

# ETSI TS 183 043 V1.1.1 (2006-05)

---

*Technical Specification*

## **Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); IMS-based PSTN/ISDN Emulation Stage 3 specification**

---



---

**Reference**

DTS/TISPAN-03044-NGN-R1

---

**Keywords**

IMS, ISDN, PSTN, Stage 3

**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

---

**Important notice**

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Copyright Notification**

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

© European Telecommunications Standards Institute 2006.  
All rights reserved.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup> and **UMTS**<sup>TM</sup> are Trade Marks of ETSI registered for the benefit of its Members.  
**TIPHON**<sup>TM</sup> and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.  
**3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

# Contents

Intellectual Property Rights .....	7
Foreword.....	7
1 Scope .....	8
2 References .....	8
3 Definitions and abbreviations.....	10
3.1 Definitions .....	10
3.2 Abbreviations .....	11
4 IMS-based PSTN Emulation Subsystem (PES) overview .....	12
4.1 General .....	12
4.2 URI and address assignments.....	13
5 Protocol using SIP and SIP events for PES.....	13
5.1 Introduction .....	13
5.2 Functional Entities.....	13
5.2.1 User Equipment (UE) .....	13
5.2.2 Access Gateway Control Function (AGCF) .....	13
5.2.3 Application Server (AS) .....	13
5.2.4 Media Resource Function Controller (MRFC) .....	13
5.2.5 Media Gateway Controller Function (MGCF).....	14
5.2.6 Interconnection border control function (IBCF).....	14
5.3 Role .....	14
5.3.1 PES Endpoint.....	14
5.3.1.1 General .....	14
5.3.1.2 Subscription for dial tone management.....	14
5.3.1.3 Registration procedures.....	14
5.3.2 PES Access Point.....	15
5.3.2.1 General .....	15
5.3.2.2 Subscription for dial tone management.....	15
5.3.2.3 Registration Procedures .....	15
5.3.2.4 Outgoing Call Control procedures .....	16
5.3.2.5 Incoming Call Control procedures .....	16
5.3.3 PES Application Server .....	16
5.3.3.1 General .....	16
5.3.3.2 Basic call procedures.....	16
5.3.3.3 Announcement procedures.....	17
5.3.3.4 Dial Tone Management.....	17
5.3.3.5 Transport of ISUP information .....	17
5.3.3.5.1 General .....	17
5.3.3.5.2 Sending NSS message bodies to a peer SIP signalling entity.....	18
5.3.3.5.3 Receiving an NSS message body from a peer SIP signalling entity.....	20
5.3.3.6 Handling of charging information.....	20
5.3.4 PES Announcement Server.....	20
5.3.4.1 General .....	20
5.3.4.2 Announcement procedures.....	20
5.3.5 PES Interworking Application.....	20
5.3.5.1 General .....	20
5.3.5.2 Routing procedures .....	21
5.3.5.3 Handling of charging information.....	21
5.3.5.4 Transport of ISUP information .....	21
5.3.5.4.1 General .....	21
5.3.5.4.2 Sending ISUP information to a peer SIP signalling entity .....	21
5.3.5.4.3 Receiving an NSS message body from a peer SIP signalling entity.....	23
5.3.5.4.4 ISUP messages for special consideration .....	24
5.3.5.5 Optional SIP/ISUP interworking procedures for PSTN Bridging.....	25

5.3.6	PES interconnection application .....	26
5.3.6.1	General .....	26
5.3.6.2	Procedures related to NSS message bodies .....	26
6	Protocol using SIP/SDP for PES .....	26
6.1	Introduction .....	26
6.2	Functional Entities.....	26
6.2.1	User Equipment (UE) .....	26
6.2.2	Access Gateway Control Function (AGCF) .....	26
6.2.3	Application Server (AS) .....	26
6.2.4	Media Resource Function Controller (MRFC) .....	26
6.3	Roles.....	27
6.3.1	PES Endpoint.....	27
6.3.2	PES Access Point.....	27
6.3.2.1	General .....	27
6.3.2.2	Originating calls .....	27
6.3.2.3	Terminating calls.....	27
6.3.2.4	Modifying SDP within existing dialogues .....	28
6.3.3	PES Application Server .....	28
6.3.3.1	General .....	28
6.3.4	PES Announcement Server.....	28
6.3.4.1	General .....	28
7	Protocol using H.248 for PES .....	28
7.1	Introduction .....	28
7.2	Functional Entities.....	28
7.2.1	Access Gateway Control Function (AGCF) .....	28
7.2.2	Media Gateway Function (MGF).....	28
7.3	Roles.....	29
7.3.1	PES Access Point.....	29
7.3.1.1	General .....	29
7.3.1.2	Registration .....	29
7.3.1.3	Basic Session control procedures for analog lines .....	29
7.3.1.3.1	Originating side procedures.....	29
7.3.1.3.2	Terminating side procedures .....	32
7.3.1.4	Procedures for fax/modems calls over analog access.....	34
7.3.1.5	Message Waiting Indication.....	35
7.3.2	PES Media Gateway .....	35
<b>Annex A (normative):</b>	<b>XML document structure for Dial Tone Management .....</b>	<b>36</b>
<b>Annex B (normative):</b>	<b>AGCF internal communication .....</b>	<b>37</b>
B.1	General .....	37
B.2	Internal communication principles .....	37
B.3	Internal primitives .....	38
B.4	Feature manager behaviour .....	39
B.4.1	Registration procedures .....	39
B.4.1.1	Global registration procedures .....	39
B.4.1.2	Per line registration procedures .....	39
B.4.1.2.1	User-initiated registration.....	39
B.4.1.2.2	User-initiated deregistration .....	39
B.4.1.2.3	Exception procedures .....	40
B.4.2	Call Processing .....	40
B.4.2.1	General procedures .....	40
B.4.2.2	Flash-Hook Management.....	40
B.4.2.2.1	General rules .....	40
B.4.2.2.2	Loose coupling procedures .....	41
B.4.2.2.3	Tight coupling procedures.....	42
<b>Annex C (Informative):</b>	<b>Implementation of Supplementary Services.....</b>	<b>44</b>

C.1	General principles .....	44
C.1.1	Introduction .....	44
C.1.2	Supplementary service control .....	44
C.1.2.1	Service code commands.....	44
C.1.2.1.1	Command syntax.....	44
C.1.2.1.2	Generic procedure at the AGCF side .....	45
C.1.2.1.3	Generic procedure at the AS side.....	45
C.1.2.2	Switching order commands .....	45
C.1.3	Setting of initial filter criteria.....	46
C.1.4	Supplementary services using ISUP information .....	47
C.2	Advice of Charge .....	47
C.2.1	Actions at the Originating AGCF.....	47
C.2.2	Actions at the Originating AS .....	47
C.2.3	Actions at the Terminating AGCF .....	48
C.2.4	Actions at the Terminating AS .....	48
C.3	Anonymous Call Rejection .....	48
C.3.1	Actions at the Originating AGCF.....	48
C.3.2	Actions at the Originating AS .....	48
C.3.3	Actions at the Terminating AS .....	48
C.3.4	Actions at the Terminating AGCF .....	48
C.4	Automatic Call Return.....	48
C.4.1	Actions at the AGCF at the invoker side .....	48
C.4.2	Actions at the AS at the invoker side .....	48
C.5	Calling Line Identity Presentation / Restriction .....	49
C.5.1	Actions at the Originating AGCF.....	49
C.5.2	Actions at the Originating AS .....	49
C.5.3	Actions at the Terminating AS .....	49
C.5.4	Actions at the Terminating AGCF .....	50
C.6	Calling Name Delivery.....	50
C.6.1	Actions at the Originating AGCF.....	50
C.6.2	Actions at the Originating Application Server .....	50
C.6.3	Actions at the Terminating Application Server .....	50
C.6.4	Actions at the Terminating AGCF .....	50
C.7	Call Forwarding.....	50
C.7.1	Activation/Deactivation/Interrogation.....	50
C.7.1.1	Actions at the AGCF.....	50
C.7.1.2	Actions at the AS .....	50
C.7.2	Invocation.....	51
C.7.2.1	Actions at the Originating AGCF .....	51
C.7.2.2	Actions at the Originating AS .....	51
C.7.2.3	Actions at the Forwarding AS.....	51
C.7.2.4	Actions at the Forwarding AGCF .....	51
C.7.2.5	Actions at the Terminating AS .....	51
C.7.2.6	Actions at the Terminating AGCF.....	51
C.8	Distinctive Ringing .....	51
C.8.1	Actions at the Originating AGCF.....	51
C.8.2	Actions at the Originating Application Server .....	51
C.8.3	Actions at the Terminating Application Server .....	51
C.8.4	Actions at the Terminating AGCF .....	51
C.9	Call Waiting .....	52
C.9.1	General .....	52
C.9.1.1	Actions at the AGCF at the terminating side .....	52
C.9.1.2	Actions at the AS at the terminating side.....	52
C.9.2	Option 1 (Loose coupling) .....	53
C.9.2.1	Actions at the AGCF at the terminating side .....	53
C.9.2.2	Actions at the AS at the terminating side.....	54
C.9.3	Option 2 (Tight coupling).....	55

C.9.3.1	Actions at the AGCF at the terminating side .....	55
C.9.3.2	Actions at the AS at the terminating side.....	56
C.10	Incoming Call Barring.....	58
C.10.1	Activation/Deactivation/Interrogation.....	58
C.10.1.1	Actions at the AGCF.....	58
C.10.1.2	Actions at the AS .....	58
C.10.2	Invocation.....	58
C.10.2.1	Actions at the Originating AGCF .....	58
C.10.2.2	Actions at the Originating AS .....	58
C.10.2.3	Actions at the Terminating AS .....	58
C.10.2.4	Actions at the Terminating AGCF.....	58
C.11	Malicious Call Identification.....	58
C.11.1	Actions at the Originating AGCF.....	58
C.11.2	Actions at the Originating AS .....	58
C.11.3	Actions at the Terminating AS .....	59
C.11.4	Actions at the Terminating AGCF .....	59
C.12	Message Waiting Indicator.....	59
C.12.1	Actions at the AGCF.....	59
C.12.2	Actions at the AS.....	59
C.13	Outgoing Call Barring.....	59
C.13.1	Activation/Deactivation/Interrogation.....	59
C.13.1.1	Actions at the AGCF.....	59
C.13.1.2	Actions at the AS .....	59
C.13.2	Invocation.....	59
C.13.2.1	Actions at the Originating AGCF .....	59
C.13.2.2	Actions at the Originating AS .....	60
C.13.2.3	Actions at the Terminating AS .....	60
C.13.2.4	Actions at the Terminating AGCF.....	60
C.14	Three party service .....	60
C.14.1	General .....	60
C.14.1.1	Actions at the AGCF at the service invocation side .....	60
C.14.1.2	Actions at the AS at the service invocation side .....	61
C.14.2	Option 1 (Loose coupling) .....	62
C.14.2.1	Actions at the AGCF at the invoking side .....	62
C.14.2.2	Actions at the Originating AS at the invoking side.....	62
C.14.3	Option 2 (Tight coupling).....	63
C.14.3.1	Actions at the AGCF at the originating side .....	63
C.14.3.2	Actions at the Originating AS at the originating side .....	63
C.15	Repeat Last Call .....	63
C.15.1	AGCF at the served user side .....	63
C.15.2	AS at the served user side.....	63
<b>Annex D (normative):</b>	<b>Mapping between SIP and the subscriber line protocol.....</b>	<b>64</b>
D.1	Introduction .....	64
D.2	Call Setup message.....	64
D.3	Message Waiting Indicator message .....	65
D.4	Advice of Charge message .....	65
<b>Annex E (informative):</b>	<b>Bibliography.....</b>	<b>67</b>
History .....		68

---

## 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 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

---

# 1 Scope

The present document defines call control protocols and procedures for use in the IMS-based PSTN/ISDN Emulation subsystem based on the Media Gateway Control Protocol (MEGACO), the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

NOTE: The present document relies on the architectural framework defined in TS 182 012 [3] for IMS-based PES Emulation and may need to be updated once the open issues identified in the present document are resolved.

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);
- the interface between the Access Gateway Control Function (AGCF) and the Media Gateway Function (MGF);
- the interface between the Access Gateway Control Function (AGCF) and the Call Session Control Function (CSCF);
- the interface between the CSCF and any other CSCF;
- the interface between the CSCF and an Application Server (AS);
- the interface between the CSCF and the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the Multimedia Resource Function Controller (MRFC);
- the interface between the CSCF and the Breakout Gateway Control Function (BGCF);
- the interface between the BGCF and the MGCF;
- the interface between the BGCF and any other BGCF;
- the interface between the CSCF and an external Multimedia IP network;
- the interface between the CSCF and the IBCF;
- the interface between the CSCF and the IBCF.

---

# 2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

- [1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".
- [2] ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)".



- [3] ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Subsystem; Functional architecture".
- [4] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]".
- [5] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".
- [6] ETSI TS 183 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Common Basic Communication procedures; Protocol specification".
- [7] ETSI TS 183 047: TISPAN NGN "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN IMS Supplementary Services; Advice of Charge (AoC)".
- [8] ETSI TS 183 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Communication HOLD (HOLD); PSTN/ISDN simulation services".
- [9] ETSI TS 183 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification".
- [10] ETSI ES 200 659-3: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 3: Data link message and parameter codings".
- [11] ETSI EG 201 973-2: "Access and Terminals (AT); Public Switched Telephone Network; Support of legacy terminals by Broadband IP networks and equipment; Part 2: Analogue PSTN terminals".
- [12] ETSI ETS 300 738: "Human Factors (HF); Minimum Man-Machine Interface (MMI) to public network based supplementary services".
- [13] ITU-T Recommendation H.248.23: "Gateway control protocol: Enhanced Alerting packages".
- [14] ITU-T Recommendation H.248.26: "Gateway control protocol: Enhanced analog lines packages".
- [15] IETF draft-ietf-sipping-config-framework-08: "A Framework for Session Initiation Protocol User Agent Profile Delivery".
- [16] IETF RFC 4240: "Basic Network Media Services with SIP".
- [17] IETF RFC 2833: "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [18] IETF RFC 3842: "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)".
- [19] IETF RFC 3966: "The tel URI for Telephone Numbers".
- [20] ETSI EN 383 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control (BICC) Protocol or ISDN User Part (ISUP) [ITU-T Recommendation Q.1912.5, modified]".
- [21] IETF RFC 2805: "Media Gateway Control Protocol Architecture and Requirements".
- [22] ITU-T Recommendation H.248.1: "Gateway control protocol".
- [23] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

- [24] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
- [25] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".
- [26] ETSI TS 183 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Message Waiting Indication (MWI): Protocol specification".
- [27] ETSI TS 183 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".
- [28] ETSI ES 282 010: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Charging [Endorsement of 3GPP TS 32.240 v6.3.0, 3GPP TS 32.260 v6.3.0, 3GPP TS 32.297 v6.1.0, 3GPP TS 32.298 v6.1.0 and 3GPP TS 32.299 v6.4.0 modified]".
- [29] IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method".
- [30] ITU-T Recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".
- [31] ITU-T Recommendation Q.764: "Signalling System No. 7 - ISDN User Part signalling procedures".
- [32] ITU-T Recommendation Q.1980.1: "The Narrowband Signalling Syntax (NSS) - Syntax definition".
- [33] ETSI ES 283 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of the SIP-ISUP Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks [3GPP TS 29.163 (Release 7), modified]".
- [34] ETSI TS 183 023: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".
- [35] ETSI EN 300 356: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".
- [36] ITU-T Recommendation Q.735.3: "Multi-level precedence and preemption".
- [37] ITU-T Recommendation Q.735.6: "Global Virtual Network Service".
- [38] ITU-T Recommendation Q.736.3: "Reverse charging (REV)".
- [39] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [40] ETSI EN 301 798: "Services and Protocols for Advanced Networks (SPAN); Anonymous Call Rejection (ACR) Supplementary Service; Service description".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

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

**access gateway:** gateway that interworks a significant number of analogue lines to a packet network and is located at the operator's premises

**media gateway:** See Recommendation H.248.1 [22].

NOTE: In the present document, Media Gateway refers both to Access Gateways and to Residential Gateways.

**media gateway controller:** See Recommendation H.248.1 [22].

**residential gateway:** gateway that interworks a small number of analogue lines

NOTE: A residential gateway typically contains one or two analogue lines and is located at the customer premises.

**Voice over IP gateway:** gateway that implements both a media gateway function and a media gateway controller function as defined in IETF RFC 2805 [21] and supports the provision of voice-based services to analog lines

## 3.2 Abbreviations

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

3PTY	Three-Party service
ACR	Automatic Communication Rejection
AGCF	Access Gateway Control Function
AS	Application Server
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
CCBS	Call Completion on Busy Subscriber
CCNR	Call Completion on No Reply
CD	Call Deflection
CFB	Call Forwarding on Busy
CFNR	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restriction
CN	Core Network
CPG	Call ProGress
CSCF	Call Session Control Function
CONF	Conference
CUG	Closed User Group
CW	Call Waiting
ECT	Explicit Call Transfer
FM	Feature Manager
FQDN	Fully Qualified Domain Name
GPL	Generic Parameter List
GVNS	Global Virtual Network Service
HOLD	Call Hold
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating CSCF
IM	IP Multimedia
I-MGCF	Incoming - MGCF
IMS	IP Multimedia core network Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MCID	Malicious Call Identification
MG	Media Gateway
MGCF	Media Gateway Control Function
MGW	Media Gateway
MGF	Media Gateway Function
MLPP	Multi-Level Precedence and Pre-emption
MRF	Multimedia Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor

MWI	Message Waiting Indicator
NGN	Next Generation Network
NSS	Narrowband Signalling Syntax
O-MGCF	Outgoing - MGCF
PSTN	Public Switched Telephone Network
P-CSCF	Proxy - CSCF
REV	REVerse Charging
RFC	Request For Comments
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SOC	Switch Order Command
SUB	Subaddressing
TAS	Terminal Alerting Signal
TP	Terminal Portability
UA	User Agent
UE	User Equipment
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
UUS	User-to-User Signalling
VGW	Voice over IP GateWay
VMS	Voice Mail System
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

---

## 4 IMS-based PSTN Emulation Subsystem (PES) overview

### 4.1 General

The IMS-based PSTN/ISDN Emulation Subsystem (PES) supports the emulation of PSTN services for analogue terminals connected to the TISpan NGN, through residential gateways or access gateways. The IMS-based PES functional architecture is defined in [3].

ISDN terminals are out of scope.

Emulating PSTN/ISDN services using the IMS-based PES architecture assumes that the logic of the service to be emulated resides in one or more application servers playing the role of a PES application server.

Analogue terminals are connected to residential gateways or access gateways using standard analogue interfaces. The protocol running on interfaces between these gateways and the PES is either the gateway control protocol according to ITU-T Recommendation H.248.1 [22] (P1 reference point) or the session initiation protocol (SIP) according to RFC 3261 [39] (Gm reference point), depending on the type of gateway:

- call control agnostic H.248-based voice over IP media gateway (MGW); or
- call control aware SIP-based voice over IP gateway (VGW).

Call control agnostic means that the media gateway is relaying call control signalling between the PSTN terminal and the AGCF. The relay function has similarities with a signalling gateway function (as defined for common channel signalling systems), i.e., both are stateless from perspective of the call control protocol. Call control awareness implies a complete and stable function concerning call control or session control protocols.

Media gateways incorporate the Media Gateway Functional (MGF) entity identified in ES 282 001 [1] and are controlled by an Access Gateway Control Function (AGCF), at the P1 reference point.

Annex C illustrates the use of the PES for implementing usual PSTN services identified in EG 201 973-2 [11].

## 4.2 URI and address assignments

In case multiple subscribers are connected to the same gateway, there is no need to allocate a private user identity per subscriber. Whether a private user identity is allocated per gateway, group of subscribers or per subscriber is a matter for each operator to decide.

The AGCF stores private user identities and public user identities in a local data base.

---

# 5 Protocol using SIP and SIP events for PES

## 5.1 Introduction

This clause identifies the functional entities of the IMS-based PES architecture [3] that play a specific role in the implementation of PES services with regards to SIP processing.

## 5.2 Functional Entities

### 5.2.1 User Equipment (UE)

Conventional IMS UEs do not exist in PES. In PES, the User Equipment comprises one or more analogue terminals and include the gateway to which they are connected. This gateway may be a H.248-controlled media gateway or a SIP-based Voice over IP Gateway (VGW). SIP-based Voice over IP Gateways (VGW) appear as conventional IMS UEs with regards to the P-CSCF, i.e., they play the role of a SIP user agent from SIP perspective. Analogue terminals are not visible to PES network entities.

NOTE: The gateway may be located in the customer's premises or in the operator's premises.

For the purpose of the PES, the VGW shall implement the role of a PES endpoint as described in clause 5.3.1.

### 5.2.2 Access Gateway Control Function (AGCF)

For the purpose of the PES, the AGCF shall implement the role of the PES access point as described in clause 5.3.2.

The AGCF is part of the trust domain.

The AGCF entity encompasses the functionality of an H.248 Media Gateway Controller (MGC) as defined in ITU6 Recommendation H.248.1 [22] and of a SIP User Agent as defined in RFC 3261 [39]. Within the AGCF, the MGC and SIP UA components are coordinated by a Feature Manager entity whose logical behaviour is described in annex B.

The AGCF shall appear to other CSCFs as if it were a P-CSCF.

### 5.2.3 Application Server (AS)

For the purpose of the PES, the AS shall implement the role of a PES application server, as described in clause 5.3.3.

NOTE: The PES architecture does not require that all application servers involved in sessions initiated/addressed by/to PES users adhere to the procedures prescribed for the PES application server role. Any application server that conforms to TS 182 006 [2] may be involved in such sessions.

### 5.2.4 Media Resource Function Controller (MRFC)

For the purpose of the PES, an MRFC shall implement the role of the PES announcement server as described in clause 5.3.4.

## 5.2.5 Media Gateway Controller Function (MGCF)

For the purpose of the PES, the MGCF shall implement the role of a PES interworking application as described in clause 5.3.5.

## 5.2.6 Interconnection border control function (IBCF)

For the purpose of the PES, the IBCF shall implement the role of a PES Interconnection Application as described in clause 5.3.6.

## 5.3 Role

### 5.3.1 PES Endpoint

#### 5.3.1.1 General

In addition to the procedures specified in the rest of clause 5.3.1, the PES endpoint shall support the procedures specified in ES 283 003 [4] and TS 183 028 [6] appropriate to an IMS UE.

#### 5.3.1.2 Subscription for dial tone management

The PES Endpoint shall subscribe to the "ua-profile" event defined in [15] and support the Dial Tone Management document defined in annex A of the present document.

NOTE 1: The PES endpoint sets the current dial tone to the value of the dial-tone-pattern element received in the Dial Tone Management document.

The subscription may be implicit or explicit. If explicit subscription is required, the identity of the AS acting as the profile delivery server where the subscription request shall be sent may be provisioned in the functional entity in which the PES endpoint is implemented. Alternatively, the user profile may contain an appropriate Initial Filter Criteria on SUBSCRIBE messages that ensure that such requests are sent to the AS acting as the profile delivery server.

NOTE 2: For dial tone changes due to the Message Waiting service, the PES endpoint may, as an option, subscribe to the "message-summary" event package defined in RFC 3842 [18]. If the "message-summary" event is received with a Messages-Waiting field set to "yes", the message waiting tone becomes the current dial tone. If the message-summary event is received with a "messages-waiting" field set to "no", the default dial tone becomes the current dial tone. Some Voice Mail Servers (VMS) do not require an explicit subscription to the message-summary event package, so the PES endpoint should also be prepared to accept "unsolicited" SIP NOTIFY requests with the "message-summary" event.

#### 5.3.1.3 Registration procedures

The allocation of private and public user identities is left to each operator to decide. Two approaches are identified:

- One private user identity is assigned to a group of subscriber. A temporary public user identity is associated with this private user identity. Real public user identities representing the subscribers connected to the analogue ports of the VGW are registered using implicit registration procedures defined in ES 283.003 [4].
- A pair of private and public user identity is associated with each analogue port connected to the VGW.

The two approaches are not mutually exclusive.

## 5.3.2 PES Access Point

### 5.3.2.1 General

In addition to the procedures specified in the rest of clause 5.3.2, the behaviour of the PES access point shall be equivalent to the concatenation of the behaviour of a UE and a P-CSCF entity, as defined in ES 283.003 [4] and TS 183 028 [6].

NOTE: The above statement does not require AGCF implementations to execute UE and P-CSCF procedures in sequence.

### 5.3.2.2 Subscription for dial tone management

The PES access point shall subscribe to the "ua-profile" event defined in [15] and support the Dial Tone Management document defined in annex A of the present document.

NOTE 1: The PES access point sets the current dial tone to the value of the dial-tone-pattern element received in the Dial Tone Management document.

The subscription may be implicit or explicit. If explicit subscription is required, the identity of the AS acting as the profile delivery server where the subscription request shall be sent may be provisioned in the functional entity in which the PES access point is implemented. Alternatively, the user profile may contain an appropriate Initial Filter Criteria on SUBSCRIBE messages that ensure that such requests are sent to the AS acting as the profile delivery server.

NOTE 2: For dial tone changes due to the Message Waiting service, the PES access point may, as an option, subscribe to the "message-summary" event package defined in RFC 3842 [18]. If the "message-summary" event is received with a "Messages-Waiting" field set to "yes", the message waiting tone becomes the current dial tone. If the "message-summary" event is received with a "Messages-Waiting" field set to "no", the default dial tone becomes the current dial tone. Some Voice Mail Servers (VMS) do not require an explicit subscription to the "message-summary" event package, so the PES access point should also be prepared to accept "unsolicited" SIP NOTIFY requests with the "message-summary" event.

### 5.3.2.3 Registration Procedures

The following IMS parameters are assumed to be available in a local data base:

- a private user identity;
- a public user identity; and
- a home network domain name to which SIP REGISTER requests are addressed.

The allocation of private and public user identities is left to each operator to decide. Two approaches are identified:

- One private user identity is assigned to a group of subscribers. Groups should not contain subscribers connected to different gateways. A temporary public user identity is associated with this private user identity. Public user identities representing the subscribers connected to the analogue ports controlled by the AGCF are registered using implicit registration procedures defined in ES 283.003 [4].
- A pair of private and public user identity is associated with each analog port connected to the MGWs controlled by the AGCF.

A combination of the two approaches may also be used.

The PES access point populates REGISTER messages as follows:

- a) an Authorization header, with the username field, set to the value of the private user identity associated with the subscriber or subscriber group to be registered;
- b) a From header set to the SIP URI that contains the temporary public user identity associated with the group to be registered or the public user identity associated with the subscriber to be registered;

- c) a To header set to the SIP URI that contains the temporary public user identity associated with the group to be registered or the public user identity associated with the subscriber to be registered;
- d) a Contact header set to include SIP URI(s) containing its own IP address in the hostport parameter or FQDN;
- e) a Via header set to include the IP address or FQDN of the AGCF in the sent-by field;
- f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE: A greater value may be used as an operator's option when registration applies to access gateways.

- g) a Request-URI set to the SIP URI of the domain name of the home network associated with the group to be registered;
- h) the Supported header containing the option tag "path";
- i) a Path header including an entry containing:
  - the SIP URI identifying the AGCF;
  - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the AGCF) are expected to be treated as for the terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- j) a Require header containing the option tag "path";
- k) a P-Charging-Vector header with the icid parameter populated as specified in ES 282 010 [28];
- l) the P-Access-Network-Info header set as specified for the DSL access network technology; and
- m) a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the network where the AGCF resides

When group registration applies, the contents of the P-Associated-URI header received in the response to the REGISTER request is ignored.

#### 5.3.2.4 Outgoing Call Control procedures

Calls initiated by a PES user via a PES access point shall operate following the UE call origination procedures defined in TS 283 003 [4]. The P-Asserted-Identifier shall be populated following the same rules defined for Registration in clause 5.3.2.3.

#### 5.3.2.5 Incoming Call Control procedures

Incoming calls received by a PES access point shall operate following the UE call termination procedures defined in TS 283 003 [4]. The P-Called-Party header value is used to fetch the termination to which the call shall be delivered.

### 5.3.3 PES Application Server

#### 5.3.3.1 General

In addition to the procedures specified in the rest of clause 5.3.3, the PES application server shall support the procedures specified in ES 283 003 [4] appropriate to an application server.

#### 5.3.3.2 Basic call procedures

A PES application server can act either as a proxy server or as a Back to Back User Agent (B2BUA) while processing calls. When acting as a B2BUA, the PES application server provides both originating UA and terminating UA functions as described in TS 283 003 [4]. As an originating UA that sends outbound INVITE requests, the PES application server must appropriately handle responses received from a forking proxy and must appropriately interwork provisional and final INVITE responses, as well as other SIP requests, between the originating UA and terminating UA functions employed on a single call.



When handling an outgoing call, the PES application server shall populate the "cpc" URI parameter in the contents of the P-Asserted-Identifier header as defined in ES 283 003 [4] in each INVITE request, unless the parameter value is "ordinary". How the PES application server determines the value of this parameter (UPSF query, local configuration data...) is outside the scope of the present document.

### 5.3.3.3 Announcement procedures

The PES application server shall have the capability of requesting announcements during any phase of a session, according to the procedures described in TS 183 028 [6].

The PES application server shall use the ANNC URL syntax defined in [16] when requesting a PES announcement server to play an announcement.

A PES application server acting as a B2BUA must appropriately handle received Call-Info, Alert-Info, and Error-Info headers that contain requests to play announcements, as defined in TS 183 028 [6]. Depending on the application, this may mean relaying the header toward the originating PES endpoint or PES access point, connecting the originating UE to an MRF, or ignoring the announcement request and providing some other call processing (such as with a simultaneous ringing application that ignores failure announcements from unsuccessful call legs).

### 5.3.3.4 Dial Tone Management

The PES application server shall act as a profile delivery server and manage Dial Tone Management documents as described in annex A. Changes to these documents shall be notified by reporting the "ua-profile" event defined in [15]. How the PES server keeps track of changes to these documents is outside the scope of the present document.

### 5.3.3.5 Transport of ISUP information

#### 5.3.3.5.1 General

Clause 5.3.3.5 describes the general behaviour of the PES application server in the case the PES application server is capable of exchanging ISUP information, as defined in ITU-T Recommendation Q.763 [30], carried within Narrowband Signalling Syntax (NSS) [32] message bodies with its SIP signalling peers to perform service related signalling that is capable of interworking with PSTN services. Clause C.1.4 lists examples of services some of which may require the use of encapsulated ISUP information. The sending or receiving of ISUP information in NSS message bodies is applicable to any of the following roles of the Application Server:

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

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

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

The PES application server shall support parameter translations and defaults defined in ES 283 027 [33] for the ISUP information needed for supported services. The PES application server shall also send each piece of ISUP information in the appropriate SIP message so as to allow the valid interworking with the corresponding PSTN services according to ES 283 027 [33]. The PES application server shall not include in NSS message bodies any ISUP information that is already represented by SIP signalling.

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

### 5.3.3.5.2 Sending NSS message bodies to a peer SIP signalling entity

#### 5.3.3.5.2.1 General

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

- The PES application server is capable of performing service related signalling using ISUP information for one or more of the services it supports.
- An event associated with one of the supported services occurs that requires that ISUP information be sent to the peer SIP signalling entity. This event may be the receipt of signalling information from another SIP interface to the PES application server, or a service event internal to the PES application server.
- Either the encapsulating message is the initial INVITE request, or the peer SIP signalling entity has previously indicated support for NSS message bodies within the associated dialog (see clause 5.3.3.5.2.2).
- The SIP signalling in the encapsulating message cannot represent the information, and the information is different from the default values defined in ES 283 027 [33].

#### 5.3.3.5.2.2 Determining support for NSS message bodies

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

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

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

#### 5.3.3.5.2.3 NSS message bodies

The PES application server shall format the NSS message body according to ITU-T Recommendation Q.1980.1[32]. The Content-Type header field associated with the NSS message body shall be included as follows:

- Content-Type: application/nss.

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

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

#### 5.3.3.5.2.4 ISUP information security

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

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

#### 5.3.3.5.2.5 Determining in which message to encapsulate ISUP information

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

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

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

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

#### 5.3.3.5.2.6 Determining the NSS message identifier code

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

#### 5.3.3.5.2.7 Determining the content disposition handling

##### 5.3.3.5.2.7.1 Content disposition for the initial INVITE request

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

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

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

##### 5.3.3.5.2.7.2 Content disposition for the INFO request

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

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

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

#### 5.3.3.5.2.7.3 Content disposition for other SIP messages

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

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

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

##### 5.3.3.5.3.1 General

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

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

##### 5.3.3.5.3.2 ISUP compatibility procedures

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

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

#### 5.3.3.6 Handling of charging information

The PES application server shall be able to process charging information contained in SIP messages received from downstream.

The PES application server shall be able to insert charging information in SIP messages sent in the upstream direction, using the mechanism described in TS 183 047 [7].

### 5.3.4 PES Announcement Server

#### 5.3.4.1 General

In addition to the procedures specified in the rest of clause 5.3.4, the PES announcement server shall support the procedures specified in ES 283 003 [4] appropriate to an MRFC.

#### 5.3.4.2 Announcement procedures

The PES announcement server shall support the ANNC URL syntax defined in [16] when providing announcements, prompt & collect functions, and multi-party conferencing.

### 5.3.5 PES Interworking Application

#### 5.3.5.1 General

In addition to the procedures specified in the rest of clause 5.3.5, the PES interworking application shall support the procedures specified in ES 283 003 [4] and TS 183 028 [6] appropriate to an MGCF.

### 5.3.5.2 Routing procedures

In case of incoming calls from legacy networks, the PES interworking application determines the next hop in IP routing depending on received signalling information, based on configuration data and/or data base look up. The next hop may be an I-CSCF, a BGCF or an IBCF.

Based on the destination and local policy rules, the PES interworking application may include ISUP information in the messages sent to the next entity, as described in clause 5.3.5.4.

### 5.3.5.3 Handling of charging information

The PES interworking application shall be able to insert charging information in SIP messages sent in the upstream direction, based on charging information received from the PSTN.

### 5.3.5.4 Transport of ISUP information

#### 5.3.5.4.1 General

The procedures in the clause 5.3.5.4 allow the PES interworking application to discover whether or not its peer SIP signalling entity is capable of supporting the encapsulation of ISUP information in Narrowband Signalling Syntax (NSS) [32] message bodies within SIP messages, and to successfully support the additional exchange of ISUP information needed for those services supported in common by endpoints supporting potentially different sets of services. These procedures are based on ES 283 027 [33] with the extended capabilities described in the present document. When signalling ISUP information within a SIP dialog, the PES interworking application shall act as either a Type A or Type B exchange depending on the role (e.g., gateway between operators, transit) the PES interworking application is performing for that particular call and the ability to exchange ISUP information during the call. Clause C.1.4 lists examples of services some of them may require the use of encapsulated ISUP information. Each IMS PES must assure that ISUP information is not shared with UEs and untrusted SIP networks according to local policy. Clause 5.3.5.4.2.4 describes the PES interworking application's role in maintaining NSS security.

The PES interworking application shall support parameter translations and defaults defined in ES 283 027 [33] for the ISUP information needed for supported services. The PES interworking application shall also send each piece of ISUP information in the appropriate SIP message so as to allow valid interworking with the corresponding PSTN services according to ES 283 027 [33]. The PES interworking application shall not include in NSS message bodies any ISUP information that is already represented by SIP signalling.

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

#### 5.3.5.4.2 Sending ISUP information to a peer SIP signalling entity

##### 5.3.5.4.2.1 General

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

- Either the encapsulating message is the initial INVITE request, or the peer SIP signalling entity has previously indicated support for NSS message bodies within the associated dialog (see clause 5.3.5.4.2.2).
- An event occurs requiring signalling to the peer SIP signalling entity. This event may be the receipt of an ISUP message from the PSTN, or an event internal to the MGCF.
- According to local configuration, selected ISUP information shall be encapsulated and sent towards the peer SIP signalling entity.
- The SIP signalling in the encapsulating message cannot represent the information, and the information is different from the default values defined in ES 283 027 [33].

#### 5.3.5.4.2.2 Determining support for NSS message bodies

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

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

#### 5.3.5.4.2.3 NSS message bodies

The PES interworking application shall format the NSS message body according to ITU-T Recommendation Q.1980.1 [33]. The Content-Type header field associated with the NSS message body shall be included as follows:

- Content-Type: application/nss.

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

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

#### 5.3.5.4.2.4 ISUP information security

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

#### 5.3.5.4.2.5 Determining in which SIP message to encapsulate ISUP information

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

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

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

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

#### 5.3.5.4.2.6 Determining the NSS message identifier code

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

#### 5.3.5.4.2.7 Determining the content disposition handling

##### 5.3.5.4.2.7.1 Content disposition for the initial INVITE request

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

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

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

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

##### 5.3.5.4.2.7.2 Content disposition for the INFO request

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

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

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

##### 5.3.5.4.2.7.3 Content disposition for other SIP messages

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

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

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

##### 5.3.5.4.3.1 General

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

### 5.3.5.4.3.2 ISUP compatibility procedures (local policy options)

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

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

### 5.3.5.4.3.3 Alignment of SIP signalling and NSS message body contents

On receipt of a SIP message containing an NSS message body, the PES interworking application shall use the encapsulated ISUP information in preference to any value determined by interworking procedures and default values defined in ES 283 027 [33].

### 5.3.5.4.4 ISUP messages for special consideration

#### 5.3.5.4.4.1 General

Table 1 lists the PES interworking application behaviour upon receipt of ISUP messages that have no counterparts in basic SIP call control messages.

**Table 1: ISUP messages for special consideration**

ISUP message	Reference
Subsequent address message	5.3.5.4.4.6
Reset circuit	5.3.5.4.4.2
Call progress	5.3.5.4.4.3 (note 1)
Circuit group blocking	5.3.5.4.4.2
Circuit group blocking acknowledgement	5.3.5.4.4.2
Circuit group query (national use)	5.3.5.4.4.2
Circuit group query response (national use)	5.3.5.4.4.2
Group reset	5.3.5.4.4.2
Circuit group reset acknowledgement	5.3.5.4.4.2
Confusion	5.3.5.4.4.2 or 5.3.5.4.4.3 (note 2)
Facility reject	5.3.5.4.4.2 or 5.3.5.4.4.3 (note 2)
User-to-user information	5.3.5.4.4.3
Forward transfer	5.3.5.4.4.3
Subsequent directory number (national use)	5.3.5.4.4.3
Suspend	5.3.5.4.4.3 or 5.3.5.4.4.5
Resume	5.3.5.4.4.3 or 5.3.5.4.4.5
Blocking	5.3.5.4.4.2
Blocking acknowledgement	5.3.5.4.4.2
Continuity check request	5.3.5.4.4.2
Continuity	5.3.5.4.4.2
Unblocking	5.3.5.4.4.2
Unblocking acknowledgement	5.3.5.4.4.2
Unequipped CIC (national use)	5.3.5.4.4.2
Circuit group unblocking	5.3.5.4.4.2
Circuit group unblocking acknowledgement	5.3.5.4.4.2
Charging information (national use)	5.3.5.4.4.3
Facility accepted	5.3.5.4.4.3
Facility request	5.3.5.4.4.3
User part test	5.3.5.4.4.2
User part available	5.3.5.4.4.2
Facility	5.3.5.4.4.3
Network resource management	5.3.5.4.4.3
Identification request	5.3.5.4.4.3
Identification response	5.3.5.4.4.3
Information (national use)	5.3.5.4.4.3
Information request (national use)	5.3.5.4.4.3
Segmentation	5.3.5.4.4.4
Loop back acknowledgment (national use)	5.3.5.4.4.3



ISUP message	Reference
Loop prevention	5.3.5.4.4.3
Overload (national use)	5.3.5.4.4.2
Pass-along (national use)	5.3.5.4.4.3
Application transport	5.3.5.4.4.2 or 5.3.5.4.4.3 (note 2)
Pre-release information	5.3.5.4.4.3
Release complete	5.3.5.4.4.2
NOTE 1: This is the default handling of the ISUP information associated with the Call Progress (CPG) message when other clauses in the present document do not apply. The ISUP information associated with a CPG message may be encapsulated in a 18X response, an UPDATE request, a reINVITE request, or an INFO request.	
NOTE 2: The ISUP information in these messages is either locally terminated or sent transparently depending on whether it is destined for the PES interworking application or for another exchange.	

#### 5.3.5.4.4.2 ISUP side procedures only

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

#### 5.3.5.4.4.3 Transparent messages

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

#### 5.3.5.4.4.4 ISUP segmentation

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

#### 5.3.5.4.4.5 Receipt of network initiated SUS and RES

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

If the I-MGCF is the controlling exchange for network initiated Suspend procedures or is unable to forward SUS information to the peer SIP signalling entity, the I-MGCF shall invoke the procedures described in ITU-T Recommendation Q.764 clause 2.4.1c [31] on the ISUP interface and shall not forward ISUP information from either SUS or RES.

#### 5.3.5.4.4.6 Subsequent address message

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

### 5.3.5.5 Optional SIP/ISUP interworking procedures for PSTN Bridging

If the PES interworking application can determine that a call is for PSTN bridging (i.e. that the call will end up in an ISUP network) then the PES interworking application may, as a network option, use the interworking procedures defined in EN 383 001 [20] for Profile C.

The way the PES interworking application detects that a call is for PSTN bridging is outside the scope of the present document (local tables or data base lookups may be used).

For PSTN bridging, the PES interworking application may route the SIP INVITE request according to the IMS transit mechanism, or any other mechanism, based on local policy.

## 5.3.6 PES interconnection application

### 5.3.6.1 General

In addition to the procedures specified in the rest of clause 5.3.6, the PES interconnection application shall support the procedures specified in ES 283 003 [4] appropriate to an IBCF.

### 5.3.6.2 Procedures related to NSS message bodies

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

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

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

---

# 6 Protocol using SIP/SDP for PES

## 6.1 Introduction

This clause identifies the functional entities of the IMS-based PES architecture [3] that play a specific role in the provision of PES services with regards to SDP processing in the context of SIP signalling.

## 6.2 Functional Entities

### 6.2.1 User Equipment (UE)

Conventional SIP UEs do not exist in PES (see clause 5.2.1).

For the purpose of the PES, the VGW shall implement the role of a PES endpoint as described in clause 6.3.1.

### 6.2.2 Access Gateway Control Function (AGCF)

For the purpose of the PES, the AGCF shall implement the role of the PES access point as described in clause 6.3.2.

The AGCF entity encompasses the functionality of a Media Gateway Controller (MGC) and of a SIP User Agent.

### 6.2.3 Application Server (AS)

For the purpose of the PES, the AS shall implement the role of a PES application server, as described in clause 6.3.3.

### 6.2.4 Media Resource Function Controller (MRFC)

For the purpose of the PES, an MRFC shall implement the role of the PES announcement server as described in clause 6.3.4.

## 6.3 Roles

### 6.3.1 PES Endpoint

The PES endpoint shall support the procedures specified in ES 283 003 [4] appropriate to an IMS UE.

### 6.3.2 PES Access Point

#### 6.3.2.1 General

In addition to the procedures specified in the rest of clause 6.3.2, the PES access point shall support the procedures specified in ES 283 003 [4] appropriate to an AGCF.

#### 6.3.2.2 Originating calls

The usage of SDP by a PES access point is the same as its usage by a PES endpoint with the following exception:

- Only one media description shall be included (i.e. one m= line).

NOTE: Support of T.38 is outside the scope of TISPAN NGN Release 1.

When sending an SDP, the PES access point shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" lines in the SDP, and it shall ignore them when received in the SDP.

When generating an INVITE request, the PES access point shall:

- populate the SDP with the codecs supported by the associated H.248 media gateway; and
- in order to support DTMF, populate the SDP with MIME subtype "telephone-event" as described in RFC 2833 [17], unless ITU-T Recommendation G.711 [23] is the only proposed codec.

#### 6.3.2.3 Terminating calls

The usage of SDP by the PES access point is the same as its usage by a PES endpoint as defined in ES 283 003 [4], with the following exceptions:

- When the PES access point sends a 183 (Session Progress) response with SDP payload, it shall only request confirmation for the result of the resource reservation at the originating endpoint if there are any remaining unfulfilled preconditions.
- Any media description whose media type is different from audio shall be ignored.

When sending an SDP, the PES access point shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" lines in the SDP, and it shall ignore them when received in the SDP.

When receiving an initial INVITE request, the PES access point shall:

- check for a codec that matches the requested SDP, which may include the MIME subtype "telephone-event" as described in RFC 2833 [17].

When the PES access point generates and sends a 183 (Session Progress) response to an initial INVITE request, the PES access point shall:

- set SDP indicating the selected codec, which may include the MIME subtype "telephone-event" as described in RFC 2833 [17].

#### 6.3.2.4 Modifying SDP within existing dialogues

Once a SIP dialog is confirmed (e.g. after a 200 OK and ACK have been used to acknowledge an INVITE request), the PES access point must be prepared to accept a re-INVITE request that contains a new SDP offer. While a SIP dialog remains unconfirmed (e.g. a 200 OK and ACK have not been used to acknowledge an INVITE request), the PES access point must be prepared to accept an UPDATE request that contains a new SDP offer, following the rules defined in RFC 3311 [29].

### 6.3.3 PES Application Server

#### 6.3.3.1 General

In addition to the procedures specified in the rest of clause 6.3.3, the PES application server shall support the procedures specified in ES 283 003 [4] appropriate to an application server.

When acting as a B2BUA, the PES application server must appropriately handle SDP received in responses received from a forking Proxy and must appropriately interwork SDP received in provisional and final INVITE responses, as well as other SIP requests, between the originating UA and terminating UA functions employed on a single call.

### 6.3.4 PES Announcement Server

#### 6.3.4.1 General

In addition to the procedures specified in clause 6.3.4, the PES announcement server shall support the procedures specified in ES 283 003 [4] appropriate to an MRFC.

---

## 7 Protocol using H.248 for PES

### 7.1 Introduction

This clause identifies the functional entities of the IMS-based PES architecture [3] that play a specific role in the provision of PES services with regards to H.248 processing.

### 7.2 Functional Entities

#### 7.2.1 Access Gateway Control Function (AGCF)

For the purpose of the PES, the AGCF shall implement the role of the PES access point as described in clause 7.3.1.

The AGCF entity encompasses the functionality of an H.248 Media Gateway Controller (MGC) and of a SIP User Agent. Within the AGCF, the MGC and SIP UA components are coordinated by a Feature Manager entity whose logical behaviour is described in annex B.

#### 7.2.2 Media Gateway Function (MGF)

For the purpose of the PES, the MGF shall implement the role of the PES media gateway as described in clause 7.3.2

## 7.3 Roles

### 7.3.1 PES Access Point

#### 7.3.1.1 General

In addition to the procedures specified in the rest of clause 7.3.1, the PES access point shall support the procedures specified in ES 283 002 [5] appropriate to an MGC.

#### 7.3.1.2 Registration

Registration is supported using the H.248 Service Change procedure. Registration can be performed on a global basis (all lines connected to the same PES media gateway), on a group basis or on a per line basis. This event is passed to the Feature Manager.

When the global basis registration mechanism applies, on receipt of a ServiceChange command with "Root" TerminationID from the PES media gateway reporting the MG state changing event and after processing the event according to normal service change procedures has finished, the MGC in the PES access point shall send a **Service-Change** primitive to inform the Feature Manager if the ServiceChangeMethod is set to "Restart" with ServiceChangeReasons 901 ("Cold Boot") or 902 ("Warm Boot") or "Forced" or "Graceful".

Receipt of a ServiceChange command from the PES media gateway reporting a Terminations state changing event shall not cause the MGC in the PES access point to notify the Feature Manager.

When the per line basis registration mechanism applies, on receipt of a ServiceChange command from the PES media gateway, and after processing the event according to normal service change procedures has finished, the MGC in the PES access point shall send a **Service-Change** primitive to inform the Feature Manager if the ServiceChangeMethod is set to "Restart" with ServiceChangeReasons 900 ("Service Restored") or 902 ("Warm Boot") or "Forced" or "Graceful".

When the MGC in the PES access point detects that the PES media gateway lost communication with the MGC in the PES access point, but it was subsequently restored, since MG state may have changed, the MGC in the PES access point may use the H.248 Audit mechanism to resynchronize its state with the PES media gateways. If the MGC in the PES access point detects that the audited state of the specified Terminations is different from the recorded state, the MGC in the PES access point shall use a Service-Change primitive with proper parameters to inform the Feature Manager about the event.

When the MGC in the PES access point detects that the PES media gateway lost the communication with the PES media gateway, the MGC in the PES access point shall use Service-Change primitive with proper parameters to inform the Feature Manager about this event.

#### 7.3.1.3 Basic Session control procedures for analog lines

##### 7.3.1.3.1 Originating side procedures

###### 7.3.1.3.1.1 Call Initiation

###### *Step 0*

On receipt of a notify command from the PES media gateway reporting the off-hook (**al/of**) event the PES access point shall:

- Derive the user identity associated with the termination reporting the event.
- Report the occurrence of the off-hook event to the Feature Manager using a **Session-Attempt** primitive.
- Interact with the Feature Manager to determine which dial tone pattern shall be applied (see clause 5.3.2.2).
- Request the PES media gateway to apply the signal that correspond to the selected dial tone (cg/dt or srvt/mwt or xcg/spec) according to the value of the dial-tone-pattern element of the Dial Tone Management document described in annex A.

- Request the PES media gateway to detect and report the following events:
  - the **xdd/xce** event, according to the digit map in force;
  - the **al/on** event.

NOTE 1: The PES media gateway terminations may also be preconfigured by the PES access point, using signals and events descriptors embedded in the **al/of** event descriptor, in such a way that upon detection of the off-hook event, the dial tone is automatically delivered and the digit collection is automatically started. The PES access point replaces the event descriptors in case the dial tone is modified.

- Proceed with step 1

#### *Step 1*

On receipt of the **al/on** event, the PES access point shall:

- Initiate call clearing procedures.
- Report the occurrence of the on-hook event to the feature manager using a **Session-Release** primitive.

On receipt of the notification of the **xdd/xce** event, the PES access point shall:

- If the received digits do not correspond to a valid number but receipt of additional digits may lead to a valid number, request the PES media gateway to detect and report the following events:
  - the **xdd/xce** event, according to a subsequent digit map;
  - the **al/on** event.

This step may be repeated several times, until a valid number has been collected or the user has abandoned the call attempt by going back on-hook.

- If the received digits do not correspond to a valid number and receipt of additional digits cannot lead to a valid number, request the PES media gateway to:
  - play an appropriate announcement using the **an/apf** signal;
  - report the **g/sc** signal completion event for the **an/apf** signal;
  - initiate call clearing.
- If the received digits correspond to a complete number, the PES access point shall:
  - request the PES media gateway to create an H.248 context with the caller's analogue termination and an ephemeral termination;
  - send a **Setup-Request** primitive to the Feature Manager. SDP information shall be set according to the information received in the response to the Add command;
  - request the PES media gateway to detect and report the following events:
    - 1) the **al/fl** event;
    - 2) the **al/on** event;
  - wait for either of these events and for events from the Feature Manager. Proceed to step 2 on the occurrence of any of these events.

#### *Step 2*

On receipt of the notification of the **al/on** event, the PES access point shall initiate call clearing procedures.

On receipt of the notification of the **al/fl** event, the PES access point shall notify its Feature Manager using a **Feature Request** primitive.

On receipt of a **Session Progress** primitive from the Feature Manager without alerting indication, the PES access point shall:

- If the primitive contains an early media indication, request the PES media gateway to modify the ephemeral termination properties accordingly so that the calling party can perceive in band information.

NOTE 2: The termination mode may be set to send-receive or receive-only depending on the network operator's policy.

- If the primitive does not contain an early media indication, ignore the event.
- Remain in the same state.

On receipt of a **Session Progress** primitive from the Feature Manager indicating alerting, the PES access point shall:

- If the primitive contains an early media indication, request the PES media gateway to modify the ephemeral termination properties accordingly so that the calling party can perceive in band information.

NOTE 3: The termination mode may be set to send-receive or receive-only depending on the network operator's policy.

- If the primitive does not contain an early media indication, request the PES media gateway to apply the **cg/rt** signal to the physical termination.
- Proceed with step 3.

On receipt of an internal **Setup-Response** primitive reporting a busy condition, the PES access point shall:

- Request the PES media gateway to apply the **cg/bt** signal to the physical termination.
- Initiate call clearing after expiry of an operator's defined local timer.

On receipt of an internal **Setup-Response** primitive reporting that no response has been received from the destination, the PES access point shall:

- Initiate Call Clearing.

On receipt of an internal **Setup-Response** primitive reporting answer from the destination, the PES access point shall

- Request the PES media gateway to set the mode of the termination to send-receive.
- Modify the ephemeral termination's remote descriptor properties in accordance with information received from the remote side.
- As an operator's option request the PES media gateway to apply the **xal/las** signal.
- Proceed with step 4.

### Step 3

On receipt of the **al/on** event, the PES access point shall:

- initiate call clearing procedures.
- Report the occurrence of the on-hook event to the feature manager using a **Session-Release** primitive.

On receipt of the notification of the **al/fl** event, the PES access point shall notify the feature manager using a **Feature Request** primitive.

On receipt of an internal **Setup-Response** primitive reporting that no response has been received from the destination, the PES access point shall:

- Request the PES media gateway to stop the ring back (**cg/rt**) signal if application of this signal had been requested before.
- Initiate Call Clearing procedures.

On receipt of an internal **Setup-Response** primitive reporting answer from the destination, the PES access point shall

- Request the PES media gateway to set the mode of the ephemeral termination to send-receive if not performed previously.
- Modify the ephemeral termination's remote descriptor properties in accordance with information received from the remote side.
- As an operator's option request the PES media gateway to apply the **xal/las** signal.
- Proceed with step 4.

#### *Step 4*

On receipt of an internal **Session-Release** primitive, the PES access point shall initiate call clearing procedures.

On receipt of an internal **Charging-Indication** primitive, the PES access point shall request the PES media gateway to apply one of the signals for sending metering pulses (**amet/em** or **amet/mpb**).

On receipt of an internal **Session-Update** primitive, the PES access point shall modify the ephemeral termination properties accordingly.

On receipt of the **al/on** event, the PES access point shall:

- initiate call clearing procedures;
- report the occurrence of the on-hook event to the feature manager.

On receipt of the notification of the **al/fl** event, the PES access point shall notify the feature manager.

#### 7.3.1.3.1.2 Call Clearing

The PES access point shall:

- If the **xal/las** signal was applied on the termination when entering the active phase, request the PES media gateway to apply the **xal/nt** signal.
- Send a **Session-Release** primitive to the internal SIP UA (via the feature manager), if the call clearing phase has been entered on receipt of an **al/on** event.
- Request the PES media gateway to subtract the ephemeral termination from the current context.
- If the calling party is still off-hook, request the PES media gateway to apply the off-hook warning tone (**xcg/roh**) to the physical termination. When the calling party becomes on-hook, the PES access point shall:
  - Request the PES media gateway to move the termination back to the Null context (i.e.; subtract command).
  - Report the occurrence of the on-hook event to the feature manager.

#### 7.3.1.3.2 Terminating side procedures

##### 7.3.1.3.2.1 Call Initiation

#### *Step 0*

On receipt of a **Setup-Request** primitive from the internal SIP UA (via the Feature Manager), the PES access point shall:

- Check that the required bearer service is compatible with analogue lines, otherwise return a **Setup-Response** to the Feature Manager, with a reject indication.
- Determine which physical termination is associated with the called party. If no termination is associated with the called part, the PES access point shall send a **Setup-Response** primitive with a failure indication to the internal SIP UA via the Feature Manager.



- Check the administrative status of this termination. If the termination is out of service, with the called part, the PES access point shall send a setup-response primitive with a failure indication to the internal SIP UA via the Feature Manager.
- Create an H.248 context with an ephemeral termination, based on the session description information received in the **Setup-Request**.
- Check whether it is already engaged in a call.

NOTE: As an operator's option, an AuditValue command may be sent to the Media Gateway to verify the status of the termination.

If the termination is not engaged in a call, the PES access point shall:

- Request the PES media gateway to apply ringing to the physical termination. The signal that is used (**alert/ring** or **andisp/dwa**) depends on whether or not information need to be displayed to the terminal. Annex D specifies the mapping between SIP headers and the Display Data Block parameter of the andisp/dwa signal. As directed by the AS (with a SIP Alert-Info header in the INVITE request), the PES access point may direct the PES media gateway to apply a distinctive ringing tone.
- Send a **Session-Progress** (Alerting) primitive to the Feature Manager.
- Start a no-answer timer.
- Request the PES media gateway to detect the off-hook event (**al/of**).
- Proceed to step 1.

If the termination is already engaged in a call, the PES access point shall either (as an operator's option):

- Option 1: Send a **Setup-Response** (busy) primitive to the internal SIP UA; or
- Option 2: Initiate a call waiting procedure:
  - Request the PES media gateway to apply the call waiting tone to the physical termination. The signal that is used (**cg/cw** or **andisp/dwa**) depends on whether or not information need to be displayed to the terminal. Annex D specifies the mapping between SIP headers and the Display Data Block parameter of the andisp/dwa signal. As directed by the AS (with a SIP Alert-Info header in the INVITE request), the PES access point may direct the PES media gateway to apply a distinctive call waiting tone.
  - Start a call-waiting timer.
  - Proceed to step 1.

If a **Session-Release** primitive is received from the internal UA, via the feature manager, the PES access point shall initiate call clearing procedures.

#### *Step 1*

If an off-hook (**al/of**) event is notified, the PES access point shall:

- Request the PES media gateway to detect the following events:
  - the **al/fl** event;
  - the **al/on** event.
- Report the occurrence of the off-hook event to the Feature Manager.
- Move the physical termination representing the called party's line to the context created during the previous step.
- Proceed to step 2.

If the no-answer timer (line free) or call-waiting-timer (line busy) expires, the PES access point shall:

- send a **Setup-Response** (no answer) primitive to the internal UA via the Feature Manager.
- Request the PES media gateway to stop the signal sent to the called party (ringing or call waiting signal).
- Request the PES media gateway to stop the signal sent to the calling party (ring back tone or the announcement).
- Initiate call clearing procedures.

#### Step 2

If the **al/fl** event is received from the PES media gateway, notify the Feature Manager using a **Feature Request** primitive.

On receipt of an internal **Session-Update** primitive, the PES access point shall modify the ephemeral termination properties accordingly.

If the **al/on** event is received from the PES media gateway, the PES access point shall:

- Initiate call clearing procedures.
- Report the occurrence of the on-hook event to the Feature Manager.

If a **Session-Release** primitive is received via the Feature Manager from the internal UA, the PES access point shall initiate call clearing procedures.

#### 7.3.1.3.2.2 Call Clearing

If the call clearing phase has been entered on receipt of an **al/on** event, the PES access point shall:

- send a **Session-Release** primitive to the internal SIP UA;
- request the PES media gateway to subtract the ephemeral termination;
- request the PES media gateway to move the physical termination back to the Null context.

If the call clearing phase has been entered on receipt of an internal **Session-Release** primitive, the PES access point shall:

- request the PES media gateway to subtract the ephemeral termination;
- request the PES media gateway to apply the off-hook warning tone (**xcg/roh**) to the physical termination;
- on receipt of the **al/on** event:
  - Request the PES media gateway to move the physical termination back to the Null context.
  - Report the occurrence of the on-hook event to the Feature Manager using a **Session-Release** primitive.

#### 7.3.1.4 Procedures for fax/modems calls over analog access

In order to be able to properly handle fax and modem calls, the PES access point requests the media gateway to monitor the **ctyp/dtone** event.

On receipt of a notification of the **ctyp/dtone** event, the AGCF notifies the Feature Manager if the recognized tone corresponds to a supported fax/modem. Otherwise, the event is discarded.

### 7.3.1.5 Message Waiting Indication

On receipt of a Service Notification internal primitive reporting the "message-summary" event, the PES access point requests the media gateway to apply the Generic Data Signalling signal of the **andisp** package defined in Recommendation H.248.23 [13]. The value of the TAS parameter is provisioned in the media gateway or in the PES access point, per media gateway or per line. Annex D specifies the populating rules for the Data Block parameter of the Generic Data Signalling signal.

### 7.3.2 PES Media Gateway

The PES media gateway shall support the procedures specified in ES 283 002 [5] appropriate to an MG.

## Annex A (normative): XML document structure for Dial Tone Management

Dial Tone Management documents are sub-trees or the *simservs* XML document defined in TS 183 023 [34]. The following schema shall be used to describe XML documents that specify the dial tone pattern applicable to an endpoint.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:ss="urn:org:etsi:ngn:params:xml:ns:simservs"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:org:etsi:ngn:params:xml:ns:simservs" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="dial-tone-management" substitutionGroup="ss:absService">
    <xs:annotation>
      <xs:documentation>Dial Tone Management
    </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
            <xs:element name="dial-tone-pattern" default="standard-dial-tone"
minOccurs="0">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="standard-dial-tone"/>
                  <xs:enumeration value="special-condition-tone"/>
                  <xs:enumeration value="message-waiting-tone"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:element>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

## Annex B (normative): AGCF internal communication

### B.1 General

The AGCF entity encompasses the functionality of a Media Gateway Controller (MGC) and of a SIP User Agent. The MGC functionality is involved in registration and session processing. The SIP UA functionality provides the interface to the other components of the IMS-based architecture and the NASS and the RACS, including procedures provided by a P-CSCF on behalf of endpoints. It is involved in registration and session processing as well as in event subscription/notification procedures between the AGCF and application servers. Within the AGCF, the MGC and SIP UA components are coordinated by a Feature Manager entity (see figure B.1).

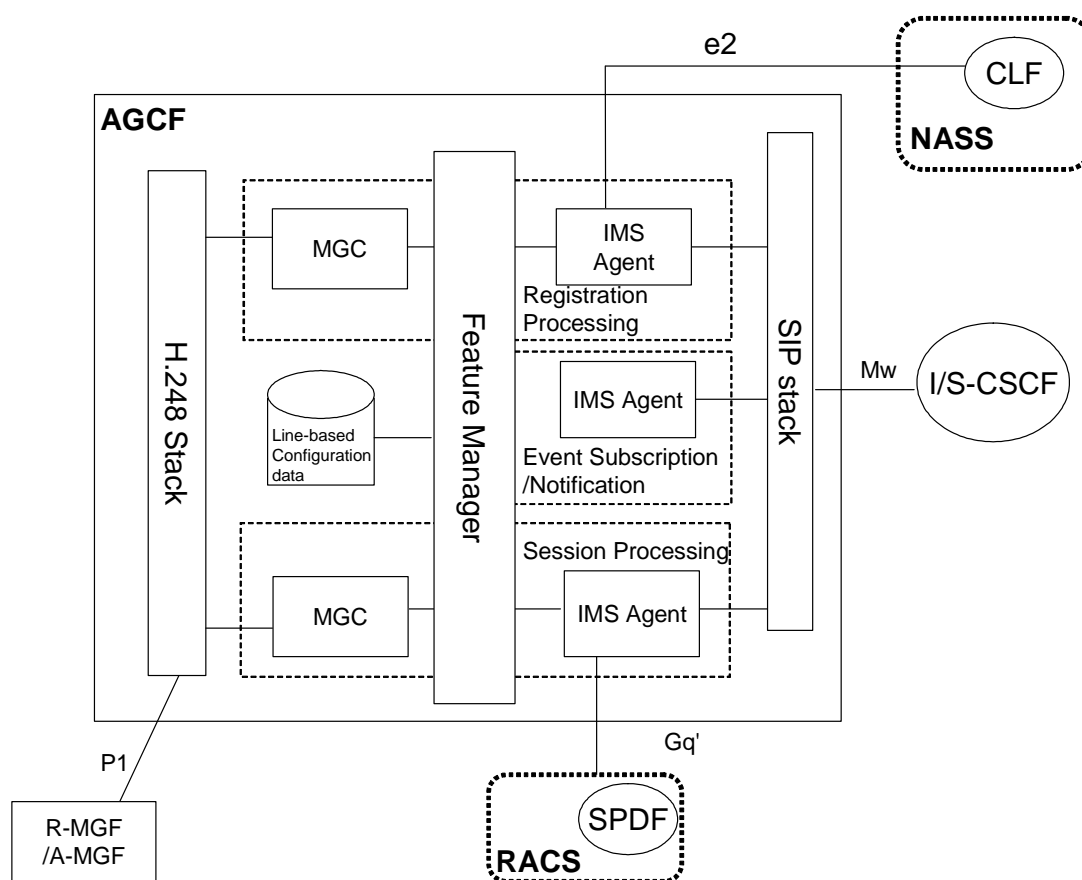
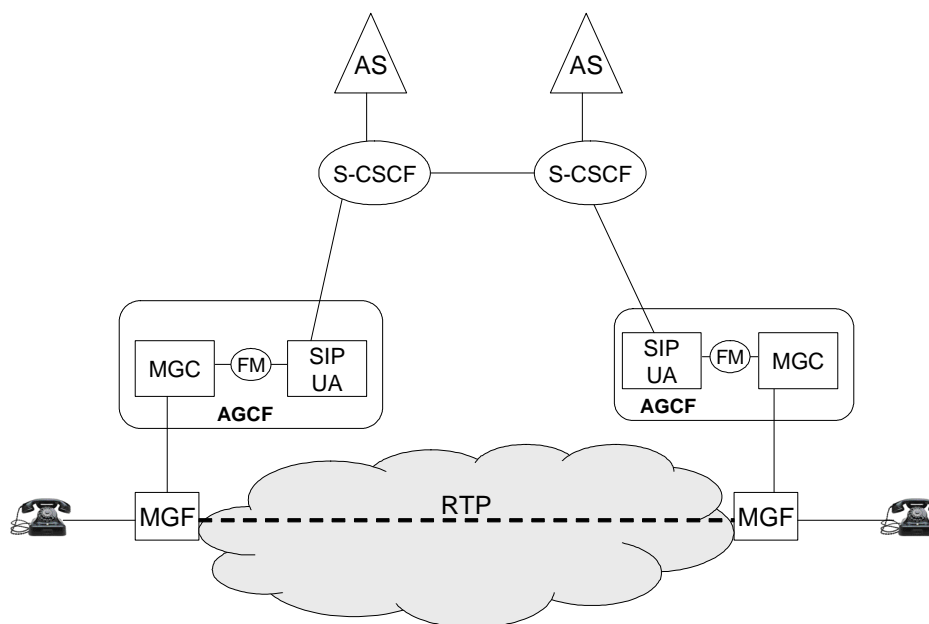


Figure B.1: AGCF functional model

### B.2 Internal communication principles

Session and registration processing in the AGCF involves two halves: H.248-based MGC processing and SIP User Agent (UA) processing (see figure B.2). MGC processing focuses on the interactions with the media gateway functions, while SIP UA processing focuses on the interactions with the IMS components. The Feature Manager (FM) coordinates the two processing activities.



**Figure B.2: AGCF session processing model**

## B.3 Internal primitives

The communication between the Feature Manager, MGC and SIP User Agent components of the AGCF is modelled using primitives. This modelling is used as an ease to describe the AGCF behaviour and is not intended to constrain implementations.

The following primitives are defined:

- **Service-Change:** This primitive is used by the MGC in the PES access point for reporting the ServiceChange event to the Feature Manager.
- **Register-Request:** This primitive is used by the Feature Manager for requesting the SIP User Agent to initiate appropriate SIP registration procedures on behalf of emulation users.
- **Deregister-Request:** This primitive is used by the Feature Manager for requesting the SIP User Agent to initiate appropriate SIP deregistration procedures on behalf of emulation users.
- **Session-Attempt:** This primitive is used to notify the Feature Manager of an outgoing call attempt.
- **Setup-Request:** This primitive is used to request establishment of a session.
- **Setup-Response:** This primitive is used to confirm the establishment of a session.
- **Session-Update:** This primitive is used to update a session description.
- **Session-Progress:** This primitive is used to report intermediate events during session establishment.
- **Session-Release:** This primitive is used to request the release of a session.
- **Feature-Request:** This primitive is used to report the occurrence of a service feature activation request from the user.
- **Charging-Indication:** This primitive is used to report the occurrence of a charging event.
- **Service-Notification:** This primitive is used to report the occurrence of a service notification.

## B.4 Feature manager behaviour

### B.4.1 Registration procedures

Based on the information received from the MGC in the PES access point side and local configuration data (mapping between line ids and IMS identities, authentication parameters...) the Feature Manager requests the SIP UA component to initiate appropriate SIP registration procedures (per line registration, "en bloc" registration etc.).

#### B.4.1.1 Global registration procedures

On receipt of a ServiceChange internal primitive indicating "restart", the Feature Manager sends one or more Register-Request primitives to the SIP UA.

On receipt of a ServiceChange internal primitive indicating "forced" or "graceful", the Feature Manager sends one or more Deregister-Request primitives to the SIP UA.

The number of primitives sent to the SIP UA depends on the AGCF configuration with regards to identity management. The following two cases are identified and lead to different procedures:

- One private user identity is assigned to the AGCF (or each MGF) – Each termination connected to the MG is represented by one public user identity.
- A pair of private and public user identity is associated with each termination connected to the MGs controlled by the AGCF.

In the first case, the Feature Manager sends a single primitive with the private user identity associated with the AGCF (or the MGF) and one of the public user identities. All other public user identities will be implicitly registered or deregistered using implicit registration procedures defined in ES 283 003 [4].

In the second case, the Feature Manager sends one primitive for each termination connected to the MGF that caused the service change event.

#### B.4.1.2 Per line registration procedures

There may a lot of terminations to register and deregister at the same time from the MGC side. In order to avoid the impact of the flood registration and deregistration on the IMS core network, the Feature Manager may use some mechanism to control the number of registration/deregistration during a specified period of time.

##### B.4.1.2.1 User-initiated registration

On receipt of a **Service-Change** primitive from the MGC component with ServiceChangeMethod parameter set to "Restart" indicating that service will be restored on the specified Terminations, the Feature Manager shall:

- According to the MGF address and the TerminationIDs, lookup the configured data for the public user identities and the private user identities of the related users.
- If the related users have not been registered, use a Register-Request primitive to request the SIP UA to initiate appropriate SIP registration procedures.

##### B.4.1.2.2 User-initiated deregistration

On receipt of a Service-Change primitive from the MGC component with ServiceChangeMethod parameter set to "Graceful" or "Forced" indicating that the specified Terminations will be taken out of service, the Feature Manager shall:

- According to the MGF address and the TerminationIDs, lookup the configured data for the public user identities and the private user identities of the related users.
- If the related users have been registered, use a Deregister-Request primitive to request SIP UA to initiate appropriate SIP deregistration procedures.

### B.4.1.2.3 Exception procedures

On receipt of a Service-Change primitive from the MGC component indicating that the communication between the AGCF and the MGF has been lost, the Feature Manager shall use the Deregister-Request primitive to request the SIP UA to initiate appropriate SIP deregistration procedures for all the registered users belong to the MGF.

## B.4.2 Call Processing

### B.4.2.1 General procedures

The Feature Manager processes internal events received from the MGC side and request the SIP UA to generate the appropriate SIP messages based on the mapping described in table B.1.

**Table B.1: Mapping from MGC side to SIP UA side**

Internal primitive	SIP message
Setup Request	INVITE
Session Progress (alerting)	180 Ringing
Setup Response (no Answer)	480 (Temporary Not Available)
Setup Response (answer)	200 OK
Setup Response (busy)	486 Busy Here
Setup Response (reject)	606 Not Acceptable
Feature Request	re-INVITE
Release	BYE

The Feature Manager processes SIP messages received from the SIP UA side and transmit appropriate internal primitives to the MGC side, based on the mapping described in table B.2.

**Table B.2: Mapping from SIP UA side to MGC side**

SIP message	Internal primitive
INVITE	Setup Request
183 Session Progress	Session Progress
180 Ringing	Session Progress(alerting)
200 OK	Setup Response (answer)
603 (Decline), 408 (Request Timeout), 480 (Temporary Not Available)	Setup Response (no answer)
Other 4xx, 5xx, 6xx	Setup Response (failure)
486 (Busy Here) , 600 (Busy Everywhere)	Setup Response (busy)
re-INVITE with SDP, UPDATE	Session Update (SDP)
REFER	Session Update (refer)
INFO (charging) or NOTIFY (charging)	Charging Indication
NOTIFY (other)	Service Notification
BYE	Release

### B.4.2.2 Flash-Hook Management

#### B.4.2.2.1 General rules

Processing flash-hook event notifications depends on the call configuration:

*Call Configuration: 1-party*

In this configuration, an unconfirmed INVITE dialog exists between the SIP UA and another endpoint.

On receipt of a flash-hook notification from the MGC component, the Feature Manager shall request the MGC component to interact with the media gateway in order to play a dial tone and collect digits.

If the digit collection succeeds, the Feature Manager shall request the SIP UA to send an INVITE request to the PES application server, with the collected digits as Request-URI. Otherwise, the events shall be discarded.



*Call Configuration : Stable 2-party*

In this configuration, one confirmed INVITE dialog exists between the SIP UA and another endpoint.

On receipt of a flash-hook notification from the MGC component, the Feature Manager shall:

- Request the SIP UA to send a re-INVITE request towards the connected party (B party). The re-INVITE request is built as follows:
  - The Request URI is set to the B party's identity.
  - The SDP description for the active media stream is set to a=sendonly.

NOTE 1: This information may be used by an AS to request the sending of an announcement to the B Party.

- Request the MGC component to initiate an outgoing call process as if an off-hook event had been received.

*Call Configuration : Stable 2-party call with additional held/waiting party*

In this configuration, a confirmed INVITE dialog exists between the SIP UA and some other endpoint (the "active party", and either an unconfirmed dialog exists with a third endpoint (the "waiting party") or another confirmed dialog exists with a third party that is on hold ("held party").

On receipt of a flash-hook notification from the MGC component, the Feature Manager shall request the MGC component to interact with the media gateway in order to:

- Set the stream mode of the ephemeral termination to "inactive".
- Play a dial tone.
- Collect a feature code.

The number of digits is provisioned in the AGCF. The AGCF shall also send a re-INVITE request on the initial dialogue to hold the associated media stream, as described in TS 183 010 [8].

NOTE 2: This information may be used by an AS to request the sending of an announcement to the B Party.

Processing of the feature code depend on whether loose or tight coupling procedures are applied between the AGCF and the AS. The decision to use tight coupling or loose coupling is left to the network operator. However, it is important that both the AGCF and the PES application server are configured the same way.

**B.4.2.2.2 Loose coupling procedures**

With loose coupling, the AGCF provides call processing logic to manipulate call legs, much like a simulation endpoint would operate.

The Feature Manager analyses the feature code according to a local mapping table. For each feature code, this table indicates the user expected feature:

- The served user wishes to be connected to a particular held/waiting party and keep the other party held/waiting.
- The served user wishes to be connected to a particular held/waiting party and release the other party.
- The served user wishes to establish a 3-party conference with both of the other parties.

If the feature code received from the internal MGC component does not match any known feature, the FM ignores the feature code and optionally requests the MGC component to interact with the media gateway in order to play an error tone or an announcement to the served user.

If the feature code received from the internal MGC component indicates that the served user wishes to be connected to a particular held/waiting party, the Feature Manager shall:

- Request the SIP UA to send either:
  - A 200 OK response to the INVITE request received from the waiting party if the dialogue is not confirmed yet; or
  - A re-INVITE request if the dialogue with the held party is already confirmed. The Re-INVITE request is built as follows:
    - The Request URI is set to the held party's identity.
    - The SDP description for the active media stream is set to a=sendrecv.
- Request the MGC component to interact with the media gateway in order to:
  - Modify the Remote Descriptor of the ephemeral termination according to the SDP information received from the held/waiting party.
  - Set the Stream Mode of the ephemeral termination to sendrecv.
  - Monitor the flash-hook event on the physical termination.

If the feature code received from the internal MGC component indicates that the served user wishes to release the call with the other held/waiting party, the Feature Manager shall:

- Request the SIP UA to send a 603 response or a BYE request to the waiting/held party depending on the dialogue state.
- Request the MGC component to interact with the media gateway in order to monitor the flash-hook event on the physical termination.

If the feature code received from the internal MGC component indicates that the served user wishes to establish a 3-party conference, the Feature Manager shall:

- Request the MGC component to interact with the media gateway in order to add a termination to the current context based on SDP information associated with the initial held party (i.e. the party that was already held before the flash-hook has been detected).
- Request the SIP UA to send a re-INVITE request towards each of the held/waiting parties. The re-INVITE request is built as follows:
  - The Request URI is set to the held/waiting party's identity.
  - The SDP description for the active media stream is set to a=sendrecv. The address and port are set according to the contents of the local descriptor of the termination representing this party on the media gateway.

#### B.4.2.2.3 Tight coupling procedures

With tight coupling procedures, all collected digits are reported to the PES application server and the AS determines the appropriate call processing actions to take. Manipulation of call legs for call waiting and 3-party calls is managed by the AS, so feature logic for these services is not required in the AGCF. Unlike loose coupling, where a flash-hook notification must be followed by dialled digits in order for the AGCF to generate an INVITE request, tight coupling procedures support the reporting of a flash-hook event even when no additional digits are dialled by the user.

The Feature Manager shall request the SIP UA to create a new dialogue and send an INVITE request to the Application Server, built as follows:

- The Request URI is structured as follows:
  - A user part containing a provisioned prefix followed by collected digits. If no digits were collected following the flash-hook notification, the request URI sent to the AS shall contain a unique user part that signifies that a flash-hook without additional digits was detected (such as [flash@pes-scc.operator.com](mailto:flash@pes-scc.operator.com)).

- A domain name which together with the user part provides sufficient information to the S-CSCF to forward the INVITE request to the appropriate AS, based on Initial Filter Criteria stored in the user profile (see annex C).
- A P-Asserted-Identity containing the public identity of the subscriber requesting the service.
- An SDP offer for a voice call.

The Feature Manager shall request the MGC component to interact with the media gateway in order to modify the H.248 Remote Descriptor and stream mode according to the SDP information received in re-INVITE messages sent by the Application Server.

Release of the dialogue opened for the purpose of sending the feature code is the responsibility of the application server.

---

## Annex C (Informative): Implementation of Supplementary Services

### C.1 General principles

#### C.1.1 Introduction

This annex describes guiding principles for implementing commonly deployed PSTN supplementary services using the IMS-based PES architecture. The list of services is taken from EG 201 973-2 [11].

The actual service logic resides in the Application Server and is outside the scope of standardization. This annex focuses on the interactions between the AGCF and PES application servers. Only the part of the service logic which has an impact on signalling to/from the AGCF is described in this annex. Similar procedures may also be used in case of analog lines connected to a VGW acting as a UE with regard to a P-CSCF in the PES.

AGCF involvement in the execution of these services is limited to the generic capabilities described in the main body of the present document for supporting interworking between SIP and H.248 protocols and in annex B for processing flash-hook events.

#### C.1.2 Supplementary service control

This annex assumes that subscribers can control their supplementary services using service code commands and switching order commands as defined in ETS 300 738 [12].

More than one command can be dialled on a single call. For instance, a caller may dial the "inhibit call waiting" command, followed by the "calling line identity restriction" command, followed by a the called party number.

##### C.1.2.1 Service code commands

Service codes commands are user requests to perform an action that does not result in a call to another party. Actions such as feature activation, feature deactivation, and feature status inquiries are triggered by service code commands.

###### C.1.2.1.1 Command syntax

The format of service code commands as defined in ETS 300 738 [12] is reproduced below:

**"START PX SC (SR SI) SX" or "PX SC (SR SI) SX FINISH"**

Where:

- **START** is the start command, e.g. "Off-hook", an alternative to the finish command;
- **PX** is a mandatory service prefix;
- **SC** is a mandatory service code;
- **SR** is one or more separator/s, as required;
- **SI** is one or more units of supplementary information, as required;
- **SX** is a service suffix as required;
- **FINISH** is a finish command, e.g. SEND, an alternative to the start command.

NOTE: Digit maps used by the media gateways to collect digits shall include appropriate alternatives to cope with the syntax of service code commands.

### C.1.2.1.2 Generic procedure at the AGCF side

On receipt of a service code command from a media gateway, the AGCF sends an INVITE request to the S-CSCF with the following information:

- A Request-URI structured as follows:
  - A user part containing the service code command, excluding the START and FINISH fields.
  - A domain name which together with the user part provides sufficient information to the S-CSCF to forward the INVITE request to the appropriate AS, based on Initial Filter Criteria stored in the user profile, e.g.

["PX SC \(SR SI\) SX"@pes-scc.operator.com](#)

NOTE 1: If the service code command includes a square "#" symbol, the userinfo portion of the Request-URI shall be in the form of a telephone-subscriber. The series of digits that form the service code command shall be encoded as a local-number. The phone-context attribute shall be set to a domain name of the PES operator, e.g. phonecontext=pes-scc.homedomain.com that is specific enough to enable the application server to interpret the commandcode. Setting the phone-context attribute is required for conformance purposes with RFC 3966 [19]. PES network entities (e.g. CSCF) ignore this attribute.

- A P-Asserted-Identifier header containing the public user identity of the subscriber issuing the service code command.
- An SDP offer for a voice call.

NOTE 2: The SDP offer may be used by the Application Server in case an announcement has to be delivered.

### C.1.2.1.3 Generic procedure at the AS side

On receipt of the INVITE request that includes a service code command as Request-URI, the AS sends back a 183 (Session Progress) message.

NOTE: An SDP Answer may be included in the 183 (Session Progress) response in case the user is expected to key-in additional digits before the procedure can be completed. In such cases, the AS requests an MRFC/MRFP to play an appropriate prompting announcement and collect digits. The procedure for supporting user interactions during the call establishment phase is described within TS 183 028 [6].

If the procedure identified by the service code command is successfully performed, the AS modifies the subscriber profile according to the service code received, requests an MRFC/MRFP to play a positive acknowledgment tone or announcement and sends a 200 OK response towards the AGCF when the MRFC is connected. If the service code command corresponds to an interrogation procedure, the AS selects the appropriate announcement to notify the requested information (e.g. current supplementary service status) to the calling user. Release of the dialogue occurs when a BYE request is received from the MRFC or if a BYE/CANCEL request is received from the AGCF.

If the procedure identified by the service code command cannot be performed successfully, the AS requests an MRFC/MRFP to play a negative acknowledgment tone or announcement and releases the call by sending a suitable 4xx or 5xx response to the INVITE request or by sending a BYE request if the dialogue is already established. The procedure for sending a tone or an announcement during the call establishment phase is described within TS 183 028 [6].

### C.1.2.2 Switching order commands

Switching order commands are typically used to invoke a service or modify the characteristics of a call, such as a request to invoke the automatic call return service, or a request to inhibit call waiting on the call that is about to be placed.

The format of switching order commands (SOC) is reproduced below:

**"START SO (SR SI)" or "SO (SR SI) FINISH"**

Where:

- **START** is a start command, e.g. "Register Recall (R)", an alternative to the finish command, as required;
- **SO** is a mandatory switching order;
- **SR** is one or more separators, as required;
- **SI** is one or more units of supplementary information, as required;
- **FINISH** is a finish command, e.g. "send", an alternative to the start command, as required.

Processing of switching order commands where the start command is a Register Recall (also known as Flash-Hook event) is described in annex B. Processing of the Register Recall at the AGCF depends on the call configuration and usually involves requesting the media gateway to deliver a dial tone and collect digits.

### C.1.3 Setting of initial filter criteria

Emulation of PSTN services requires that Initial Filter Criteria stored in the user profile be set on the following methods:

- Originating INVITE methods.
- Terminating INVITE methods.
- Terminating MESSAGE methods.

The user profile is selected based on the contents of the P-Asserted-Identity (originating method) or Request-URI (terminating method) headers.

How many Initial Filter Criteria are actually required depend on how many application servers are involved in the provision of these services.

When several application servers are involved, each implementing a particular service set or feature set, other service point triggers (SPT) may be added to Initial Filter Criteria so as to route the SIP messages to the appropriate server, in the right order.

In case of outgoing calls (including special calls for service control purposes), the Request-URI may typically be part of an Initial Filter Criteria. The content tag will typically contain an Extended Regular Expressions (ERE) as defined in clause 9 in IEEE 1003.1-2004 Part 1 such that any Request-URI that includes a particular pattern (e.g. a domain name) matches the criteria.

The following example illustrates the case of an IFC used to trigger an application server dedicated to the processing of service code commands, assuming that the AGCF appends the pes-scc.homedomain.com domain name to the service code commands.

```
<InitialFilterCriteria>
  <Priority>0</Priority>
  <TriggerPoint>
    <ConditionTypeCNF>0</ConditionTypeCNF>
    <SPT>
      <ConditionNegated>0</ConditionNegated>
      <Group>0</Group>
      <Method>INVITE</Method>
    </SPT>
    <SPT>
      <ConditionNegated>0</ConditionNegated>
      <Group>0</Group>
      <RequestURI>@pes-scc.homedomain.com$</RequestURI>
    </SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:PES-AS1@homedomain.com</ServerName>
    <DefaultHandling>0</DefaultHandling>
```

```
</ApplicationServer>
</InitialFilterCriteria>
```

## C.1.4 Supplementary services using ISUP information

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

**Table C.1: Supplementary Service References**

Supplementary Service	ETSI/ITU-T Reference
Calling Line Identification Presentation (CLIP)	EN 300 356-3 [35]
Calling Line Identification Restriction (CLIR)	EN 300 356-4 [35]
Connected Line Identification Presentation (COLP)	EN 300 356-5 [35]
Connected Line Identification Restriction (COLR)	EN 300 356-6 [35]
Terminal Portability (TP)	EN 300 356-7 [35]
User-to-User Signalling (UUS)	EN 300 356-8 [35]
Closed User Group (CUG)	EN 300 356-9 [35]
Subaddressing (SUB)	EN 300 356-10 [35]
Malicious Call Identification (MCID)	EN 300 356-11 [35]
Conference Call (CONF)	EN 300 356-12 [35]
Explicit Call Transfer (ECT)	EN 300 356-14 [35]
Call Forwarding Busy (CFB)	EN 300 356-15 [35]
Call Forwarding No Reply (CFNR)	EN 300 356-15 [35]
Call Forwarding Unconditional (CFU)	EN 300 356-15 [35]
Call Deflection (CD)	EN 300 356-15 [35]
Call Hold (HOLD)	EN 300 356-16 [35]
Call Waiting (CW)	EN 300 356-17 [35]
Completion of Calls to Busy Subscriber (CCBS)	EN 300 356-18 [35]
Three-Party (3PTY)	EN 300 356-19 [35]
Completion of Calls on No Reply (CCNR)	EN 300 356-20 [35]
Anonymous Communication Rejection (ACR)	EN 301 798 [40]
Multi-Level Precedence and Pre-emption (MLPP)	ITU-T Recommendation Q.735.3 [36]
Global Virtual Network Service (GVNS)	ITU-T Recommendation Q.735.6 [37]
Reverse charging (REV)	ITU-T Recommendation Q.736.3 [38]

---

## C.2 Advice of Charge

### C.2.1 Actions at the Originating AGCF

The AGCF converts charging pulses received from the Application Server (via the S-CSCF) into appropriate signals of the H.248 **amet** package.

Generation of the Advice Of Charge message (see EN 200 659-3 [10]) by the AGCF is described in annex D.

### C.2.2 Actions at the Originating AS

Implementation of this service assumes that the AS providing the service is involved in all outgoing calls for which advice of charge information is expected (e.g. all outgoing calls, all outgoing international calls,...). It is the responsibility of the network operator to configure the appropriate Initial Filter Criteria in the user profile.

Charging pulses are transmitted from the Application Server to the AGCF using the method described in [7]. It is the responsibility of the AS to ensure that the information contained in these messages is in the form of a number of units.

## C.2.3 Actions at the Terminating AGCF

Not applicable.

## C.2.4 Actions at the Terminating AS

Not applicable.

---

# C.3 Anonymous Call Rejection

## C.3.1 Actions at the Originating AGCF

This service does not require the originating AGCF to perform any specific action.

## C.3.2 Actions at the Originating AS

This service does not require the originating AS to perform any specific action.

## C.3.3 Actions at the Terminating AS

If the service is activated, the terminating AS rejects the call if the P-Asserted-Identity header field is absent or if the Privacy header field indicates "id", "header", "user" or "critical" as specified in RFC3325. In all other cases the communication proceeds normally.

When the AS rejects a communication, the AS sends an indication to the calling user by sending a 433 (Anonymity Disallowed) response. Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure for invoking an announcement in the call establishment phase is described within TS 183 028 [6].

As a service option the ACR service may forward the communication to a voice message service instead of rejecting the communication with a 433 (Anonymity Disallowed) final response.

## C.3.4 Actions at the Terminating AGCF

The terminating AGCF is not involved in the execution of this service.

---

# C.4 Automatic Call Return

## C.4.1 Actions at the AGCF at the invoker side

The Automatic Call Return service is invoked using a service code command. On receipt of this service code command, the AGCF builds an INVITE request as described in clause C.1

## C.4.2 Actions at the AS at the invoker side

Implementation of this service assumes that the AS providing the service is involved in all incoming calls to the served user. It is the responsibility of the network operator to configure the appropriate Initial Filter Criteria in the user profile. The AS keeps track of the most recent incoming call to each served user it manages.



When receiving the service code command that identifies the Automatic Call Return service, the AS acts as a B2BUA and establishes a new call leg to the most recent caller (i.e. it sends an INVITE messages towards this most recent call party as if the number had been dialled by the served user).

---

## C.5 Calling Line Identity Presentation / Restriction

### C.5.1 Actions at the Originating AGCF

A service code command may be received by the AGCF in case the calling user wishes to override the default setting for a particular call, in which case the called party number is embedded in the command code as part of the supplementary information. The AGCF generates an INVITE request according to the rules described in clause C.1.

Otherwise the originating AGCF is not involved in the provision of this service.

### C.5.2 Actions at the Originating AS

The AS determines whether calling identification shall be presented or restricted based on user profile data (permanent mode) or based on the contents of the Request-URI (per-call mode).

Any service prefix is removed from the Request-URI before forwarding the INVITE request toward the called party.

If calling identification restriction is in force, the AS shall apply the following changes before forwarding the received INVITE request towards the called party via the S-CSCF:

- Override the contents of the From header field with an "anonymous" indication. The convention for configuring an anonymous From header field described in RFC 3323 [24] and RFC 3325 [25] should be followed; i.e.

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag= xxxxxxx.

- Include a Privacy header field set to "header" in accordance with RFC 3323 [24], and RFC 3325 [25].

On receipt of an INVITE request with a service code command requesting that the calling line identity be presented to the called party, the AS removes the service prefix from the service code command and forwards the INVITE request unchanged towards the called party, via the S-CSCF.

Otherwise the originating AS is not involved in the provision of this service.

### C.5.3 Actions at the Terminating AS

If the service is subscription dependent and the called user has not subscribed to the service, the terminating AS removes any P-Asserted-Identity and Privacy header fields included in the request. Additionally, the Application Server may as a network option set the contents of the From header to a default non significant value.

If the request includes the Privacy header field set to "header" the AS set the contents of all headers containing private information in accordance with RFC 3323 [24] and RFC 3325 [25].

If the request includes the Privacy header field set to "user" the AS removes or set the contents of all "user configurable" headers in accordance with RFC 3323 [24] and RFC 3325 [25]. In the latter case, the AS may need to act as transparent back-to-back user agent as described in RFC 3323 [24].

- NOTE: If the request includes the Privacy header field set to "id", the P-Asserted-Identity header is removed by the S-CSCF.

## C.5.4 Actions at the Terminating AGCF

User Identification information received in an INVITE request ("P-Asserted-Id" and "From" headers) is used by the AGCF to generate the appropriate Call Setup message (see EN 200 659-3 [10]) to be delivered to the called terminal, using the H.248 **andisp** package. Generation of the Call Setup message is further described in annex D.

---

## C.6 Calling Name Delivery

### C.6.1 Actions at the Originating AGCF

No specific action is performed by the AGCF.

### C.6.2 Actions at the Originating Application Server

If the calling user has subscribed to the service and no presentation restriction is invoked, the originating AS shall insert a pre-configured calling name in the Display field of the From header and possibly the same or different name in the Display field of the P-Asserted-Identifier header.

### C.6.3 Actions at the Terminating Application Server

If the service is subscription dependent and the called user has not subscribed to the service, the terminating AS removes or the From header or set its contents in accordance with RFC 3323 [24].

If the request includes the Privacy header field set to "header" the AS sets the contents of all headers containing private information in accordance with RFC 3323 [24] and RFC 3325 [25].

If the request includes the Privacy header field set to "user" the AS removes or sets the contents of all "user configurable" headers in accordance with RFC 3323 [24] and RFC 3325 [25]. In the latter case, the AS may need to act as transparent back-to-back user agent as described in RFC 3323 [24].

### C.6.4 Actions at the Terminating AGCF

User Name information received in an INVITE request ("From" header /or "P-Asserted-Identifier") is used by the AGCF to generate the appropriate Call Setup message (see EN 200 659-3 [10]) to be delivered to the called terminal, using the H.248 **andisp** package. Generation of the Call Setup message is further described in annex D.

---

## C.7 Call Forwarding

### C.7.1 Activation/Deactivation/Interrogation

#### C.7.1.1 Actions at the AGCF

Registration, Erasure, Activation, Deactivation and Interrogation of call forwarding services is performed using service code commands as described in ETS 300 738 [12].

On receipt of a service code command that corresponds to one of these procedures, the AGCF sends an INVITE request as described in clause C.1.

#### C.7.1.2 Actions at the AS

On receipt of the INVITE request that includes a service code command as Request-URI, the AS proceeds as described in clause C.1.

In case of unconditional call forwarding the AS may also send a NOTIFY request to the AGCF to update the Dial Tone Management XML document.

## C.7.2 Invocation

### C.7.2.1 Actions at the Originating AGCF

No specific action is performed by the AGCF.

### C.7.2.2 Actions at the Originating AS

No specific action is performed by the AS.

### C.7.2.3 Actions at the Forwarding AS

The AS implements procedures identical or similar to those described in TS 183 004 [9].

### C.7.2.4 Actions at the Forwarding AGCF

The AGCF at the forwarding side is not involved in the processing of forwarded calls.

### C.7.2.5 Actions at the Terminating AS

No specific action is performed by the AS.

### C.7.2.6 Actions at the Terminating AGCF

Call forwarding information received in an INVITE request ("history-info" header) is used by the AGCF to generate the appropriate Call Setup message (see EN 200 659-3 [10]) to be delivered to the called terminal, using the H.248 **andisp** package. Generation of the Call Setup message is further described in annex D.

---

## C.8 Distinctive Ringing

### C.8.1 Actions at the Originating AGCF

This service does not require the originating AGCF to perform any specific action.

### C.8.2 Actions at the Originating Application Server

This service does not require the originating AS to perform any specific action.

### C.8.3 Actions at the Terminating Application Server

The terminating AS inserts an "alert-info" header in the INVITE request with a value selected based on the value of the P-Asserted-Identity header received in the incoming INVITE request and on the called user profile.

### C.8.4 Actions at the Terminating AGCF

The terminating AGCF uses the value of the "alert-info" header to select the appropriate ring pattern. The pattern identifier is sent to the media gateway as a parameter of the H.248 **andisp/dwa** signal.

---

## C.9 Call Waiting

### C.9.1 General

#### C.9.1.1 Actions at the AGCF at the terminating side

On receipt of an INVITE request for a busy subscriber, the AGCF performs the following actions:

- Request the media gateway to apply call waiting tone using the H.248 **andisp/dwa** signal.
- Request the media gateway to monitor flash-hook events.
- Send a 180 (Alerting) towards the AS.
- Start a no answer timer.

If the no answer timer expires the AGCF sends a 486 (Busy Here) response towards the Application Server.

If a flash-hook event is reported by the media gateway, the AGCF stops the no-answer timer and requests the media gateway to perform the following actions:

- Set the stream mode of the ephemeral termination to inactive.
- Apply a dial tone.
- Collect a switching order command.

NOTE 1: In some networks, applying a dial tone and collecting an explicit switching order command is not required as the register recall is interpreted as a request to accept the waiting call. Subsequent AGCF procedures are executed as if an equivalent switching order command had been received from the user.

The number of digits is provisioned in the AGCF. The AGCF also sends a re-INVITE request on the initial dialogue to hold the associated media stream, as described in TS 183 010 [8].

Processing of the switching order command depend on whether loose or tight coupling procedures are applied between the AGCF and the AS. Figure C.1 illustrates the loose coupling case while figure C.2 illustrates the tight-coupling case.

NOTE 2: These figures do not take into account all possible service code commands that may be received from the user (e.g. service code command requesting that a waiting call be accepted and the active call be released).

#### C.9.1.2 Actions at the AS at the terminating side

Implementation of this service assumes that the AS providing the service is involved in all calls to/from the subscriber.

The AS determines whether the called user is busy based on the procedures described in TS 183 028 [6].

If the called user is busy and has not subscribed to the call waiting service, the AS sends a 486 (Busy Here) response towards the calling party.

If the called user is busy and has subscribed to the call waiting service, the AS builds an INVITE request using normal rules as for any incoming call.

On receipt of a re-INVITE request with a SDP "sendonly" attribute, the AS interacts with an MRFC in order to play an announcement to the held party, in accordance with TS 183 028 [6].

## C.9.2 Option 1 (Loose coupling)

### C.9.2.1 Actions at the AGCF at the terminating side

The AGCF evaluates the Switch Order Command based on a provisioned mapping table.

If the SOC indicates that the served user wishes to be connected to the waiting party, the AGCF performs the following actions:

- Send a 200 OK response to the INVITE request received from the waiting party.
- Request the media gateway to.
- Modify the Remote Descriptor of the ephemeral termination according to the SDP information received from the waiting party.
- Monitor the flash-hook event.

If SOC indicates that the served user wishes to reject the waiting call, the AGCF performs the following actions:

- Send a provisioned error response code (e.g. 603) to the INVITE request received from the waiting party.
- Request the media gateway to.
- Set the stream mode to send-receive.
- Monitor the flash-hook event.
- Send an re-INVITE request towards the held party (i.e. the party that has been held for the purpose of collecting the switching order command). The re-INVITE request is built as follows:
  - The Request-URI is set to the held party's identity.
  - The SDP description for the active media stream is set to a=sendrecv.

Once the communication is established with the waiting party, the user may decide to switch back to the initial party, using a Register Recall followed by new switching order command. Depending on the value of the switching order command, the AGCF performs one of the following set of actions:

- Send an re-INVITE request towards the held party. The re-INVITE request is built as follows:
  - The Request-URI is set to the held party's identity.
  - The SDP description for the active media stream is set to a=sendrecv.
- Send an re-INVITE request towards the active party. The re-INVITE request is built as follows:
  - The Request URI is set to the active party's identity.
  - The SDP description for the active media stream is set to a=sendonly.
- Request the media gateway to:
  - Modify the Remote Descriptor of the ephemeral termination according to the SDP information associated with the held party.
  - Monitor the flash-hook event.

The user may also be willing to establish a 3-party conference. On receipt of a Switch Order Command indicating that a conference shall be established, the AGCF performs the following actions:

- Request the media gateway to add a termination to the current context based on SDP information associated with the held party.

- Send a re-INVITE request towards the first held party (i.e. the party that was already held when the flash-hook event has been detected). The re-INVITE request is built as follows:
  - The Request URI is set to the held party's identity.
  - The SDP description is set to a=sendrecv. The address and port are set according to the contents of the local descriptor of the new termination.
- Send a re-INVITE request towards the second held party (i.e. the party that has been held for the purpose of collecting the Switch Order Command). The re-INVITE request is built as follows:
  - The Request URI is set to the held party's identity.
  - The SDP description is set to a=sendrecv.

If the feature code received from the internal MGC component does not match any known feature, the AGCF ignores the feature code and optionally request the media gateway to play an error tone or an announcement to the served user.

### C.9.2.2 Actions at the AS at the terminating side

On receipt of a re-INVITE request with a SDP attribute "sendonly", the AS interacts with an MRFC in order to play an announcement to the held party, in accordance with TS 183 028 [6].

On receipt of a re-INVITE request with the SDP attribute "sendrecv", the AS interacts with the MRFC to stop any ongoing announcement.

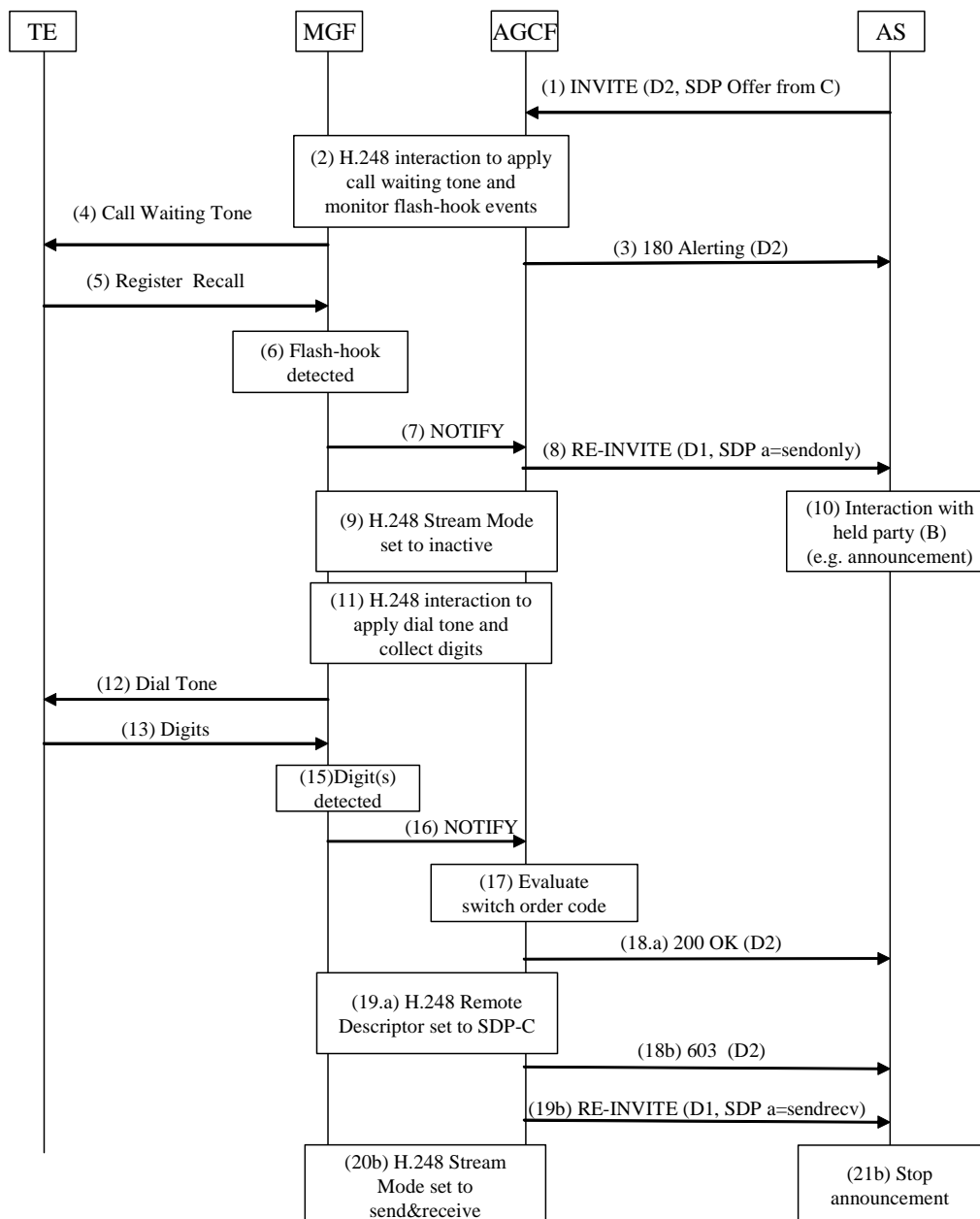


Figure C.1: Call Waiting with loose AGCF/AS coupling

## C.9.3 Option 2 (Tight coupling)

### C.9.3.1 Actions at the AGCF at the terminating side

The AGCF sends a re-INVITE request to the Application Server, built as follows:

- The Request URI is structured as follows:
- A user part containing a provisioned prefix followed by the switching order command without the start and finish fields.

NOTE: In networks where no explicit SOC is collected, a preconfigured SOC is used to populate the user part.

- A domain name that provides sufficient information to the S-CSCF to forward the INVITE request to the appropriate AS, based on Initial Filter Criteria stored in the user profile, e.g.

**SOC- "SO (SR SI)"@pes.operator.com**

- A P-Asserted-Identity containing the public identity of the subscriber issuing the switching control command.
- An SDP offer for a voice call.

The AGCF modifies the H.248 Remote Descriptor and stream mode according to the SDP information received in re-INVITE messages sent by the Application Server.

### C.9.3.2 Actions at the AS at the terminating side

The AS evaluates the Switch Order Command based on the current call configuration and issues appropriate re-INVITE messages. A CANCEL request is sent on the dialogue associated with the waiting call.

The AS interacts with an MRFC in order to play and stop announcements to the held party, in accordance with TS 183 028 [6].



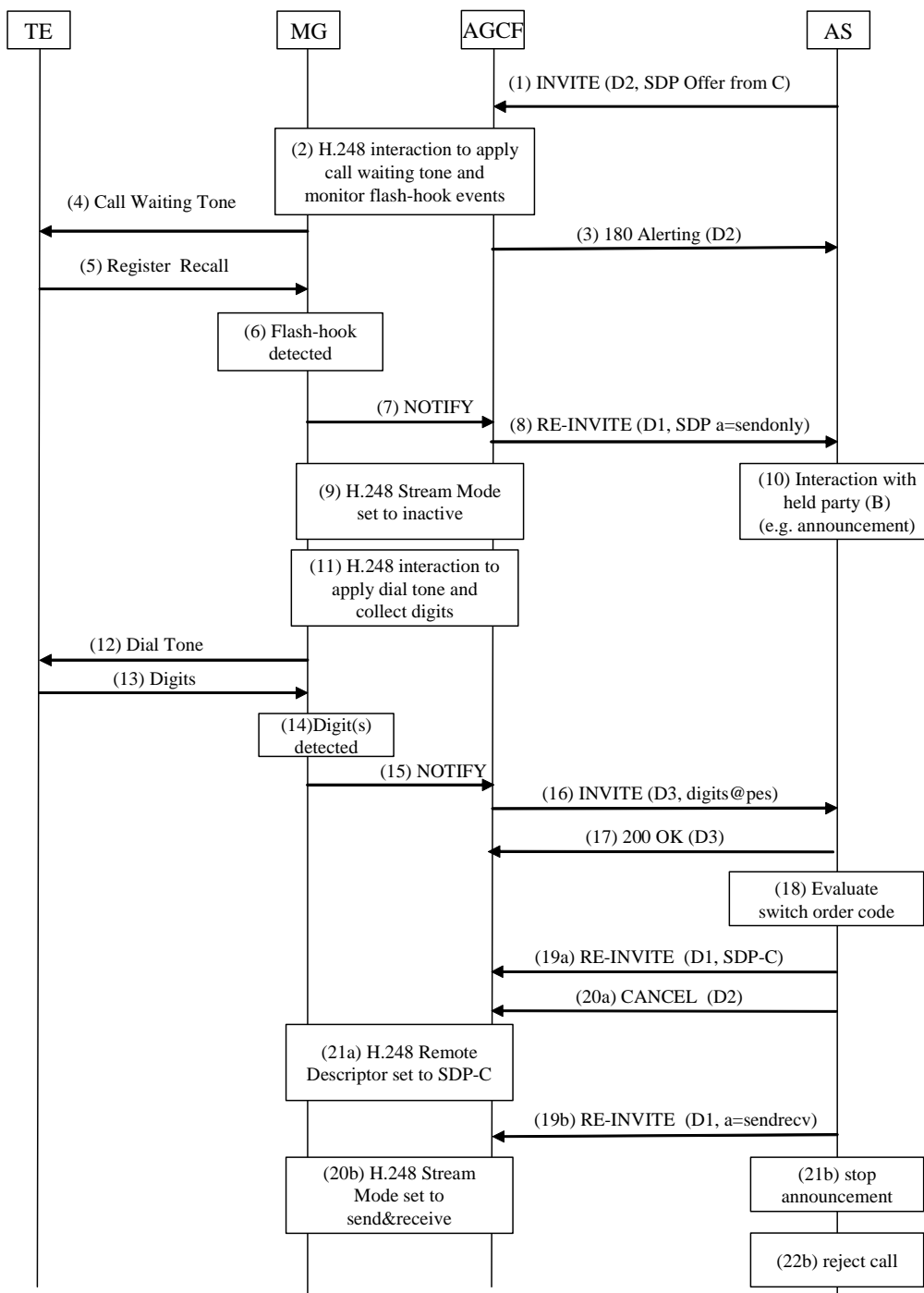


Figure C.2: Call Waiting with tight AGCF/AS coupling

---

## C.10 Incoming Call Barring

### C.10.1 Activation/Deactivation/Interrogation

#### C.10.1.1 Actions at the AGCF

Activation, deactivation and interrogation of incoming call barring is performed using service code commands as described in ETS 300 738 [12]. On receipt of a service code command, the AGCF sends an INVITE request as described in clause C.1.

#### C.10.1.2 Actions at the AS

On receipt of the INVITE request that includes a service code command as Request-URI, the AS proceeds as described in clause C.1.

### C.10.2 Invocation

#### C.10.2.1 Actions at the Originating AGCF

The originating AGCF is not involved in the invocation of the service.

#### C.10.2.2 Actions at the Originating AS

The originating AGCF is not involved in the invocation of the service.

#### C.10.2.3 Actions at the Terminating AS

On receipt of an INVITE request from a calling user, if incoming call barring is activated, the AS checks the P-Asserted-Identity against the list of allowed/forbidden calling parties. The rules and information used by the AS to evaluate whether the call shall be accepted are operator dependent. They may be compatible subset of the rules described in TS 183 011 [27].

If the call is rejected, the AS notifies the calling user by sending a 603 (Decline) response. Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure for invoking an announcement in the call establishment phase is described within TS 183 028 [6].

#### C.10.2.4 Actions at the Terminating AGCF

The terminating AGCF is not involved in the provision of the service.

---

## C.11 Malicious Call Identification

### C.11.1 Actions at the Originating AGCF

The AGCF at the originating side is not involved in the provision of this service.

### C.11.2 Actions at the Originating AS

The AS at the originating side is not involved in the provision of this service.

### C.11.3 Actions at the Terminating AS

Support of the Malicious Call Identification (MWI) service requires that the AS providing the service is involved in all incoming calls to the served user.

On receipt of a service code command requesting invocation of the MCID service, the AS registers the details of the last incoming call in a special record. Processing of this record is outside the scope of standardization.

### C.11.4 Actions at the Terminating AGCF

The MCID service is invoked using a special service code command dialled after the malicious call is released.

On receipt of this service code command, the AGCF sends an INVITE request as described in clause C.1.

---

## C.12 Message Waiting Indicator

### C.12.1 Actions at the AGCF

On receipt of a NOTIFY request reporting the "message-summary" event, the AGCF requests the following actions from the media gateway:

- Modify the default dial tone.
- Send a Message Waiting Indicator message (see EN 200 659-3 [10]) using the H.248 **andisp/data** signal.

### C.12.2 Actions at the AS

The AS implements the procedures described in TS 183 006 [26].

Generation of the Message Waiting Indicator message (see EN 200 659-3 [10]) by the AGCF is described in annex D.

---

## C.13 Outgoing Call Barring

### C.13.1 Activation/Deactivation/Interrogation

#### C.13.1.1 Actions at the AGCF

Activation and deactivation of outgoing call barring is performed using service code commands as described in ETS 300 738 [12]. On receipt of a service code command, the AGCF sends an INVITE request as described in clause C.1.

#### C.13.1.2 Actions at the AS

On receipt of the INVITE request that includes a service code command as Request-URI, the AS proceeds as described in clause C.1.

### C.13.2 Invocation

#### C.13.2.1 Actions at the Originating AGCF

The originating AGCF is not involved in the invocation of the service.

### C.13.2.2 Actions at the Originating AS

On receipt of an INVITE request from a calling user, if outgoing call barring is activated, the AS checks the Request-URI against the list of allowed/forbidden called destinations. The rules and information used by the AS to evaluate whether the call shall be accepted are operator dependent. They may be compatible subset of the rules described in TS 183 011 [27].

If the call is rejected, the AS notifies the calling user by sending a 603 (Decline) response. Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure for invoking an announcement in the call establishment phase is described within TS 183 028 [6].

### C.13.2.3 Actions at the Terminating AS

The terminating AS is not involved in the provision of the service.

### C.13.2.4 Actions at the Terminating AGCF

The terminating AGCF is not involved in the provision of the service.

---

## C.14 Three party service

### C.14.1 General

#### C.14.1.1 Actions at the AGCF at the service invocation side

The service is invoked during a stable 2 party call (without any waiting/hold call) using the Register Recall. Figure C.3 illustrates the message sequence between the AGCF and the AS.

On receipt of a NOTIFY request reporting a flash-hook event, the AGCF performs the following actions:

- Request the media gateway to play a dial tone and collect digits.
- Send a re-INVITE request to place the current call on hold.

On receipt of the dialled digits, the AGCF opens a new dialogue by sending an INVITE request with the following elements:

- The dialled digits used as a Request-URI.
- An SDP Offer for a voice call.

and wait for a 183 (Session Progress) with an SDP Answer.

On receipt of the 183 (Session Progress) response, the AGCF performs the following actions:

- Request the media gateway to modify the Remote Descriptor of the ephemeral termination associated with the physical termination representing the analog line.
- Request the media gateway to play a ringback tone, unless a P-Early-Media header is included in the SIP message, as described in TS 183 028 [6].
- Request the media gateway to monitor the flash-hook event.

On receipt of a re-INVITE request requesting a call to be placed on hold, the AS applies the procedures described in TS 183 010 [8].

Subsequent AGCF actions are identical to those described for the call waiting service.

### C.14.1.2 Actions at the AS at the service invocation side

Support of this service requires that all outgoing and incoming calls to the served user be handled by the same AS.

On receipt of a service code command requesting a three party conference, the AS may check that this request is compatible with subscription data held in the user profile. If the user is not entitled to use this service, the AS interacts with an MRFC in order to play an announcement to the invoker and sends a negative response to the re-INVITE request.

On receipt of a re-INVITE request with an SDP "a=sendonly" attribute, the AS may interact with an MRFC in order to play an announcement to the held party, in accordance with TS 183 028 [6].

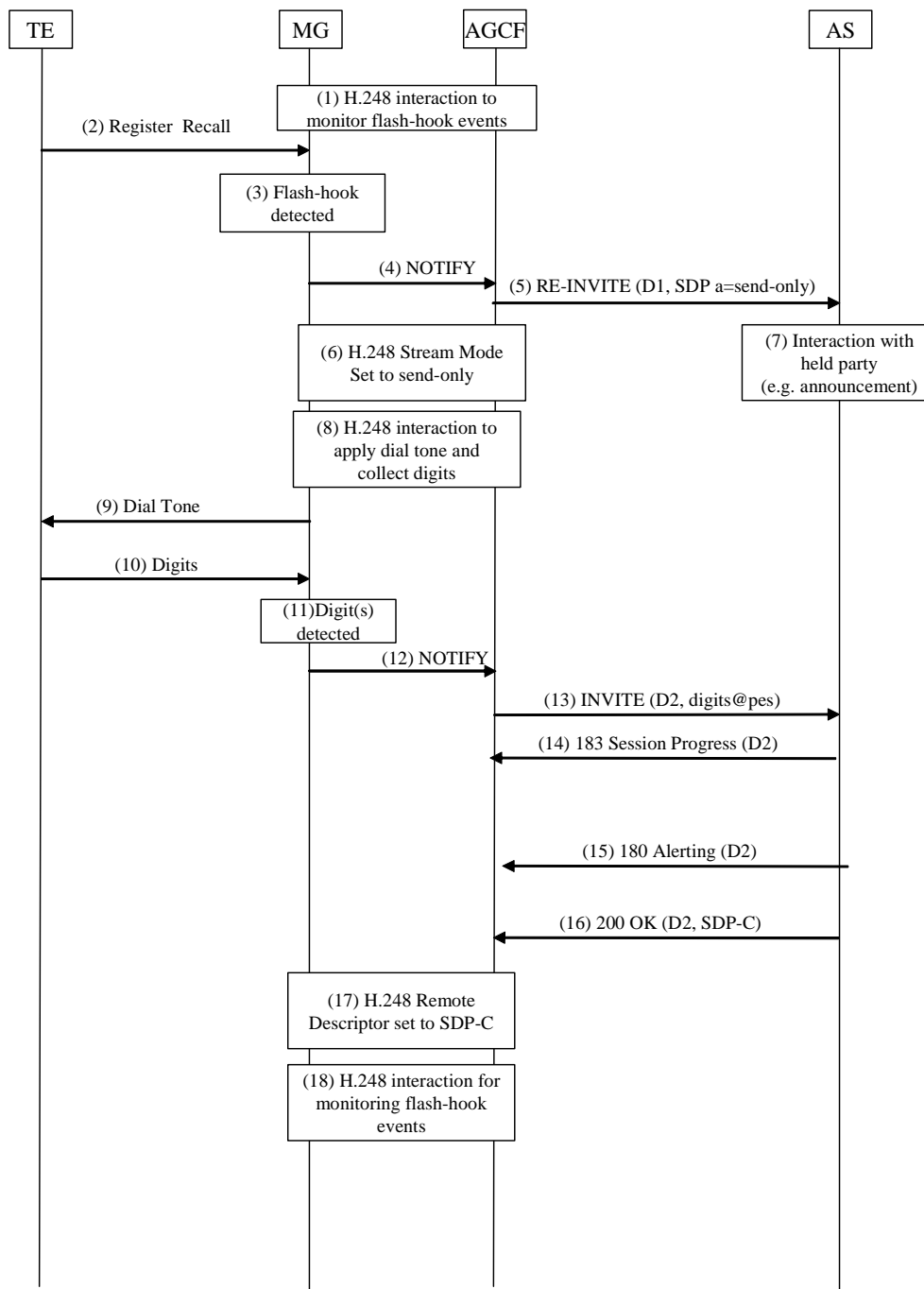


Figure C.3: Initiating a 3-Party call

## C.14.2 Option 1 (Loose coupling)

### C.14.2.1 Actions at the AGCF at the invoking side

The AGCF evaluates the Switch Order Command based on a provisioned mapping table.

If the feature code received from the internal MGC component does not match any known feature, the AGCF ignores the feature code and optionally request the media gateway to play an error tone or an announcement to the served user.

If the SOC indicates that the user wishes to establish a 3-party conference with the held parties, the AGCF performs the following actions:

- Request the media gateway to:
  - Add a termination to the current context based on SDP information associated with the held party.
  - Monitor the flash-hook event.
- Send a re-INVITE request towards the first held party (i.e. the party that was already held when the flash-hook event was detected). The re-INVITE request is built as follows:
  - The Request URI is set to the held party's identity.
  - The SDP description is set to a=sendrecv. The address and port are set according to the contents of the local descriptor of the new termination.
- Send a re-INVITE request towards the second held party (i.e. the party that has been held for the purpose of collecting the Switch Order Command). The re-INVITE request is built as follows:
  - The Request URI is set to the held party's identity.
  - The SDP description is set to a=sendrecv.

Once the 3-party call is established with the waiting party, processing of the flash-hook event is similar to the call waiting service. If SOC indicates that the served user wishes to reject one of the parties, the AGCF performs the following actions:

- Send a BYE request towards the held party.
- Request the media gateway to:
  - Remove the corresponding ephemeral termination.
  - Monitor the flash-hook event.

### C.14.2.2 Actions at the Originating AS at the invoking side

On receipt of a re-INVITE request with an SDP attribute "sendonly", the AS may interact with an MRFC in order to play an announcement to the held party, in accordance with TS 183 028 [6].

On receipt of a re-INVITE request with the SDP attribute "sendrecv", the AS interacts with the MRFC to stop any ongoing announcement.

On receipt of a BYE request, the AS releases the dialogue with the associated party.

## C.14.3 Option 2 (Tight coupling)

### C.14.3.1 Actions at the AGCF at the originating side

The AGCF opens a new dialogue and sends an INVITE request to the Application Server, built as follows:

- The Request URI is structured as follows:
  - A user part containing a provisioned prefix followed by the switching order command without the start and finish fields.

NOTE: In networks where no explicit SOC is collected, a preconfigured SOC is used to populate the user part, , such as "flash@pes.operator.com".

- A domain name that together with the user part provides sufficient information to the S-CSCF to forward the INVITE request to the appropriate AS, based on Initial Filter Criteria stored in the user profile, e.g.

**SOC- "SO (SR SI)"@pes.operator.com**

- A P-Asserted-Identity containing the public identity of the subscriber issuing the switching control command.
- An SDP offer for a voice call.

The AGCF modifies the H.248 Remote Descriptor and stream mode according to the SDP information received in re-INVITE messages sent by the Application Server.

### C.14.3.2 Actions at the Originating AS at the originating side

The AS evaluates the Switch Order Command based on the current call configuration and issues appropriate re-INVITE messages.

The AS interacts with an MRFC in order to play and stop announcements to held parties, in accordance with TS 183 028 [6].

In order to provide a network-based 3 party conference, the AS may use the ANNC URL syntax defined in [16] to form a conference using an MRFC/MRFP. In this case, the AS will send re-INVITE requests to all 3 parties in order to connect all three parties together at the MRFC/MRFP.

## C.15 Repeat Last Call

### C.15.1 AGCF at the served user side

The Repeat Last Call service is invoked using a service code command. On receipt of this service code command, the AGCF builds an INVITE request as described in clause C.1.

### C.15.2 AS at the served user side

Implementation of this service assumes that the AS providing the service is involved in all outgoing calls to the served user. It is the responsibility of the network operator to configure the appropriate Initial Filter Criteria in the user profile. The AS keeps track of the last incoming call to each served user it manages.

When receiving the service code command that identifies the Repeat Last Call service, the AS acts as a B2BUA and establishes a new call leg to the last called party (i.e. it sends an INVITE messages towards this last called party as if the number had been dialled again by the served user).

## Annex D (normative): Mapping between SIP and the subscriber line protocol.

### D.1 Introduction

This annex describes the mapping between SIP messages received by an AGCF or a VGW acting as a UE and the messages of the subscriber line protocol defined in ES 200 659-3 [10].

### D.2 Call Setup message

This message is used to send information related to an incoming call. e.g. Calling Line Identification Presentation (CLIP) and related services.

This message is built by the AGCF or the VGW on receipt of an initial INVITE request.

The AGCF requests the media gateways to send this message over the analog line using the Display Data Block parameter of the Display With Alerting signal of the **andisp** package defined in Recommendation H.248.23 [13].

The AGCF or VGW populates the message parameters as described in table D.1, based on the contents of the INVITE message and local configuration data.

**Table D.1: Call set-up message parameters**

Parameter type	O/M	Populating rules
Date and Time	O	Set from local clock (note 1)
Calling Line Identity	M	Set according to the contents of the "From" header or "P-Asserted-Identity" header dependent on national operator requirements.
Or Reason for absence of Calling Line Identity		Or Set from "Privacy" header (note 2)
Called Line Identity	O	"P-Called-Party-Id" header
Calling Party Name	O	Set according to the "Display-Name" in the "From" header or "P-Asserted-Identity" header dependent on national operator requirements
Or Reason for absence of Calling Party Name		or "Privacy" header (note 2)
Complementary Calling Line Identity	O	Setting of this parameter is based on operator specific rules.
Call type	O	Setting of this parameter is based on operator specific rules.
First Called Line Identity	O	Set according to the "hi-targeted-to-uri" in the first entry in the "History-Info" header Absent if the "Privacy" header set to "history"
Number of Messages	O	Setting of this parameter is based on operator specific rules.
Type of Forwarded call	O	Set according to the "Cause" parameter associated with the "hi-targeted-to-uri" in the last entry of the "History-Info" header. Absent if the "Privacy" header is set to "history"
Type of Calling User	O	Set from the cpc parameter of the P-Asserted-Identifier header Absent if the "Privacy" header set to "header"
Redirecting Number	O	Set according to the "hi-targeted-to-uri" in the last entry in the "History-Info" Absent if the "Privacy" header set to "history"
Network Provider Identity	O	Setting of this parameter is based on operator specific rules.
Carrier Identity	O	Setting of this parameter is based on operator specific rules.
Selection of Terminal Function	O	Setting of this parameter is based on operator specific rules.
Display Information	O	May be set from the contents of the message body
Service Information	O	May be set from the contents of the message body
Extension for network operator use	O	Setting of this parameter is based on operator specific rules.



Parameter type	O/M	Populating rules
NOTE 1:		The AGCF and the VGW shall support an appropriate clock synchronization mechanism.
NOTE 2:		If the "Privacy" header is included and set to "id" or "user" or "header", the Reason for Absence is set to "Private" (0101 0000). If the "P-Asserted-Identifier" header and the "From" header are absent, the Reason for Absence is set to "unavailable" (0100 1111).

## D.3 Message Waiting Indicator message

This message type is used to handle information related to messages in a message system.

This message is built by the AGCF or the VGW on receipt of a NOTIFY request reporting the "message-summary" event.

The AGCF requests the media gateways to send this message over the analog line using the Data Block parameter of the Generic Data Signaling signal of the **andisp** package defined in Recommendation H.248.23 [13]. The value of the TAS parameter is provisioned in the AGCF or MGF, per media gateway or per line.

The AGCF or the VGW populates the message parameters as described in table D.2, using the information contained in NOTIFY requests reporting the "message-summary" event and local configuration data.

**Table D.2: Message Waiting Indicator message parameters**

Parameter type	O/M	Populating rules
Date and Time	O	Set from local clock (see note)
Calling Line Identity Or Reason for absence of Calling Line Identity	O	Set according to the contents of the "P-Asserted-Id" header Or Privacy header
Calling Party Name Or Reason for absence of Calling Party Name	O	Set according to the "P-Asserted-Id" header or "Privacy" header
Visual Indicator	M	Set to "FF"H if the "Messages-Waiting" header is set to "yes"
Message Identification	O	Set according to the "Message-ID" header
Last Message CLI	O	"From" header associated with the last message
Complementary Date and Time	O	"Date" header associated with the last message
Complementary Calling Line Identity	O	Setting of this parameter is based on operator specific rules.
Number of Messages	O	Set according to the "Voice-Message" header
Type of Calling User	O	Setting of this parameter is based on operator specific rules.
Network Provider Identity	O	Setting of this parameter is based on operator specific rules.
Selection of Terminal Function	O	Setting of this parameter is based on operator specific rules.
Display Information	O	May be set from the contents of the message body
Extension for network operator use	O	Setting of this parameter is based on operator specific rules.
NOTE: The AGCF and the UE shall support an appropriate clock synchronization mechanism.		

## D.4 Advice of Charge message

This message is used to send information related to the charge of a call.

This message is built by the AGCF or the VGW on receipt of a SIP message that contain information defined in [7].

The AGCF requests the media gateways to send this message over the analog line using the Burst Pules Count parameter of the Metering Pulse Burst signal of the **amet** package defined in Recommendation H.248.26 [14].

The AGCF or the VGW populates the message parameters as described in table D.3, based on information defined in [7] and local configuration data.

Table D.3: Advice Of Charge message parameters

Parameter type	O/M	Populated From
Date and Time	O	Set from local clock (see note)
Calling Line Identity Or Reason for absence of Calling Line Identity	O	Setting of this parameter is based on operator specific rules.
Called line identity	O	Setting of this parameter is based on operator specific rules.
Complementary Calling Line Identity	O	Setting of this parameter is based on operator specific rules.
Charge	M	Set from information defined in [7]
Additional Charge	O	Setting of this parameter is based on operator specific rules.
Duration of the call	O	Setting of this parameter is based on operator specific rules.
Network Provider Identity	O	Setting of this parameter is based on operator specific rules.
Carrier Identity	O	Setting of this parameter is based on operator specific rules.
Selection of Terminal Function	O	Setting of this parameter is based on operator specific rules.
Display information	O	Set from information defined in [7]
Extension for network operator use	O	Setting of this parameter is based on operator specific rules.
NOTE: The AGCF and the VGW shall support an appropriate clock synchronization mechanism.		

---

## Annex E (informative): Bibliography

ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

IEEE 1003.1: " Information technology - Portable Operating System Interface (POSIX®) - Part 1: Base Definitions".

---

## History

<b>Document history</b>		
V1.1.1	May 2006	Publication