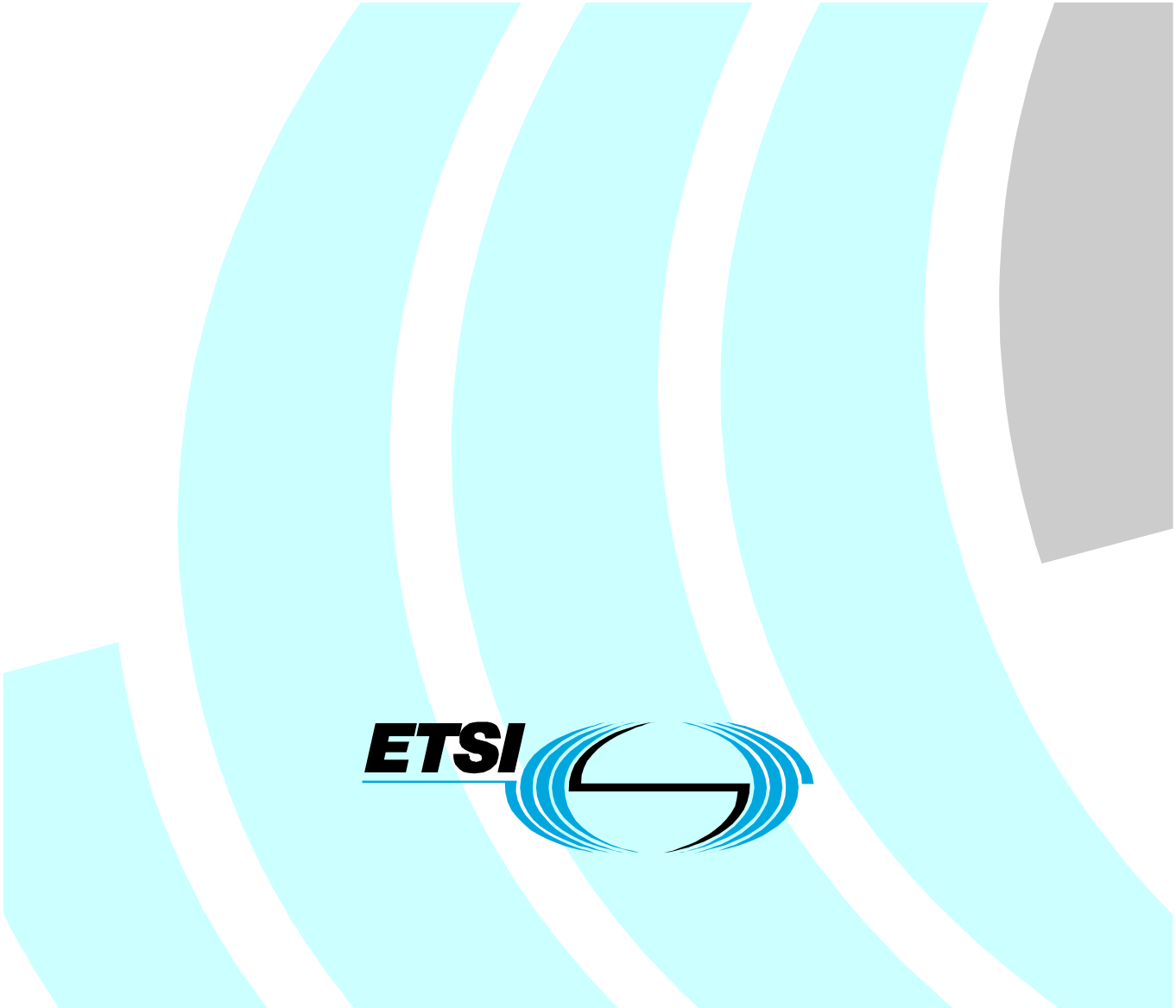
ETSI TS 101 909-16 V1.1.1 (2004-12)

Technical Specification

Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 16: Signalling for Call Management Server

[ITU-T Recommendation J.178 (2003): Pre-Published Version, modified]



Reference
DTS/AT-020020-16

Keywords
endorsement, IPcable, management

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access and Terminals (AT).

The present document is part 16 of a multi-part deliverable covering Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services.

Full details of the entire series can be found in part 1 [39].

The present document is part 16 of the series of ETSI deliverables and specifies the Call Management Server Signalling specification (CMSS). CMSS is a protocol, based upon a profile of the RFC 3261 [8] that is used to communicate between entities within the IPCablecom network implementing SIP User Agent or proxy functionality (e.g. Call Management Servers (CMS), Media Gateway Controllers (MGC), announcement servers, etc.).

Endorsement notice

The elements of ITU-T Recommendation J.178, pre-published version apply, with the following modifications:

Summary

The ITU-T Recommendation J.178 summary does not apply and is replaced by the following text:

The present document defines a profile of the IETF SIP protocol for use within IPCablecom networks. The protocol defined as a result of this profile specification is known as Call Management Server (CMS) to Call Management Server (CMS) signaling protocol (CMSS). The protocol is used within secure domains.

Introduction

ITU-T Recommendation J.178, section 1.1 "Scope", does not apply and is replaced by the following text:

Section 1.1 Scope:

The present document defines a profile of the RFC 3261 [8] for use within secure domains. This SIP profile (known as CMSS - "Call Management Server to Call Management Server Signalling Specification") contains extensions to the SIP protocol and usage rules to support services.

2 References

The references provided in this list of references supercedes those provided in ITU-T Recommendation J.178. In line with the policy implemented in ITU-T Recommendation J.178 regarding references the following text from ITU-T Recommendation J.178 explains the context under which these references are given:

"The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation."

NOTE: When reading ITU-T Recommendation J.178 as part of the present document any reference number read from ITU-T Recommendation J.178 shall refer to a reference in this list of references as opposed to the table of references supplied in ITU-T Recommendation J.178.

[1] ETSI TS 101 909-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems" (ITU-T Recommendation J.160 (02/02)).

[2] ETSI TS 101 909-11: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security" (ITU-T Recommendation J.170 (02/02)).

[3] ETSI TS 101 909-10: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 10: Event Message Requirements for the Provision of Real Time Services over Cable Television Networks using Cable Modems" (ITU-T Recommendation J.164 (03/01)).

[4] ETSI TS 101 909-5: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems" (ITU-T Recommendation J.163 (03/01)).

[5] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol" (ITU-T Recommendation J.162 (03/01)).

[6] ETSI TS 101 909-13 (Sub-part 1: H.248 option and Sub-part 2: MGCP option): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol" (ITU-T Recommendation J.171 (02/02)).

[7] ITU-T Recommendation J.174 (2002): "IPCablecom Interdomain Quality of Service".

[8] IETF RFC 3261 (2002): "SIP: Session Initiation Protocol".

[9] ITU-T Recommendation E.123 (2001): "Notation for national and international telephone numbers, e-mail addresses and Web addresses".

[10] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[11] IETF RFC 2327 (1998): "SDP: Session Description Protocol".

[12] IETF RFC 3551 (2003): "RTP Profile for Audio and Video Conferences with Minimal Control".

[13] IETF RFC 768 (1980): "User Datagram Protocol".

[14] IETF RFC 3312 (2002): "Integration of Resource Management and Session Initiation Protocol (SIP)".

[15] IETF RFC 3262 (2002): "Reliability of Provisional Responses in Session Initiation Protocol (SIP)".

[16] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[17] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[18] IETF RFC 3265 (2002): "Session Initiation Protocol (SIP) - Specific Event Notification".

[19] IETF RFC 3311 (2002): "The Session Initiation Protocol (SIP) UPDATE Method".

[20] IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[21] IETF RFC 2234 (1997): "Augmented BNF for Syntax Specifications: ABNF".

[22] IETF RFC 2397 (1998): "The data URL Scheme".

[23] IETF RFC 2396 (1998): "Uniform Resource Identifiers (URI): Generic Syntax".

[24] Void.

[25] IETF RFC 3420 (2002): "Internet Media Type message/sipfrag".

[26] IETF RFC 3515 (2003): "The Session Initiation Protocol (SIP) Refer Method".

[27] IETF RFC 3603 (2003): "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture".

3 Terms and Definitions

The elements of ITU-T Recommendation J.178 section 3 apply with the following modifications:

~~CNAM – Calling Name~~

gateway: devices bridging between secure domains~~the IPCablecom 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 Signalling Gateway which sends and receives circuit switched network signalling tot he edge of the IPCablecom network.sends and receives circuit switched network signalling tot he edge of the IPCablecom network.~~

~~LNP – Local Number Portability~~

~~**Off-Net Call:** A communication connecting a IPCablecom subscriber out to a user on the PSTN the PSTN~~

~~**On-Net Call:** A communication placed by one customer to another customer entirely on the IPCablecom Network~~

secure domain: within a secure domain CMSS signalling is passed transparently between trusted CMSS capable entities

NOTE: Between secure domains gateways are used to filter or block information per functional, regulatory or legal requirements.

4 Abbreviations and Acronyms

The elements of ITU-T Recommendation J.178 section 4 apply with the following modifications:

This Recommendation defines the following abbreviations and acronyms.

~~BLV Busy Line Verification~~
~~CLASS Custom Local Area Signalling Services~~
~~EI Emergency Interrupt~~
~~MF Multi Frequency~~
~~MG Media Gateway~~
~~MGC Media Gateway Controller~~

Sections 5 to 5.2

Sections 5 to 5.2 are not endorsed and do not apply to the present document.

5.3 CMSS Trust Model

ITU-T Recommendation J.178 section 5.3 "CMSS Trust Model" does not apply and is replaced by the following text:

Within a secure domain CMSS signalling is passed transparently between trusted CMSS capable entities. Between secure domains gateways are used to filter or block information per functional, regulatory or legal requirements.

Sections 5.4 to 5.7

Sections 5.4 to 5.7 are not endorsed and do not apply to the present document.

6 SIP Profile

All elements of ITU-T Recommendation J.178 section 6 (and associated sub-sections) apply with the exception of section 6.20.42 which is replaced as follows:

6.20.42 Via

The Via header MUST be supported as specified in RFC 3261 [8] section 20.42, except as noted below:

~~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.~~

7 SIP Extensions

The elements of ITU-T Recommendation J.178 section 7 apply with the following modifications:

~~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 IPCablecom 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 Signalling (DCS) framework, as described in [30].~~

~~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 IPCablecom 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 RFC 3261~~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 RFC 3312 [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 party, calling number delivery and calling name delivery is not provided to the called party~~destination~~ (*i.e.* Caller-ID restriction service) expect to support regulatory features.~~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 RFC 3323 [16] and RFC 3325 [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 ~~appendix III~~RFC 3603 [27].

- 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 RFC 3262 [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 ~~Appendix IV~~RFC 3515 [26], RFC 3265 [18] and Appendix V.

- 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 RFC 3311 [19].

This section, and section 6, define the nearly complete set of enhancements and requirements to a standard SIP implementation based on RFC 3261 [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.

7.1.2 Procedures at an Originating CMS

The elements of ITU-T Recommendation J.178 section 7.1.2 apply with the addition of the following Note preceding the text:

NOTE: "Originating CMS" in this section may refer to any CMSS capable entity that is originating CMSS signaling.

7.1.3 Procedures at a Terminating CMS

The elements of ITU-T Recommendation J.178 section 7.1.3 apply with the addition of the following note preceding the text:

NOTE: "Terminating CMS" in this section may refer to any CMSS capable entity that is terminating CMSS signaling.

7.1.4 Procedures at Proxy

The elements of ITU-T Recommendation J.178 section 7.1.4 apply with the addition of the following note preceding the text:

NOTE: "Terminating CMS/CMS_T" in this section may refer to any CMSS capable entity that is terminating CMSS signaling.

7.4 Integration of Resource Management and SIP

The elements of ITU-T Recommendation J.178 section 7.4 apply with the following modifications:

CMSS compliant implementations MUST support the extensions defined in RFC 3312 [14] except as noted in the subsections below.

NOTE: "Terminating CMS/CMS_T" in this section may refer to any CMSS capable entity that is terminating CMSS signaling while the term 'Originating CMS/CMS_o' may refer to any CMSS capable entity that is originating CMSS signaling.

7.6 The REFER Method

The elements of ITU-T Recommendation J.178 section 7.6 apply with the following modifications:

NOTE: "Terminating CMS/CMS_T" in this section and associated sub-sections may refer to any CMSS capable entity that is terminating CMSS signaling while the term 'Originating CMS/CMS_o' may refer to any CMSS capable entity that is originating CMSS signaling.

CMSS compliant implementations MUST support the extensions defined in ~~Appendix IV~~RFC 3515 [26]except as noted in this section. Note that this method makes use of the Notify mechanism defined in section 7.5.

7.7 SIP Proxy to Proxy Extensions for Supporting DCS

The elements of ITU-T Recommendation J.178 section 7.7 apply with the following modifications:

CMSS compliant implementations MUST support the extensions defined in ~~Appendix III~~RFC 3603 [27] except as defined in this section.

7.7.2 P-DCS-Gate

The elements of ITU-T Recommendation J.178 section 7.7.2 apply with the following modifications:

The P-DCS-Gate header is not required to be present in the initial INVITE request~~ sent between CMSes~~.

7.9 Private Extensions to the SIP Protocol for Asserted Identity within Trusted Networks

The elements of ITU-T Recommendation J.178 section 7.9 apply with the following modifications:

CMSS compliant implementations MUST support the asserted identity extensions defined in RFC 3325 [17], except as defined in this section. Note that support of the asserted identity extensions not only implies support of the P-Asserted-Identity header, but also implies support of the Privacy header with a value of "id" as described in RFC 3323 [16] and RFC 3325 [17] and a value of "critical" as described in RFC 3323 [16], as well as the Proxy-Require option tag "Privacy".

~~For an on-net originated call, there MUST be a single P-Asserted-Identity header present. For an off-net originated call, there MUST be a single P-Asserted-Identity header present if the calling party number is available; otherwise, the P-Asserted-Identity header MUST NOT be present.~~ The P-Asserted-Identity header if present MUST NOT use a SIPS URI.

The URI MUST contain the number of the calling party as defined in section 7.1, either as a tel-URI or as a SIP-URI with telephone-subscriber syntax and "user=phone". If calling name Privacy is requested, the display-name "Anonymous" MUST be used for this header. If ~~the call is initiated on-net and~~ calling name Privacy was not requested, the display-name MUST be set to the name of the calling party. ~~If the call originated off-net and calling name Privacy was not requested, the display name MAY be omitted.~~ If calling number Privacy is requested, a Privacy header with priv-values "id" and "critical" MUST be included and a Proxy-Require containing the option tag "Privacy" MUST be included, as described in RFC 3323 [16] and RFC 3325 [17].

In order to support the asserted identity extension, a Spec(T) is specified, as described in RFC 3325 [17]. ~~IPCablecom's~~The Spec(T) is defined as follows:

2. Authentication requirements

   ~~For calls that originate on-net,~~ For calls originating within the secure domain the procedure specified in TS 101 909-11 [2] must be followed.

   For calls ~~that~~ originate~~ing~~ outside the secure domain ~~off-net~~, any calling party information present in the signalling received from the originating domain~~PSTN signalling messages~~ MUST be used.~~, unless it is user-provided or the PSTN is not trusted, in which case it MUST NOT be used.~~

3. Security requirements

   Connections between nodes within the Trust Domain and between UAs and nodes in the Trust Domain MUST use secure signalling as described in TS 101 909-11 [2].

4. Scope of Trust Domain

   The CMSS Trust Domain consists of all CMSS hosts that can communicate either directly or indirectly, subject to the security requirements described in TS 101 909-11 [2].

   ~~The CMSS Trust Domain also includes the adjacent PSTN network unless configured otherwise.~~

   ~~MTAs MUST NOT be part of the Trust Domain.~~

   ~~It should be noted that the trust boundary here described for signalling is different from the trust boundary described in section 5.3, which deals with trust for event messages customer premise equipment and third parties.~~

~~Note that since CMSS (and [2] together) define(s) a single Trust Domain where all CMSes trust each other, a P-Asserted-Identity header will currently never be removed before being forwarded to another CMS.~~

8 CMS-CMS SIGNALLING

The elements of ITU-T Recommendation J.178 section 8 apply with the following modifications:

In this chapter, the CMS to CMS signalling that takes place within a secure domain~~between CMSes within a domain, and the signalling that takes place between domains~~ is presented. ~~The primary difference between intra-domain signalling and inter-domain signalling is the use of External Border Proxies, which are described in section 5.4.~~

Sections 8.1 to 8.1.2

Sections 8.1 to 8.1.2 are not endorsed and do not apply in the present document.

8.2 CMS Retransmission, Reliability, and Recovery Strategies

The elements of ITU-T Recommendation J.178 section 8.2 apply with the following modifications:

RFC 3261 [8] defines a retransmission scheme based on two timer values, T1 and T2. The retransmission interval starts at T1 seconds, and is doubled, with each attempt (up to a limit of T2 seconds), up to some maximum number of retransmissions.

When the provisioned number of message retransmissions is exceeded for an INVITE without any response being received, the CMS MUST try a different CMS address, if available. If multiple CMSes are available, the procedures defined in RFC 3263 [20], section 4.3, MUST be used. When a provisioned number (which may be infinite) of CMS addresses have been tried, the CMS MUST clear the call and return to an idle state.

~~The behavior of Tandem Proxies depends on their role in the network and is not further specified in this document. Tandem Proxies follow standard SIP processing/retransmission.~~

8.4 CMS Procedures

The elements of ITU-T Recommendation J.178 section 8.4 apply with the following modifications:

The following subsections contain sample procedures for a basic call from an originating CMS to a terminating CMS both located within a single secure domain, and for various mid-call changes that may be initiated by ~~either~~ endpoints subtended from CMSes within the secure domain. Note that relevant interworking specifications should be consulted for appropriate parameter mappings and any additional behavioural expectations placed on the CMSS capable entites involved in the call as a result of interworking in cases whereby the CMSS session is initiated either as a result of a stimulus on a gateway from outside the secure domain or as a result of a call to an endpoint outside the secure domain.

8.4.1 CMS Messages and Procedures for Basic Call Setup

The elements of ITU-T Recommendation J.178 section 8.4.1 apply with the following modifications:

The basic INVITE message sequence for a CMSS call setup includes the INVITE/183-Session-Progress/18x/200-OK/ACK exchange, an UPDATE/200-OK exchange, and one or two PRACK/200-OK message exchanges. These are ~~shown in figure 4 (section 5.6), and~~ discussed in the following subsections. ~~When it is known that the far-end is being alerted, the 18x will be a 180 Ringing. A 183 Session Progress will be used instead of 180 Ringing when there is call progress but it is not known whether the called party is being alerted[1].~~

The following sections trace a basic call from origination to completion, and give the requirements for each message exchange. It therefore switches viewpoints from origination to termination and back. For procedures followed by CMS_O (*i.e.*, the originating CMSS entity~~a call~~) see sections 8.4.1.1, 8.4.1.3, and 8.4.1.6. For procedures followed by CMS_T (*i.e.*, the terminating CMSS entity~~a call~~) see sections 8.4.1.2, 8.4.1.4, and 8.4.1.5. ~~A typical CMS implements the procedures in all of these subsections, while specialized CMSs implement only the portions needed in their application.~~

The behavior below also shows the procedures for call forwarding (unconditional and busy) and call forwarding (no answer).

~~[1] For example, when interworking with MF trunks, it is not known whether in-band media is ringback or an announcement, and hence a 183-Session-Progress with early media would be used. Please refer to [35] for details.~~

8.4.1.1 CMS_O initiating Invite

The elements of ITU-T Recommendation J.178 section 8.4.1.1 apply with the following modifications:

~~CMS_O becomes aware of a call origination attempt when it receives a Notify message from the MTA. A Media Gateway Controller (MGC) becomes aware of a call origination attempt when it receives a Notify message from the media gateway, or an IP-IAM message from the signalling gateway. A CMS also becomes aware of a call origination attempt when it receives a REFER request from another CMS.~~

CMS_O MUST check that the session originator~~indicated line~~ is authorized for outgoing service to the destination phone number.

8.4.1.1.1 CMS_O Authentication and Authorization of Originator

The elements of ITU-T Recommendation J.178 section 8.4.1.1.1 apply with the following modifications:

~~Two different cases are considered here:~~

- ~~a call originating on-net, and~~
- ~~a call originating off-net.~~

Except as specified below, ~~if the call originates on-net,~~ CMS_O MUST provide a validated originating phone number for the active line on MTA_O in the P-Asserted-Identity header. CMS_O MUST also provide a validated originating calling name for the active line on MTA_O, unless the originator has requested calling name Privacy, in which case the display-name "Anonymous" or a provisioned textual string of equivalent meaning MUST be used. See TS 101 909-11 [2] for further detail.

~~If the call originates off-net and no calling party number is available, then the P-Asserted-Identity header MUST be omitted. Otherwise, the CMS_O MUST provide the calling party number received from the PSTN in the P-Asserted-Identity header. If calling name Privacy is requested, the display-name MUST be set to "Anonymous".~~

8.4.1.1.3 IP Address Privacy Support

The elements of ITU-T Recommendation J.178 section 8.4.1.1.1 apply with the following modifications:

Footnote 15 is modified to read as follows:

15 Note that if the terminating endpoint is an NCS MTA then a trust boundary will be crossed no later than between CMS_T and MTA_T. ~~For a PSTN gateway, a trust boundary may not be crossed.~~

8.4.1.2.1 CMS_T Sending 183-Session-Progress Status Response

The elements of ITU-T Recommendation J.178 section 8.4.1.1.1 apply with the following modifications:

Footnote 16 is modified to read as follows:

16 Note that if the originating endpoint is an NCS MTA then a trust boundary will be crossed no later than between CMS_O and MTA_O. ~~If the originating endpoint is a PSTN gateway, a trust boundary may not be crossed.~~

8.4.1.5 CMS_T sends 180-Ringing or 183-Session-Progress

The elements of ITU-T Recommendation J.178 section 8.4.1.5 apply with the following modifications:

The title of this section is changed to "CMS_T sends 180-Ringing".

The text of this section shall be modified as follows:

~~When the terminating endpoint is on-net,~~ CMS_T determines, by mechanisms beyond the scope of this specification, whether alerting is necessary. If alerting of the destination user is necessary, CMS_T sends a 180-Ringing response. Otherwise, CMS_T sends a final response as described in section 8.4.1.7.

~~When the terminating endpoint is off-net, CMS_T waits for an off-net indication to determine what response to generate, as described in [31]. If the response from the PSTN indicates that alerting is being performed, CMS_T generates a 180-Ringing response. If the response indicated progress or in-band information available, the CMS_T generates a 183-Session Progress instead and ensures that the terminating endpoint can send media to the originating side. A 181 Call is Being Forwarded or 182 Queued could also be generated as described in [31]. In all other cases, CMS_T sends a final response as described in section 8.4.1.7.~~

The 180-Ringing ~~or 183 Session Progress~~ message MUST be formatted as follows:

180 Ringing~~/ 183 Session Progress:~~ (CMS_T -> CMS_O) Header:	**Requirements on CMS_T For Message Generation**
SIP/2.0 180 Ringing~~/183 Session Progress~~	Status line with status code 180 ~~or 183~~ MUST be present.
Via:	As described in section 6.13.
Require:	As defined in section 6.20.32. MUST include "100rel".
From:	As described in section 6.13.
To:	
Call-ID:	
Contact:	As defined in section 6.20.10.
Cseq:	As described in section 6.13.
Rseq:	As defined in section 7.2.
Content-Length:	MUST be present if the transport protocol is stream-based (TCP), as described in section 6.20.14.
	An empty line (CRLF) MUST be present.

After sending the 180-Ringing ~~or 183 Session Progress~~ response to the INVITE, CMS_T MUST wait for the PRACK message acknowledging the response. The PRACK message headers MUST be checked as follows:

PRACK (CMS_O -> CMS_T) Header:	**Requirements On CMS_T for Message Checking**
PRACK URI SIP/2.0	As described in section 7.2.
Via:	As described in section 6.20.42.
Max-Forwards:	As defined in section 6.20.22.
From:	As described in section 6.12.2.
To:	
Call-ID:	
Cseq:	
Rack:	As described in section 7.2.
Content-Length:	MUST be present if the transport protocol is stream-based (*e.g.*, TCP), as described in section 6.20.14.
	An empty line (CRLF) MUST be present.

200-OK (CMS_T -> CMS_O) Header:	**Requirements On CMS_T for Message Generation**
SIP/2.0 200 OK	As described in section 6.12.2.
Via:	
From:	
To:	
Call-ID:	
Cseq:	
Content-Length:	MUST be present if the transport protocol is stream-based (*e.g.* TCP), as described in section 6.20.14.
	An empty line (CRLF) MUST be present.

8.4.2 Initiating an Emergency Call

The elements of ITU-T Recommendation J.178 section 8.4.2 apply with the following modifications:

A call for emergency services, *e.g.*, 112~~9 1 1~~, MUST follow the procedures given for a basic call, as given in section 8.4.1, with the following exceptions.

~~As described in section 7.1, t~~The national emergency services telephone number is not harmonized~~an international number and hence cannot be supplied as a global number~~. Instead, the appropriate national short code for emergency services~~local number form~~ MUST be used and a "phone-context" parameter identifying the geographic location of the originating call MUST be set to the relevant prefix, e.g. "+44~~1~~" MUST be added as illustrated here:

- tel: 112~~911~~;phone-context=+44~~1~~

CMS_O, receiving a 183-Session-Progress response for a n emergency services~~9-1-1~~ call, MUST indicate enhanced priority for access network admission control in the GATE-SET command to the originating CMTS, using the mechanisms described in TS 101 909-5 [4].

An emergency call~~9-1-1~~call SHOULD NOT be put on hold or disconnected due to feature interaction. CMS_O MUST disable all call features on any line that is placing a call to emergency services.

Sections 8.4.4.4 and 8.4.4.5

Sections 8.4.4.4 and 8.4.4.5 are not endorsed and do not apply in the present document.

Appendixes I and II

The present document endorses ITU-T Recommendation J.178 appendixes I and II as normative annexes.

Appendix III Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting DCS

This appendix is not endorsed and is deleted in the present document. Instead the reader is directed to normative reference RFC 3603 [27].

Appendix IV The SIP Refer Method~~ - draft-ietf-sip-refer-06~~

This appendix is not endorsed and is deleted in the present document. Instead the reader is directed to normative reference RFC 3515 [26].

Appendix V The Session Initiation Protocol (SIP) "Replaces" Header

The present document endorses ITU-T Recommendation J.178 appendix V as a normative annex.

Appendix VI Bibliography

The present document endorses ITU-T Recommendation J.178 appendix VI as an informative appendix with the following changes:

[29] ETSI TS101 909-3: Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 3: Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems

[30] ETSI TS101 909-19 (sub-part 1: H.248 option and sub-part 2: MGCP option): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 19: IPCablecom Audio Server Protocol Specification".

~~[29] ITU-T Recommendation J.175 (07/02): "IPCablecom Audio Server Protocol".~~

[38] ETSI TS 101 909-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".~~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~~

[39] ~~PacketCable 1.2 Architecture Framework, PKT-TR-ARCH1.2-V01-001229, December 29, 2000, www.packetcable.com/specifications~~ ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General".

Appendix VII ACKNOWLEDGMENTS

The present document endorses ITU-T Recommendation J.178 appendix VII as an informative appendix.

History

Document history		
V1.1.1	December 2004	Publication