization can choose any number under its control to identify the context. For example, a context consisting of any of the organization's global numbers may be suitable, or a substring that is completely occupied by the organization. For example, +49-6151-16 would be a suitable prefix for the TU Darmstadt, as it uses all numbers starting with those digits.

The global number prefix does not imply that adding it to the number will generate a valid E.164 number. It might do this, but this behavior cannot be relied upon. (For example, "911" should be labeled with the context "+1", but "+1-911" is not a valid E.164 number.) As noted earlier, numbers that can be represented as valid E.164 numbers SHOULD NOT be represented as local numbers plus phone-context.

7.1.1.2 ISDN Subaddresses

A phone number MAY also contain an <isdn-subaddress> parameter which indicates an ISDN subaddress. Support for this parameter is mandatory, *i.e.*, a CMSS compliant implementation MUST reject the URI if it cannot interpret ISDN subaddresses. ISDN subaddresses typically contain IA5 characters, but may contain any octet value.

7.1.1.3 Other Parameters

Future extensions to this URI scheme may add other parameters (<param> in the ABNF). Such parameters can be either mandatory or optional. Mandatory parameters are required to start with "m-". An implementation MAY ignore optional parameters. An implementation MUST NOT use the URI if it contains unknown mandatory parameters. The "m-" prefix cannot be added to parameters that were already registered (except to create a new, logically distinct parameter). The "phone-context" parameter in this document is mandatory.

For example, <param> parameters can be used to store application-specific additional data about the phone number, its intended use, or any conversions that have been applied to the number.

All new parameters must be registered with IANA.

7.1.1.4 Routing Number, Number Portability, Carrier Identification Code, and Dial Around Indication

The yu-tel-param parameters are defined as follows:

- The presence of "npdi" indicates that a Number Portability Database (NPDB) dip has been performed. If "npdi" is not present, it indicates that either NPDB dip has not yet been performed or NP is not relevant.

- The first 1, 2 or 3 digits in the "global-cic" identify a country code. The rest of the digits identify a carrier ID code assigned in that country.

The "rn," "npdi," and "cic," if present, can each appear at most once. The "cic," "rn" or "npdi" may be removed when there is no need to carry it further in the call signaling messages. For example, when a freephone call reaches the freephone service provider/carrier serving that freephone number, the "cic" may no longer be needed when the call is to be routed to the called party or another network. Whether and when to remove the new parameters defined in this document are outside the scope of this document.

When the "rn" is present, the "npdi" may or may not be present. This is because the routing number may be present independent of NP. When the "npdi" parameter is not present, it indicates that either NPDB dip has not been performed or NP is not relevant. If a CMSS server is set to perform the NPDB queries, and if a received INVITE message does not contain the "npdi" parameter, the CMSS server will perform the NPDB query. The details of the NPDB query are outside the scope of this document. The routing number received in the response (converted to global-rn or local-rn format) will replace the routing number in the "rn" parameter if present, or will be used by the new "rn" parameter if the "rn" parameter is not present. The "npdi" parameter will be included in this case. The routing number can be a global routing number (*e.g.*, with "+" and the country code plus the national number) or a local (*e.g.*, network-specific) routing number.

Although rare, it is possible to have the "cic," "rn" and POTS number all in the same "tel" URI. When all three are present, the "cic" is used for call routing. When only the "rn" and the POTS number are present, the "rn" is used for making routing decisions (*e.g.*, to check against the routing tables). If the "cic" and "rn" parameters are not present, the telephone number immediately after "tel:" is used for call routing. Note that specific "cic" values can be reserved to indicate call routing information instead of indicating a valid CIC that is assigned to a carrier. For example, a "cic" value of "+1-0110" in a response from the freephone database in the U.S. indicates "local, translated number provided." In this particular case, the "cic" is ignored and the "rn" and the POTS number are used for call routing based on the rules described above.

The CICs in the U.S. are assigned to entities that purchase Feature Group B (FGB) or Feature Group D (FGD) access, FGB translation access, or are Local Exchange Carriers (LECs). CICs are also returned in the response to a freephone query, in which case they identify the freephone service provider that serves the queried freephone number. CICs in the U.S. are currently managed by the North American Numbering Plan Administration (NANPA).

The CIC can be expanded to include VoIP carriers and other types of carriers in the same country or under the same country code so that all carriers can be identified in the IP domain for routing purpose. International service providers and carriers can be identified by the E.164 country codes.

Per the definitions above, the yu-tel-param parameters are defined as optional in the tel-URI sense. However, CMSS compliant applications MUST support the yu-tel-param parameters and hence they MUST NOT be ignored.

CMSS compliant implementations will use the CIC feature to identify not only freephone carriers but also customers' pre-subscribed or dialed carrier access codes as follows:

- If the number dialed is a freephone number, then the CIC MUST identify the carrier serving that freephone number, irrespective of the customers presubscribed or dialed carrier.
- If the number dialed is a not a freephone number, then the CIC MUST identify the pre-subscribed carrier for the caller, unless the caller dialed a carrier access code, in which case that the CIC for that carrier MUST be used. In the latter case, the dial-around indicator MUST be included as well; the dial-around indicator MUST NOT be included in any other case.

7.1.2 Procedures at an Originating CMS

If the Request-URI of an initial INVITE contains a telephone number, a carrier-id-code parameter MUST be included in the telephone-subscriber part with a value corresponding to identity of the carrier preferred by the party paying for the call. Note that, for freephone numbers, this will be the carrier serving the freephone number. If CMS_O provides support for the caller to select a preferred carrier on a per-call basis, the carrier-id-code parameter MUST be included in the telephone-subscriber part and set to the carrier-id-code that the caller has dialed, unless the number dialed is a freephone number. The carrier-id-code MAY furthermore be included in the Refer-To URI of a REFER request, when the party performing the refer is the party paying for the call.

A SIP URI containing "npdi" in the telephone-subscriber part MUST NOT appear other than in an initial INVITE Request-URI or the Refer-To URI of a REFER request sent to a proxy or CMS_T.

An originating CMS that performs the local-number-portability lookup and passes the REFER or initial INVITE request to a proxy or a terminating CMS MUST generate a Request-URI containing a SIP URI with the "npdi" parameter in the