# ETSI TR 183 014 V1.1.1 (2005-12)

*Technical Report*

## Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation; Development and Verification of PSTN/ISDN Emulation

Reference

DTR/TISPAN-03033-NGN-R1

Keywords

availability, ISDN, PSTN, service

***ETSI***

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

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

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

# Contents

# Intellectual Property Rights

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

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

# Foreword

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

# 1 Scope

The present document presents the results of an analysis of bearer, basic and supplementary services currently provided in PSTN and ISDN implementations. The purpose of the analysis was to identify further areas of standardization to ensure that such services can be reliably emulated within the NGN thus enabling network operators to fulfil the technical regulatory obligations on European ECN providers of Publicly Available Telephone Service. It was assumed during the analysis that PSTN and ISDN signalling would be presented in the Integrated Services User Part (ISUP) as defined in EN 300 356-1 [3] and EN 300 356-2 [4] and that signalling within the NGN would be encapsulated in SIP-I as defined in EN 383 001[1] and ITU-T Recommendation H.248.1 [29].

# 2 References

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

[1] ETSI EN 383 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking for SIP/SIP-T (BICC, ISUP) [ITU-T Recommendation Q.1912.5, modified]".

NOTE: EN 383 001 is an endorsement of ITU-T Recommendation Q.1912.5. Throughout the present document, all clause, table and figure references to an endorsement (such as EN 383 001) should be considered as references to the endorsed document (such as Q.1912.5) unless a modification is specified in the endorsement.

[2] 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".

[3] ETSI EN 300 356-1: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface; Part 1: Basic services [ITU-T Recommendations Q.761 to Q.764 (1999) modified]".

[4] ETSI EN 300 356-2: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface; Part 2: ISDN supplementary service [ITU-T Recommendation Q.730 (1999) modified]".

[5] ETSI EN 300 356-18: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface; Part 18: Completion of Calls to Busy Subscriber (CCBS) supplementary service [ITU-T Recommendation Q.733, clause 3 (1997) modified]".

[6] ETSI EN 300 356-21: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface; Part 21: Anonymous Call Rejection (ACR) supplementary service [ITU-T Recommendation Q.731, clause 4 (1993)]".

[7] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[8] ETSI EN 302 097: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP); Enhancement for support of Number Portability (NP) [ITU-T Recommendation Q.769.1 (2000), modified]".

[9] ETSI ES 283 026: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Rq interface stage 3".

[10] ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Stage 3 description of the Gq' interface".

[11] ETSI ES 282 002: "Functional architecture for PSTN/ISDN Emulation".

[12] ETSI ES 282 003: "NGN Functional Architecture; Resource and Admission Control Subsystem (RACS); Release 1".

[13] ETSI ES 283 018: "H.248 Profile for the Ia Interface".

[14] ETSI ES 283 012: "TISPAN NGN Release l; Trunking Gateway Control Procedures for interworking between NGN and External CS Networks".

[15] ETSI ES 283 024: "TISPAN NGN Release l; PSTN/ISDN Emulation Subsystem; H.248 Profile for controlling Trunking Media Gateways".

[16] ETSI TR 101 118 (1997): "Network Aspects (NA); High level network architecture and solutions to support number portability".

[17] 1997/66/EC: "Directive of the european parliament and of the council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector".

[18] 2002/58/EC: "Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)".

[19] ITU-T Recommendation Q.711: "Functional description of the signalling connection control part".

[20] ITU-T Recommendation Q.712: "Definition and function of signalling connection control part messages".

[21] ITU-T Recommendation Q.713: "Signalling connection control part formats and codes".

[22] ITU-T Recommendation Q.714: "Signalling connection control part procedures".

[23] ITU-T Recommendation Q.771: "Functional description of transaction capabilities".

[24] ITU-T Recommendation Q.772: "Transaction capabilities information element definitions".

[25] ITU-T Recommendation Q.773: "Transaction capabilities formats and encoding".

[26] ITU-T Recommendation Q.774: "Transaction capabilities procedures".

[27] ITU-T Recommendation Q.775: "Guidelines for using transaction capabilities".

[28] ITU-T Recommendation Q.Sup45: "Technical Report TRQ.2815: Requirements for interworking BICC/ISUP network with originating/destination networks based on Session Initiation Protocol and Session Description Protocol".

[29] ITU-T Recommendation H.248.1: "Gateway control protocol: Version 2".

[30] IETF RFC 4040: "RTP Payload Format for a 64 kbit/s Transparent Call".

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

[32] IETF RFC 2633: "S/MIME Version 3 Message Specification".

[33] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

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

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

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 383 001 [1] and the following apply:

**basic service:** bearer service or teleservice

NOTE: When used in the present document it refers to those services defined for ISUP in EN 300 356-1.

**bearer service:** type of telecommunication service that provides a defined capability for the transmission of signals between user-network interfaces

**supplementary service:** service that modifies or supplements a basic telecommunication service

NOTE: When used in the present document it refers to those services defined for ISUP in EN 300 356-2.

**teleservice:** telecommunication service providing the complete capability, including terminal equipment functions, for communication between users according to protocols established by agreement between network operators (and equipment suppliers)

## 3.2 Abbreviations

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

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| 3PTY | Three-Party |
| ACR | Anonymous Call Reject |
| AGCF | Access Gateway Control Function |
| AGF | Access Gateway Function |
| ATP | Access Transport Parameter |
| AVP | Audio and Video Profile |
| BICC | Bearer Independent Call Control |
| BRA | Basic Rate Access |
| CCBS | Completion of Calls to Busy Subscriber |
| CCNR | Completion of Calls on No Reply |
| CD | Call Deflection |
| CFB | Call Forwarding Busy |
| CFNR | Call Forwarding No Reply |
| CFU | Call Forwarding Unconditional |
| CLI | Calling Line Identification |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| COLP | COnnected Line identification Presentation |
| COLR | COnnected Line identification Restriction |
| CONF | CONFerence call, add-on |
| CPE | Customer Premises Equipment |
| CS | Circuit Switched |
| CUG | Closed User Group |
| CW | Call Waiting |
| DDI | Direct-Dialling-In |
| DN | Directory Number |
| DTMF | Dual Tone Multiple Frequency |
| EC | European Commission |
| ECN | Electronic Communication Network |
| ECS | Electronic Communication Service |
| ECT | Explicit Call Transfer |
| FE | Functional Entities |
| HLC | High Layer Capability |
| HOLD | Call HOLD |

| | |
|---|---|
| HTTP | HyperText Transport Protocol |
| IAM | Initial Address Message |
| I-BGF | Interconnection Border Gateway Function |
| IE | Information Element |
| IETF | Internet Engineering Task Force |
| I-IWU | Incoming-IWU |
| IMS | IP Multimedia Subsystem |
| IN | Intelligent Network |
| ISDN | Integrated Services Digital Network |
| ISUP | Integrated Services User Part |
| IWU | InterWorking Units |
| LI | Lawful Interception |
| MCID | Malicious Call IDentification |
| MIME | Multipurpose Internet Mail Extensions |
| MSN | Multiple Subscriber Number |
| NGN | Next Generation Network |
| NP | Number Portability |
| NRN | Network Routing Number |
| NT | Network Termination |
| O-IWU | Outgoing-IWU |
| PES | PSTN/ISDN Emulation Subsystem |
| PRA | Primary Rate Access |
| PSS | PSTN/ISDN Simulation Subsystem |
| PSTN | Public Switched Telephone Network |
| RACS | Resource and Admission Control Subsystem |
| RCEF | Resource Control Enforcement Function |
| RGF | Residential Gateway Function |
| RTP | Real-Time Transport Protocol |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SAM | Subsequent Address Message |
| SCCP | Signalling Connection Control Part |
| SDP | Session Description Protocol |
| SGF | Signalling Gateway Function |
| SIP | Session Initiation Protocol |
| SIP-I | SIP Profile C of EN 383 001 |
| SP | Service Provider |
| SpoA | Service point of Attachment |
| SUB | SUBaddressing |
| TC | Transaction Capability |
| TDM | Time Division Multiplexing |
| TGCF | Trunking Gateway Control Function |
| TGF | Trunking Gateway Function |
| TLS | Transport Layer Security |
| TMR | Transmission Medium Requirement |
| TP | Terminal Portability |
| TpoA | Transport point of Attachment |
| URI | Uniform Resource Identifier |
| USI | User Service Indicator |
| UUS | User-to-User Signalling |
| VPN | Virtual Private Network |

# 4 Introduction

The PSTN/ISDN services are analysed in clause 5.

The reference points and the interfaces in the PSTN/ISDN Emulation Subsystem are shown in figure 1. Table 1 provides a short explanation of the reference points and the status of the development. Table 1 also indicates the clauses in the present document where the specifications at the various reference points are analysed.

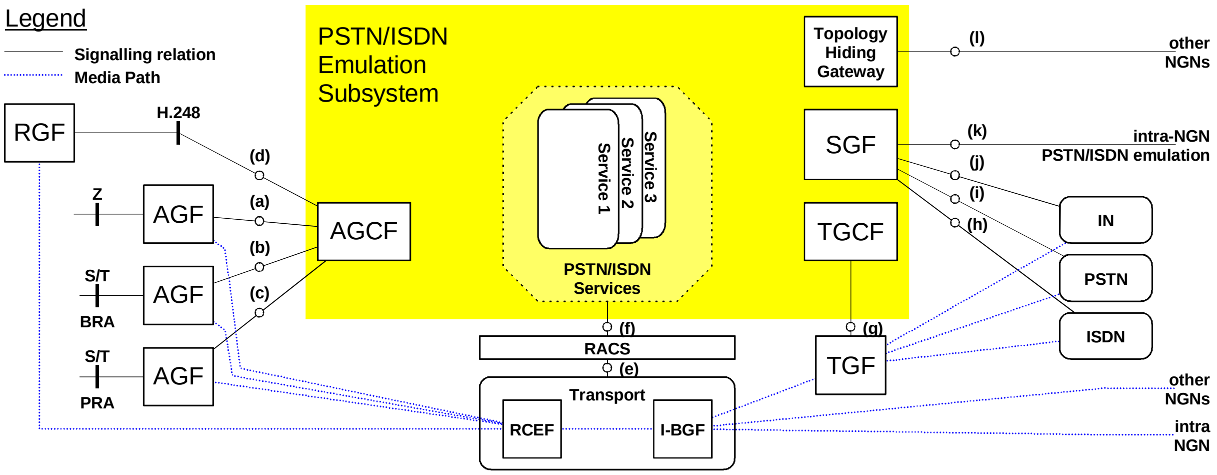

Figure 1: Overview of Functional Entities (FE)

Table 1: Overview of the PSTN/ISDN Emulation Subsystem (PES) for NGN Release 1

| Ref | Description | Stage 2 | Stage 3 | Status | Clause |
|---|---|---|---|---|---|
| (a) | Control of AGF (analog) | ES 282 002 [11] | ES 283 002 [2] | approved | 6.2 |
| (b) | Control of AGF (ISDN BRI) | ES 282 002 [11] | ES 283 002 [2] | approved | 6.2 |
| (c) | Control of AGF (ISDN PRI) | ES 282 002 [11] | ES 283 002 [2] | approved | 6.2 |
| (d) | Control of RGF | ES 282 002 [11] | Same as (a), (b), and (c) | approved | 6.2 |
| (e) | Interface RACS to Transport (Ia) | ES 282 003 [12] | ES 283 018 [13] | development | 6.4 |
| (f) | Resource reservation | ES 282 002 [11] /<br>ES 282 002 [12] | TS 183 017 [10] /<br>ES 283 026 [9] | development | 7 |
| (g) | Trunking Media Gateway Control | ES 283 012 [14] | ES 283 024 [15] | development | 6.3 |
| (h) | ISDN Signalling | | PSTN/ISDN specifications | existing | - |
| (i) | PSTN Signalling | | PSTN/ISDN specifications | existing | - |
| (j) | IN Signalling | | PSTN/ISDN specifications | existing | - |
| (k) | BICC(SIP-I) Signalling | | EN 383 001 [1] | approved | 8 |
| (l) | BICC(SIP-I) Signalling | | EN 383 001 [1] | approved | 8 |

# 5 Analysis of PSTN/ISDN services

## 5.1 Basic services

The mapping of ISUP to the Session Initiation Protocol profile C (SIP-I) is defined in EN 383 001 [1].

ISUP basic service comprises a number of capabilities which are listed in table 2. EN 383 001 [1] specifies a complete mapping between ISUP and SIP-I for these capabilities which, consequently, are not considered further in the present document.

Table 2: ISUP basic service capabilities

| Service |
|---|
| Speech/3,1 kHz audio |
| En bloc address signalling |
| Overlap address signalling from the Circuit Switched (CS) side towards the Internet Multimedia Services (IMS) |
| Out of band transport of DTMF tones and information. (BICC only) |
| Inband transport of DTMF tones and information. (BICC and ISUP) |
| Direct-Dialling-In (DDI) |
| Multiple Subscriber Number (MSN) |
| Calling Line Identification Presentation (CLIP) |
| Calling Line Identification Restriction (CLIR) |
| Connected line presentation (COLP) |
| Connected line restriction (COLR) |

### 5.1.1 Bearer services

#### 5.1.1.1 Mapping from ISUP bearer to RTP using SDP

The content of table 3 is drawn from EN 383 001 [1] which maps ISUP bearer types (described in the TMR/USI and HLC messages) to SDP/SIP. Not all of the ISUP bearer types are mapped and to ensure full support of all services the missing entries should be defined.

**Table 3: Coding of SDP media description lines from TMR/USI: BICC/ISUP to SIP**

| **TMR parameter** | **USI parameter** | | **HLC IE in ATP** | **m= line** | | | **b= line** | **a= line** |
|---|---|---|---|---|---|---|---|---|
| TMR codes | Information Transport Capabili | User Information Layer 1 Protocol Indicator | High Layer Characteristics Identific | <media> | <transport> | <fmt-list> | <modifier>:<bandwidth-value> | rtpmap: <dynamic-PT> <encoding name>/ <clock rate> [/encoding |
| speech | Speech | ITU-T Rec. G.711 [33] A-law | Ignore | audio | RTP/AVP | 8 | AS:64 | rtpmap:8 PCMA/8000 |
| speech | Speech | ITU-T Rec. G.711 [33] A-law | Ignore | audio | RTP/AVP | Dynamic PT | AS:64 | rtpmap:<dynamic-PT> PCMA/8000 |
| 3,1 kHz audio | USI Absent | | Ignore | audio | RTP/AVP | 8 | AS:64 | rtpmap:8 PCMA/8000 |
| 3,1 kHz audio | 3,1 kHz audio | ITU-T Rec. G.711 [33] A-law | (Note 1) | audio | RTP/AVP | 8 | AS:64 | rtpmap:8 PCMA/8000 |
| 3,1 kHz audio | 3,1 kHz audio | | Facsimile Group 2/3 | image | udptl | t38 | AS:64 | Based on T.38 |
| 3,1 kHz audio | 3,1 kHz audio | | Facsimile Group 2/3 | image | tcptl | t38 | AS:64 | Based on T.38 |
| 64 kbit/s unrestricted | Unrestricted digital inf. W/tone/ann. | N/A | Ignore | audio | RTP/AVP | 9 | AS:64 | rtpmap:9 G722/8000 |
| 64 kbit/s unrestricted | Unrestricted digital inf. W/tone/ann. | N/A | Ignore | audio | RTP/AVP | Dynamic PT | AS:64 | rtpmap:<dynamic-PT> CLEARMODE/8000 (Note 2) |
| NOTE 1: HLC normally absent in this case. It is possible for HLC to be present with the value "Telephony", although 6.3.1/Q.939 indicates that this would normally be accompanied by a value of "Speech" for the Information Transfer Capability element.<br>NOTE 2: The usage of the CLEARMODE IETF Draft is specified in RFC 4040 [30]. | | | | | | | | |

**Table 4: Identification of media not supported by EN 383 001 [1]**

| **TMR parameter** | **USI parameter** | | **HLC IE in ATP** | **m= line** | | | **b= line** | **A= line** |
|---|---|---|---|---|---|---|---|---|
| *"2 × 64 kbit/s unrestricted"* | *"Unrestricted digital information"* | N/A | Ignore | FFS | FFS | FFS | FFS | FFS |
| *"384 kbit/s unrestricted"* | *"Unrestricted digital information"* | N/A | Ignore | FFS | FFS | FFS | FFS | FFS |
| *"1536 kbit/s unrestricted"* | *"Unrestricted digital information"* | N/A | Ignore | FFS | FFS | FFS | FFS | FFS |
| *"1920 kbit/s unrestricted"* | *"Unrestricted digital information"* | N/A | Ignore | FFS | FFS | FFS | FFS | FFS |
| *"N × 64 kbit/s unrestricted", N from 3 to 29* | *"Unrestricted digital information"* | N/A | Ignore | FFS | FFS | FFS | FFS | FFS |

#### 5.1.1.2 3,1 kHz audio

The mapping of the ISUP 3,1 kHz audio bearer service to SIP-I is defined in EN 383 001 [1]. For details see table 3.

#### 5.1.1.3 Speech

The mapping of the ISUP speech bearer service to SIP-I is defined in EN 383 001 [1]. For details see table 3.

#### 5.1.1.4 64 kbit/s unrestricted

The mapping of the ISUP 64 kbit/s unrestricted bearer service to SIP-I is defined in EN 383 001 [1]. For details see table 3.

### 5.1.2 Basic call establishment and release

The mapping of the ISUP basic service to SIP-I is defined in EN 383 001 [1]. For each element of the basic service, table 5 identifies where details of the mapping can be found in EN 383 001 [1] for both incoming and outgoing procedures.

**Table 5: ISUP basic call function analysis**

| Function/service | Supported in EN 383 001 [1] Incoming procedures (I-IWU) | Supported in EN 383 001 [1] Outgoing procedures (O-IWU) |
|---|---|---|
| Speech/3,1 kHz audio | Table 6 | Table 26 |
| 64 kbit/s unrestricted | Table 6 | Table 26 |
| Multirate connection types | Table 6 | Table 26 |
| Nx64 kbit/s connection types | Table 6 | Table 26 |
| En-bloc address signalling | Clause 6.1 | Clause 7.1 |
| Overlap address signalling | Clause 6.1 | Clause 7.1 |
| Transit network selection | n/a | n/a |
| Continuity check | Clauses 6.1.1, 6.1.2, 6.3 | Clauses 7.1, 7.4, 7.7.3 |
| Forward transfer | Clauses 5.4.3, 5.4.3.2 | Clauses 5.4.3, 5.4.3.2 |
| Signalling procedures for connection type allowing fallback capability | X (Note 1) | X (Note 1) |
| Compatibility procedure | Clause 5.3 | Clause 5.3 |
| Simple segmentation | Clause 5.4.3.3 | Clause 5.4.3.3 |
| Tones and announcements | n/a | Clause 7.6.1 |
| Propagation delay determination procedure | n/a | Clause 7.1.5.2 |
| Enhanced echo control signalling procedures | X (Note 3) | X (Note 3) |
| Simple echo control signalling procedures | Clause 6.1.3.3 | n/a |
| Automatic repeat attempt | Clause 6.11.3 | n/a |
| Blocking and unblocking of circuits and circuit groups | Clauses 5.4.3, 5.4.3.1 | Clauses 5.4.3, 5.4.3.1 |
| Circuit group query | X (Note 2) | X (Note 2) |
| Dual seizure | X (Note 3) | X (Note 3) |
| Transmission alarm handling for digital inter-exchange circuits | X (Note 3) | X (Note 3) |
| Reset of circuits and circuit groups | Clause 5.4.3 | Clause 5.4.3 |
| Receipt of unreasonable signalling information | Clause 6.11.3 | Clause 7.7.3 |
| Access delivery information | Clause 6.1.3.5 | n/a |
| Transportation of user teleservice information | Clause 6.1.3.5 | Table 26 |
| Suspend and resume | Clauses 5.4.3, 5.4.3.2, 6.9, 6.10 | Clauses 5.4.3, 5.4.3.2 |
| Temporary trunk blocking | Clauses 5.4.3, 5.4.3.1 | Clauses 5.4.3, 5.4.3.1 |
| ISDN user part signalling congestion control | X (Note 5) | X (Note 5) |
| Automatic congestion control | X (Note 5) | X (Note 5) |
| Interaction between N-ISDN and INAP | n/a | n/a |
| Unequipped circuit identification code | X (Note 2) | X (Note 2) |
| ISDN user part availability control | Clauses 5.4.3, 5.4.3.2 | Clauses 5.4.3, 5.4.3.2 |
| MTP pause and resume | Clauses 5.4.3, 5.4.3.1 | Clauses 5.4.3, 5.4.3.1 |
| Overlength messages | X (Note 3) | X (Note 3) |
| Temporary alternative routing (TAR) | X (Note 4) | X (Note 4) |
| Hop counter procedure | Clause 6.1.3.9 | Clause 7.1.4 |
| Collect call request procedure | X (Note 2) | X (Note 2) |
| Hard-to-Reach | X (Note 4) | X (Note 4) |

| Function/service | Supported in<br>EN 383 001 [1]<br>Incoming procedures<br>(I-IWU) | Supported in<br>EN 383 001 [1]<br>Outgoing procedures<br>(O-IWU) |
|---|---|---|
| Calling Geodetic location procedure | X (Note 2) | X (Note 2) |
| Carrier Selection Information | X (Note 3) | X (Note 3) |
| Global Call Reference | X (Note 2) | X (Note 2) |
| NOTE 1: This feature not required in NGN Release 1.<br>NOTE 2: This is an end-to-end procedure involving no interaction with the intermediate network(s).<br>NOTE 3: This requires processing within the ISUP side of the originating or terminating exchange.<br>NOTE 4: This is a network management procedure.<br>NOTE 5: Within the NGN ISDN/PSTN Emulation Subsystem, congestion is detected and reported only within the ISUP. | | |

## 5.2 Regulatory services

### 5.2.1 Privacy and data protection

Article 8 of the Directive on privacy and electronic communication [18] identifies the following obligations on service providers:

- The SP shall offer the calling user a means of preventing the presentation of the CLI on a per-call basis.
- The SP shall offer the calling user a means of preventing the presentation of the CLI on a per-line basis.
- The SP shall offer to the called user a means of preventing the presentation of the CLI on incoming calls.
- If CLIP is offered prior to call establishment, the SP shall offer to the called user a means of rejecting the call if CLIR is invoked by the calling user (ACR service, user based solution).
- If CLIP is offered, the SP shall offer to the called user a means of preventing the presentation of the CLI on incoming calls.

Article 10 of the Directive defines a set of exceptions to the provisions of article 8 that allow for the tracing of malicious and nuisance calls (MCID) and for the support of emergency calls. Article 10 also allows for the obligations of article 9 related to the processing of location information to be overridden.

### 5.2.2 Caller identity transport

The Calling Party Number parameter is transferred in the Initial Address Message (IAM) if it is available. This parameter is also transferred encapsulated with the complete ISUP message within a SIP message. The transport of the caller identity is thus guaranteed.

### 5.2.3 Number Portability (NP)

Enhancements to ISUP for the support of Number Portability are described in EN 302 097 [8].

#### 5.2.3.1 Main body of EN 302 097

Clause 6.1.1 of EN 302 097 [8] (Handling of network routing number and directory number) states:

> The network routing number and the directory number are transferred in the Initial Address Message (IAM) as follows:
>
> > The network routing number (NRN) is transferred in the Called Party Number parameter and the directory number (DN) is transferred in the Called Directory Number parameter.

Clause 7.1.2 of EN 383 001 [1] (Request-URI and To header field) states:

> The Called Party Number parameter of the IAM and possibly the Address Signals indicators in the Subsequent Number parameter of SAMs contain the forward address information to derive the `userinfo` component of the INVITE Request-URI.
>
> For the basic call the address information contained in the Called Party Number parameter (and Subsequent Number parameters, if any) is also considered as the identification of the called party. This information is used to derive the `addr-spec` component of the To header field.

As SIP routing is based on the information in the To header field, routing is correctly performed on the NRN.

Clause 5.4.2.1.1 of EN 383 001 [1] (Alignment of SIP headers and ISUP body contents) states:

> Where a SIP header mapping to ISUP field(s) is defined (for example the mapping of Request-URI to Called Party Number in 6.1.3.1), the SIP header should be given precedence over the encapsulated ISUP value in the alignment process unless otherwise stated.

As the Called Party Number is encapsulated while the IAM remains in the SIP domain, this requirement implies that the Request-URI might change. Such a change would be reflected in the Called Party Number during parameter mapping in the I-IWU (see the following clause).

Clause 6.1.3.1 of EN 383 001 [1] (Called Party Number (mandatory)) states:

> The information contained in the `userinfo` component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM. The Internal Network Number Indicator shall be coded to "routing to internal network number not allowed".

The table 3 in EN 383 001 [1] summarizes this mapping. The network routing number (NRN) may be changed by this procedure but the ported directory number (DN) remains unchanged in the Called Directory Number parameter.

### 5.2.3.2 Annexes of EN 302 097

Annex A of EN 302 097 [8] specifies the exceptions to its own clause 6 which are needed for the support of the Concatenated Addressing method. It states that:

> The network routing number and directory number are transferred in the IAM as follows:
>
> > The DN is contained in the Called Party Number parameter and is prefixed by some digits used as a NRN.

Conclusion: This procedure is compatible with the specifications for NGN Release 1 if the Request-URI remains unchanged or the modifications retain the original ported directory number. No such specifications are known to exist.

Annex B of EN 302 097 [8] specifies the exceptions to its own clause 6 which are needed for the support of the Separate Network Routing Number Addressing method. It states that:

> The NRN is transferred in the Network Routing Number parameter. The DN is transferred in the Called Party Number parameter with `NoA` value 0000011 - "national (significant) number".

Conclusion: This procedure is not compatible with the specifications for NGN Release 1. The ported Directory Number remains in the Called Party Number parameter and is mapped into the To and Request-URI fields. This annex should be removed or additional procedures should be defined in EN 383 001 [1].

## 5.2.4 Emergency 112 calling

Emergency calls are handled by the AGW or RGW and MGC (see clauses 6.2.4 and 6.2.5).

## 5.2.5 Anonymous Call Reject (ACR)

In EN 300 356-21 [6] the procedures for the Anonymous Call Reject (ACR) supplementary service are defined. The mapping of ISUP to the NGN is defined in EN 383 001 [1].

### 5.2.6 Malicious Call IDentification (MCID)

The mapping of ISUP MCID to the NGN is defined in EN 383 001 [1].

### 5.2.7 Lawful Interception (LI)

The requirement for lawful interception is identified in Article 5 of 1997/66/EC [17]. Compliance for PES is addressed in DES/TISPAN-07013 and supported by existing provisions in ES 201 671 [7].

## 5.3 Non-regulatory services

### 5.3.1 Calling Line Identification Presentation (CLIP)

The mapping of the ISUP CLIP supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.2 Connected Line Identification Restriction (CLIR)

The mapping of the ISUP CLIR supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.3 COnnected Line identification Presentation (COLP)

The mapping of the ISUP COLP supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.4 COnnected Line identification Restriction (COLR)

The mapping of the ISUP COLR supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.5 Terminal Portability (TP)

The mapping of the ISUP TP supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.6 User-to-User Signalling (UUS)

The mapping of the ISUP UUS supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.7 Closed User Group (CUG)

The mapping of the ISUP CUG supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.8 Subaddressing (SUB)

The mapping of the ISUP SUB supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.9 Conference call, add-on (CONF)

The mapping of the ISUP CONF supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.10 Explicit Call Transfer (ECT)

The mapping of the ISUP ECT supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.11 Diversion supplementary service; Call Forwarding Busy (CFB)

The mapping of the ISUP CFB supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.12 Diversion supplementary service; Call Forwarding No Reply (CFNR)

The mapping of the ISUP CFNR supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.13 Diversion supplementary service; Call Forwarding Unconditional (CFU)

The mapping of the ISUP CFU supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.14 Diversion supplementary service; Call Deflection (CD)

The mapping of the ISUP CD supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.15 Call Hold (HOLD)

The mapping of the ISUP HOLD supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.16 Call Waiting (CW)

The mapping of the ISUP CW supplementary service to SIP-I is defined in EN 383 001 [1].

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

The mapping of the ISUP CCBS supplementary service to SIP-I is defined in EN 383 001 [1].

#### 5.3.17.1 CCBS - regular case

EN 383 001 [1] identifies EN 300 356-18 [5] as the normative specification of the ISUP Completion of Calls to Busy Subscriber (CCBS) supplementary service.

Clause B.11 of EN 383 001 [1] (Interworking of Completion of Calls to Busy Subscriber (CCBS) supplementary service to SIP networks) states:

> Profile C (SIP-I): No additional interworking beyond the use of ISUP encapsulation and SCCP connectivity between originating and terminating ISDN networks.

EN 300 356-18 [5] makes reference to the following ITU-T Recommendations:

1) ITU-T Recommendations Q.711 [19] to Q.714 [22], Signalling connection control part (SCCP).

2) ITU-T Recommendations Q.771 [23] to Q.775 [27], Transaction capabilities application part [23].

Clause 3.3.2 of EN 300 356-18 [5] (Requirements on the originating network) states:

> In order to operate the CCBS supplementary service, the originating local exchange shall have TC capabilities [23]. The originating network shall have SCCP capability [19] for routing the TC operations.

Conclusion: This procedure is not compatible with the specifications for NGN Release 1. The ported Directory Number remains in the Called Party Number parameter and is mapped into the To and Request-URI fields. This annex should be removed or additional procedures should be defined in EN 383 001 [1].

#### 5.3.17.2 CCBS - diverted call

The interactions between CCBS and call diversions are described in EN 300 356-18 [5].

#### 5.3.17.3 CCBS - Number Portability (NP)

EN 302 097 [8] specifies relay methods for non-circuit related signalling which are required for the support of number portability with services such as CCBS.

Clause 8.8.2 in EN 302 097 [8] states:

> It is left to operator and implementation decisions which relay type(s) is used, taking into account the regulatory and architectural constraints that may prevail.
>
> Details of the relay functions are for further study.

Clause 8 of TR 101 118 [16] specifies stage 2 information flows for three scenarios.

There are no ETSI documents that specify stage 3 procedures for SCCP routing for ported numbers.

Conclusion: Routing for ported numbers is left to proprietary implementations.

### 5.3.18 Three-Party (3PTY)

The mapping of the ISUP Three-Party supplementary service to SIP-I is defined in EN 383 001 [1].

### 5.3.19 Completion of Calls on No Reply (CCNR)

The mapping of the ISUP CCNR supplementary service to SIP-I is defined in EN 383 001 [1]. The further analysis follows the same lines as shown in clause 5.3.17 on Completion of Calls to Busy Subscribers.

## 5.4 Conclusions

### 5.4.1 Number Portability (NP)

The procedures of EN 302 097 [8] are compatible with EN 383 001 [1] except for:

1) The procedures in annex A of EN 302 097 [8] "Procedures for the Concatenated Addressing method" are compatible with the specifications for NGN Release 1 if the Request-URI remains unchanged or the modifications retain the original ported directory number. No such specifications are known to exist.

2) The procedures in annex B of EN 302 097 [8] are not compatible with the specifications for NGN Release 1. The ported Directory Number remains in the Called Party Number parameter and is mapped into the To and Request-URI fields. This annex should be removed or additional procedures should be defined in EN 383 001 [1].

If the donor network is a legacy PSTN/ISDN network and deploys onward routing, undesirable multiple transcoding may happen as illustrated in figure 2. Although when selecting a clear channel code for RTP/IP the data loss and delay variations might impact QoS.

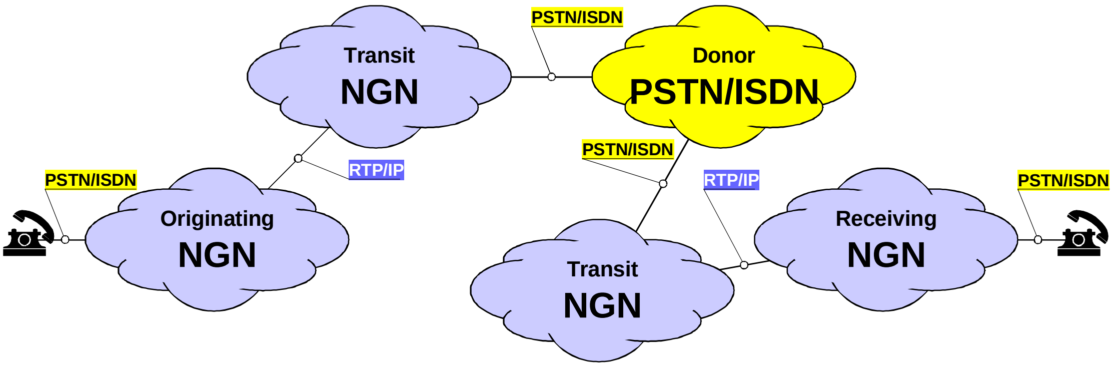

**Figure 2: Undesirable multiple transcoding with onward routing by donor**

Under unfavourable conditions, up to four IP islands are in the bearer path. This is illustrated in figure 3.

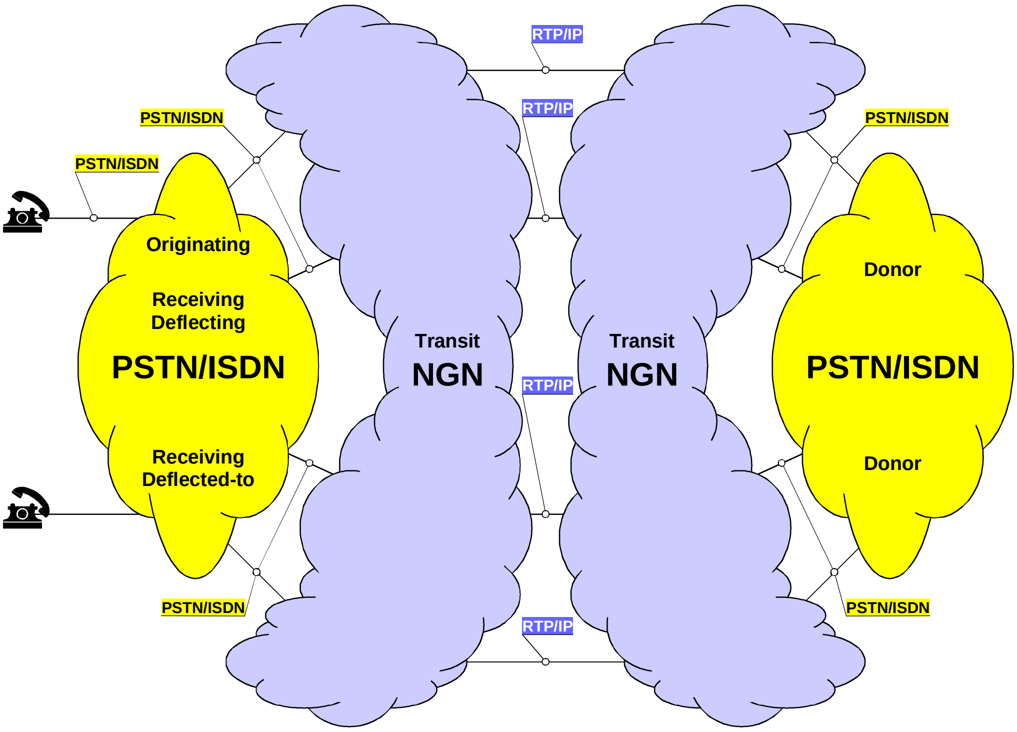

**Figure 3: Undesirable multiple transcoding with onward routing by donors and deflection**

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

The procedures of EN 300 356-18 [5] are compatible with EN 383 001 [1] except for the following areas where specifications do not exist:

a) SCCP connectivity over an IP network.

b) Stage 3 procedures for SCCP routing for ported numbers.

# 6 Bearer services (H.248)

Bearer services, and interworking and switching functions in Media Gateways (MG) are controlled via the Gateway Control Protocol (GCP) according H.248. The specification is based on the H.248 Profile concept according to clause 13/H.248.1. The MGC-MG interfaces are "profiled" in that sense, that needed capabilities on top of H.248.1 (like H.248.x-series Packages) are indicated, potential options are minimized, or not required functions are pointed out.

## 6.1 Profile identification

The H.248 profile for access and residential media gateways is defined in ES 283 002 [2].

The H.248 profile for trunking media gateways is defined in ES 283 024 [15], the procedures for interworking between NGN and external CS Networks are defined in ES 283 012 [14].

NOTE: The two documents are for TB approval in October and November 2005 and are hence not completely stable yet. Therefore the analysis of the two documents is only a snapshot based on the document versions that have been input to TISPAN#8.

# 6.2 Profile analysis, access and residential media gateways

## 6.2.1 Functional requirements

ES 283 002 [2], clause 4.1 names the reference points supported, i.e. Z, T, S/T, T*. No further reference points are needed for support of ISDN and PST emulation.

Table 6 shows the functional requirements and their status as defined in ES 283 002 [2], clause 4.2.

**Table 6: Functional requirements support**

| Functional Requirement | Access/Residential gateways<br>ES 283 002 [2], clause 4.2 |
|---|---|
| IP support | IPv4 mandatory<br>IPv6 optional |
| Codec | G.711 A-law mandatory<br>All other optional |
| Detect fax/modem, data/modem and text/modem traffic | Mandatory |
| Detect and forward DTMF tones for non G.711 A-law codecs | Mandatory |
| Provision of tone properties | Mandatory |

Besides the version of IP used, which is irrelevant for the delivery of media at the ISDN and PSTN ends of the call, all functions required for end-to-end transmission of speech and tones are available.

## 6.2.2 Profile description

Table 7 gives a cross-reference list between ITU-T Recommendation H.248.1 [29] and ES 283 002 [2] listing clause numbers and the analysis results.

**Table 7: Analysis of profile description**

| Clause No in ITU-T Rec. H.248.1 [29] | Clause No in ES 283 002 [2] | Clause title and analysis |
|---|---|---|
| 6 | 5.4 | Connection Model<br>Minimum requirements for physical terminations are analog and ISDN terminations as needed for PSTN/ISDN emulation. |
| 6.1, 6.1.1 | Table 2, 5.5 | Contexts, Context Attributes<br>All attributes including the emergency indicator are supported, no restrictions apply. |
| 6.2 | 5.6 | Terminations<br>Multiplexed terminations are not supported but are not necessary for NGN Release 1 functionalities. |
| Descriptors | | |
| 7.1 | 5.7 | Descriptors<br>See details below. |
| 7.1.2 | No specification indicating not applicable | Modem descriptor<br>Deprecated parameter. |
| 7.1.3 | No specification indicating not applicable | Multiplex descriptor<br>Not relevant for NGN Release 1 functionalities. |
| 7.1.4 | No specification indicating implicit applicability (note) | Media descriptor<br>Comprised of TerminationState and Stream descriptor below. |
| 7.1.5 | No specification indicating implicit applicability (note) | TerminationState descriptor |
| 7.1.6 | 5.7.1 | Stream descriptor<br>Profiled to the relevant termination types, i.e. RTP, ANALOG, ISDN |
| 7.1.7, 7.1.8 | 5.7.1.1 | Local and remote descriptors, LocalControl descriptor |

| Clause No in ITU-T Rec. H.248.1 [29] | Clause No in ES 283 002 [2] | Clause title and analysis |
|---|---|---|
| | | Profiled to reserve and commit RTP, ANALOG, ISDN terminations |
| 7.1.9 | 5.7.2 | Event descriptor<br>All termination type/ event type combinations covered. Event buffer control not used. |
| 7.1.10 | 5.7.3 | Event Buffer Descriptor<br>Not applicable, as event buffer control is not used. |
| 7.1.11 | 5.7.4 | Signals descriptor<br>Optional NotifyCompletion parameter not supported. |
| 7.1.12 | No specification indicating implicit applicability (note) | Audit descriptor |
| 7.1.13 | No specification indicating implicit applicability (note) | ServiceChange descriptor<br>See ServiceChange Command |
| 7.1.14 | 5.7.5 | DigitMap descriptor<br>Made mandatory by profile. Used to detect digits. |
| 7.1.15 | 5.7.6 | Statistics Descriptor<br>Supported on all relevant termination types. |
| 7.1.16 | No specification indicating implicit applicability (note) | Packages Descriptor |
| 7.1.17 | 5.7.7 | ObservedEvent descriptor |
| 7.1.18 | 5.7.8 | Topology descriptor<br>Descriptor optional, all values supported. |
| 7.1.19 | 5.7.9 | Error descriptor<br>All error values supported. |
| Command | | |
| 7.2 | 5.8 | Command API |
| 7.2.1 | 5.8.1 | Add<br>Multiplex descriptor not used, as not relevant for NGN Release 1 functionalities. |
| 7.2.2 | 5.8.2 | Modify<br>Multiplex descriptor not used, as not relevant for NGN Release 1 functionalities. |
| 7.2.3 | 5.8.3 | Subtract |
| 7.2.4 | 5.8.4 | Move<br>Multiplex descriptor not used, as not relevant for NGN Release 1 functionalities. |
| 7.2.5 | 5.8.5 | AuditValue<br>No restrictions. |
| 7.2.6 | 5.8.6 | AuditCapabilities<br>No restrictions. |
| 7.2.7 | No specification indicating implicit applicability (note) | Notify |
| 7.2.8 | 5.8.7 | ServiceChange<br>Optional ServiceChange parameter not used. |
| 7.2.9 | 5.8.8 | Manipulating and auditing context attributes<br>No restrictions. |
| 7.2.10 | 5.9 | Generic command syntax<br>Text format: Mandatory for sending/receiving<br>Binary format : Optional for sending, mandatory for receiving<br>No impact on PSTN/ISDN Emulation |
| Transactions, Messages, Transport, Security, Packages | | |
| 8 | 5.10 | Transactions<br>Number of transaction elements per message restricted to two. Segmentation package not required. |
| 8.3 | 5.11 | Messages<br>Clarification on use of domain names. |
| 9 | 5.12 | Transport<br>UDP: Mandatory<br>SCTP: Optional<br>No impact on PSTN/ISDN Emulation |

| Clause No in ITU-T Rec. H.248.1 [29] | Clause No in ES 283 002 [2] | Clause title and analysis |
|---|---|---|
| 10 | 5.13 | Security considerations |
| 12 | 5.14 | Packages<br>All packages needed for PSTN/ISDN emulation are listed. |
| NOTE: For this clause in ITU-T Recommendation H.248.1 [29] there exists no corresponding clause in the profile document. Where applicable, explanations can be found in the analysis column of the table. Absence of a specification by default indicates an implicit unchanged applicability of the specification in H.248.1. | | |

### 6.2.3 Procedures at IP Side

ES 283 002 [2], clause 6 covers voice-band data, 64 kbit/s unrestricted, comfort noise and silence suppression, DTMF transmission, call progress tones and the support of G.711 variants. The functional requirements identified in clause 6.2.1 of the present document are described in more detail.

### 6.2.4 Procedures for Physical H.248 terminations

ES 283 002 [2], clause 7 covers DTMF detection, sending of tones and announcements, support of emergency calls, echo control and specific procedures for analog lines and ISDN interfaces.

Detection of emergency calls is put into the responsibility of the MGC. All aspects associated with connection to analog lines and ISDN basic rate or primary rate interfaces are covered.

### 6.2.5 MG and MGC management

ES 283 002 [2], clause 8 covers overload control, IP QoS control and monitoring and testing of analog and digital lines.

Priority is given to emergency calls and priority lines in case of overload.

## 6.3 Profile analysis, trunking media gateways

### 6.3.1 Functional requirements

Clause 4.1 of both ES 283 024 [15] and ES 283 012 [14] describe an architecture with the assumption that for call control signalling ISUP is used on the PSTN/ISDN side and SIP on the IP side of the MGC. Reference is made to ITU-T Recommendation Q.1912.5 [31] which should be replaced by references to EN 383 001 [1]. The text in both documents is identical.

Table 8 shows the functional requirements and their status as defined in ES 283 012 [14], clause 4.2.

**Table 8: Functional requirements support**

| Functional Requirement | Access/Residential gateways<br>ES 283 012 [14], clause 4.2 |
|---|---|
| IMS (ephemeral) terminations | Establishment and release required |
| IP support | IPv4 mandatory<br>IPv6 mandatory |
| TDM (physical) terminations | Establishment and release required |
| Interworking of User Plane stacks | Required |
| Detect fax/modem , data/modem and text/modem traffic | Recommended |
| Codec | G.711 A-law mandatory<br>All other optional |
| Detect fax/modem traffic for non G.711 codecs | Recommended |
| Detect, forward and generate DTMF tones for non G.711 codecs | Mandatory |
| Generation of tones and announcements | Optional |

| Functional Requirement | Access/Residential gateways<br>ES 283 012 [14], clause 4.2 |
|---|---|
| Provision of tone properties | Mandatory |
| ISDN bearer service | TDM-to-TDM mandatory<br>TDM-to-RTP mandatory |
| Testing of circuit-oriented bearer connections | H.248 or OAM driven procedure required |
| Echo Control Device | Required on call by call basis |
| Codec negotiation | Mandatory |
| PACKETIZATION time indication | Mandatory |
| Emergency call identification | Mandatory |

For the given architecture, i.e. using ISUP/SS7 on the TDM side and SIP on the IP side, all functions required for end-to-end transmission of speech and tones are available.

### 6.3.2 Profile description

Table 9 gives a cross-reference list between ITU-T Recommendation H.248.1 [29] and ES 283 024 [15] listing clause numbers and the analysis results.

**Table 9: Analysis of profile description**

| Clause No in ITU-T Rec. H.248.1 [29] | Clause No in ES 283 024 [15] | Clause title and analysis |
|---|---|---|
| 6 | 5.4 | Connection Model<br>Two terminations per context are required (32 for 3GPP), all combinations are allowed, where NGN Release 1 requires on TDM, TDM and RTP, TDM contexts, i.e. not more than two termination types per context. |
| 6.1, 6.1.1 | Table 5.5 | Contexts, Context Attributes<br>All attributes including the emergency indicator are supported, no restrictions apply. |
| 6.2 | 5.6 | Terminations<br>Multiplexed terminations are not supported but are not necessary for NGN Release 1 functionalities. |
| Descriptors | | |
| 7.1 | 5.7 | Descriptors<br>See details below. |
| 7.1.2 | No specification indicating not applicable | Modem descriptor<br>Deprecated parameter. |
| 7.1.3 | No specification indicating not applicable | Multiplex descriptor<br>Not relevant for NGN Release 1 functionalities. |
| 7.1.4 | No specification indicating implicit applicability (note) | Media descriptor<br>Comprised of TerminationState and Stream descriptor below. |
| 7.1.5 | No specification indicating implicit applicability (note) | TerminationState descriptor |
| 7.1.6 | 5.7.1 | Stream descriptor<br>No restriction, all termination types supported |
| 7.1.7, 7.1.8 | 5.7.2 | LocalControl descriptor<br>For TDM, RTP and AAL1/2 terminations. All relevant stream mode values are allowed. This clause of ES 283 024 [15] may need clarification. |
| 7.1.9 | 5.7.3 | Event descriptor<br>All termination type/ event type combinations covered. Event buffer control not used. |
| 7.1.10 | 5.7.4 | Event Buffer Descriptor<br>Not applicable, as event buffer control is not used. |
| 7.1.11 | 5.7.5 | Signals descriptor<br>This clause of ES 283 024 [15] may need clarification. |
| 7.1.12 | No specification indicating implicit applicability (note) | Audit descriptor |

| Clause No in ITU-T Rec. H.248.1 [29] | Clause No in ES 283 024 [15] | Clause title and analysis |
|---|---|---|
| 7.1.13 | No specification indicating implicit applicability (note) | ServiceChange descriptor<br>See ServiceChange Command |
| 7.1.14 | 5.7.6 | DigitMap descriptor<br>Not supported by profile. |
| 7.1.15 | 5.7.7 | Statistics Descriptor<br>Not supported by profile. Waiting for stage 2 description. |
| 7.1.16 | No specification indicating implicit applicability (note) | Packages Descriptor |
| 7.1.17 | 5.7.8 | ObservedEvent descriptor |
| 7.1.18 | 5.7.9 | Topology descriptor<br>Descriptor optional, all values supported. |
| 7.1.19 | 5.7.10 | Error descriptor<br>This clause of ES 283 024 [15] may need clarification. |
| Command | | |
| 7.2 | 5.8 | Command API. |
| 7.2.1 | 5.8.1 | Add<br>MuxDescriptor, EventBufferDescriptor, DigitMapDescriptor not supported, as not supported by profile. |
| 7.2.2 | 5.8.2 | Add<br>MuxDescriptor, EventBufferDescriptor, DigitMapDescriptor not supported, as not supported by profile. |
| 7.2.3 | 5.8.3 | Subtract |
| 7.2.4 | 5.8.4 | Move<br>Command made optional; MuxDescriptor, EventBufferDescriptor, DigitMapDescriptor not supported, as not supported by profile. |
| 7.2.5 | 5.8.5 | AuditValue<br>This clause of ES 283 024 [15] may need clarification. |
| 7.2.6 | 5.8.6 | AuditCapabilities<br>This clause of ES 283 024 [15] may need clarification. |
| 7.2.7 | 5.8.9 | Notify<br>No restriction, both ObservedEvents and Error supported. |
| 7.2.8 | 5.8.7 | ServiceChange<br>All ServiceChange methods are supported, ServiceChange reasons restricted to certain values. |
| 7.2.9 | 5.8.8 | Manipulating and auditing context attributes<br>None described. |
| 7.2.10 | 5.9 | Generic command syntax<br>Text format: Mandatory for NGN Release 1 for sending/receiving<br>Binary format : Optional. |
| Transactions, Messages, Transport, Security, Packages | | |
| 8 | 5.10 | Transactions<br>Number of transaction elements per message restricted to two. Segmentation package not required. |
| 8.3 | 5.11 | Messages |
| 9 | 5.12 | Transport<br>SCTP: Recommended<br>SCTP/'M3UA: Optional<br>No impact on PSTN/ISDN Emulation. |
| 10 | 5.13 | Security considerations<br>None specified in Profile. |
| 12 | 5.14 | Packages. |
| NOTE: For this clause in ITU-T Recommendation H.248.1 [29] there exists no corresponding clause in the profile document. Where applicable, explanations can be found in the analysis column of the table. Absence of a specification by default indicates an implicit unchanged applicability of the specification in H.248.1. | | |

### 6.3.3 Procedures

ES 283 024 [15], clause 5.17 covers the following procedures:

- Call independent procedures.
- Procedures for IMS terminations.
- Voiceband Data support.
- Support of ISDN unrestricted 64 kbit/s.
- Comfort noise insertion and suppression.
- DTMF digit transfer.
- Echo control.

These clauses seem still under construction; hence no analysis has been performed on the procedures clause of ES 283 024 [15].

## 6.4 Profile for the «Ia» Interface

H.248 Profile for the «Ia» Interface is still under development and has not been analysed.

## 6.5 Conclusions

ES 283 002 [2] profiles ITU-T Recommendation H.248.1 [29] and clarifies the use of parameters and the procedures for PSTN/ISDN emulation purposes for residential media gateways. Detailed descriptions of the procedures at the IP and the analog/ISDN ends allow complete implementation of PSTN/ISDN emulation functionality for access and residential gateways.

ES 283 024 [15] profiles ITU-T Recommendation H.248.1 [29] and clarifies the use of parameters for PSTN/ISDN emulation purposes for trunking media gateways. The description of the procedures is not yet stable enough for a complete analysis. ES 283 012 [14] provides the functional requirements and procedures for interworking between NGN and external CS networks. This document should be completed and made basis for a complete state 3 description of those procedures.

In both profiles to ITU-T Recommendation H.248.1 [29] where there exists no corresponding clause in the profile document, the clause of H.248.1 is applicable unchanged by default. Nevertheless, in both profiles there exist absent specifications that have to be interpreted as "not applicable".

# 7 Resource and admission control

Resource and Admission Control procedures are still under development and have not been analysed.

# 8 Security analysis of PES

## 8.1 Interworking between BICC/ISUP and SIP

### 8.1.1 Overview

ITU-T Technical Report TRQ.2815 [28] identifies a set of interworking profiles.

### 8.1.2 Profile A

Profile A is not relevant for NGN Release 1.

### 8.1.3 Profile B

Profile B is not relevant for NGN Release 1.

### 8.1.4 Profile C

Profile C is normally referred to as SIP-I.

SIP-I elements originate in a trusted domain and terminate in a trusted domain. A transit network could, potentially, intercept and manipulate ISUP content and SIP-I headers using a "man-in-the-middle" attack. This can be mitigated using the S/MIME extensions for SIP carriage to counter the likelihood of a successful attack. If the transit network forms part of the trusted domain then the content of the message may be assumed to be trusted and the likelihood of the attack being successful is mitigated further.

## 8.2 Security in PES

Figure 4 illustrates the PES scenario overlaid on the regulatory model for the NGN (on the assumption that the NGN is an instance of an ECN&S system).

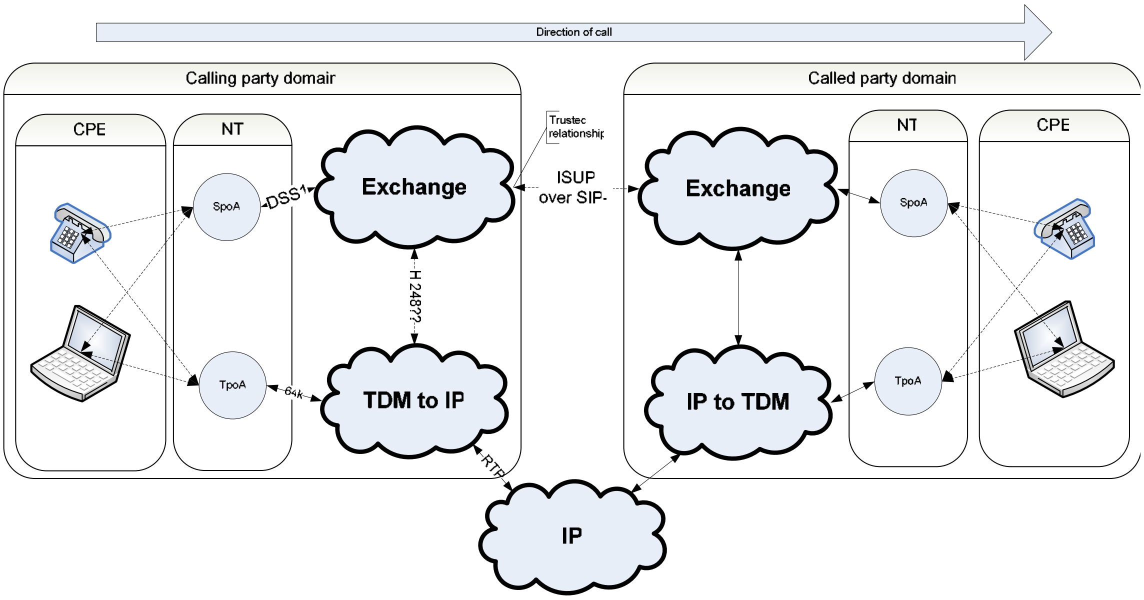

**Figure 4: PES scenario**

The ECN&S (regulatory) model is shown in figure 5.

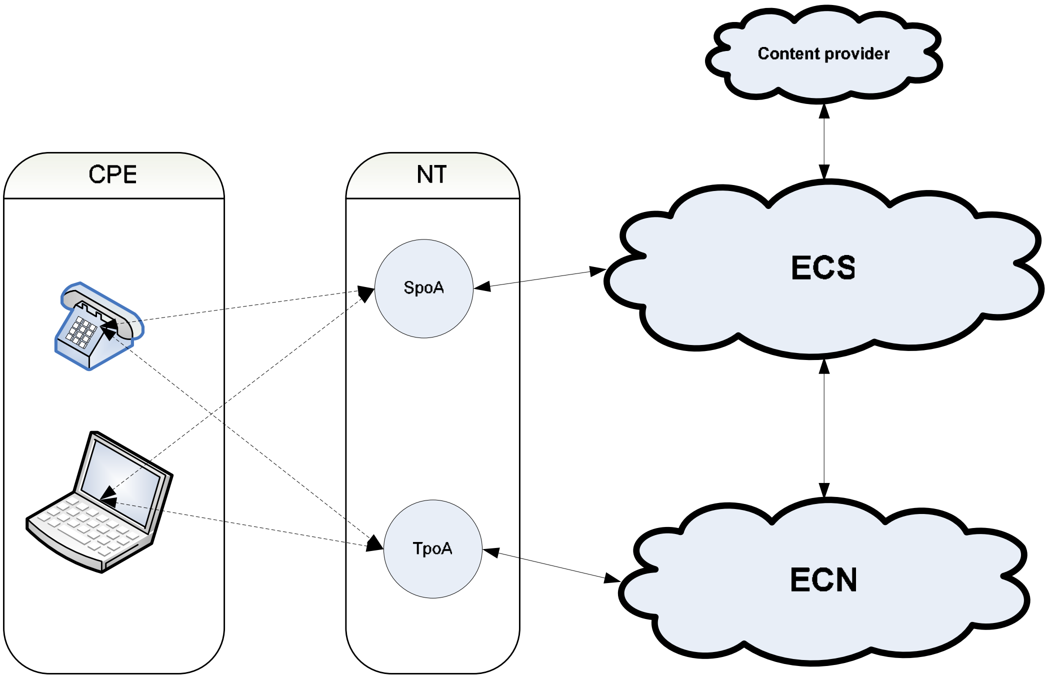

**Figure 5: ECN&S regulatory model for the Framework directive**

## 8.3 PES security requirement

The PES system links two trusted ISUP domains across a SIP/IP network. The PES shall provide assurance that the security in the SIP/IP link is equivalent to that provided in each of the connected ISUP domains. As the traffic enters the SIP/IP network from the ISUP domains, we assume the following:

Assumption 1: All user signalling is translated from ISDN/PSTN to ISUP and encapsulated in SIP.

Assumption 2: The user content is translated from TDM to RTP over UDP for carriage over the IP domain.

In order to provide the equivalent security, the control plane (SIP signalling) and the data plane (RTP traffic) have to be secured. However, the data plane protection for PES is not yet examined and will not be part of NGN Release 1.

### 8.3.1 PSTN/ISDN security provisions

There is no explicit authentication of terminals in the ISDN/PSTN as a terminal is assumed to be fixed in a location and the registered keeper of the terminal is contractually bound to pay for calls originating from that terminal. In most cases, the individual responsible for the bill is collocated with the terminal. Basic security is provided by the existence of a wire connection to the terminal which can be physically protected and which is difficult to move. Furthermore, the link from terminal to exchange traverses only cables and devices which are physically protected (this is the link behind network termination and hence not in scope of this document). Although wire tapping is feasible as a means of intercepting calls between a terminal and an exchange, this can prove to be difficult as access to the wires requires access to the end user premises or to cables buried underground. Confidentiality in the PSTN/ISDN is provided in large part by these physical mechanisms that make interception difficult and the fact that the wires carrying the user signalling and traffic do not broadcast. Message integrity is not guaranteed in PSTN/ISDN as the error rate of the physical network is considered to be low and, thus, the scope for performing manipulation attacks is also low.

### 8.3.2 SIP and SIP-I security requirements

In contrast to the PSTN/ISDN the generic Internet is a mesh connecting untrusted nodes at which routing decisions are made. There are two ways to consider the carriage of SIP-I for PES with respect to the transit network:

- Trusted network (with preferred routing):
    - Route selection based upon data elements from the ISUP message.
- Untrusted network.

Trusted networks could be of two types. It could be a single operator trusted network where the transit networks are owned by a single operator. If many operators with transit networks are involved, they should mutually trust each other.

The use of an untrusted network in PES may lead to loss of availability of the network if routing delays or packet losses are high. As such, the PES should use only trusted networks for the carriage of SIP-I; however, there are mechanisms which can change an un-trusted network to a trusted network.

Trust in the SIP/SIP-I network may be provided by authentication of the SIP-agent acting as the O-IWU to the SIP-agent acting as the I-IWU (authentication should be performed in each direction as a single SIP-agent may act as both O-IWU and I-IWU). The SIP/SIP-I network carries the ISUP message in the message body of the SIP message and as integrity is not guaranteed across SIP/SIP-I networks integrity checking may be added to the SIP message body which along with source/destination authentication will ensure that the transferred ISUP message is received without modification.

## 8.4 SIP security mechanisms

### 8.4.1 Overview

SIP security is possible in a number of ways either at the SIP (ECS) level or by utilizing capabilities inherent in the transport (ECN).

NOTE 1: Native security protocols are those that exist exclusively for SIP and in the ECS domain.

If SIP is used as a preamble to a second transaction (i.e. creates a session within which other protocols may be used and sub-sessions created) the security measures associated with SIP may be considered less important than those of the subsequent session.

NOTE 2: In the NGN environment this outer-session view may not be valid as SIP is used to replace existing protocols.

### 8.4.2 Authentication

Authentication of system entities in SIP can be accomplished by means of the "HTTP Digest" scheme.

SIP defines the "Authorization" header which contains a signature computed across those components of the SIP message which do not change in transit between proxies, as follows:

- the nonce;
- the realm;
- the request method (the type of request message dispatched by a user agent client);
- the request method version; and
- the authorization type.

In the context of SIP-I, the user is not aware that signalling is transported by SIP and hence, if HTTP digest authentication has to be used, the in-coming and the out-going IWUs have to be suitably configured. As the SIP and HTTP protocols are "text" based it is noted that the 128-bit MD5 checksum used by default is represented as a string of 32 ASCII printable characters.

### 8.4.3 Confidentiality

Confidentiality is accomplished within SIP (as elsewhere) by use of encryption. However, there are a few restrictions that preclude total confidentiality. Critical headers in the SIP message, such as the TO and FROM fields, which are interpreted by intermediate devices (proxies), cannot be encrypted end-to-end. For this reason, lower layer security implementations (such as VPNs) would need to be considered for global end-to-end security across an Internet. SIP messages pass through intermediate stations, which by default would not be able to interpret fully encrypted transactions at the application layer.

### 8.4.4 Use of S/MIME in SIP-I

The message body in SIP is defined using MIME [34] and as such the message bodies may be secured (giving assurance of confidentiality and integrity) using the mechanisms of S/MIME (RFC 2633 [32]). S/MIME can be tailored for those cases where no user intervention is required which is the normal case where the SIP-agent acts as either O-IWU or I-IWU. However, there are some problems associated with the usage of S/MIME for SIP-I protection:

1) The headers of the SIP-I messages carrying the ISUP messages need to be protected. SIP headers are not protected by the normal usage of S/MIME with SIP. The only way to protect it is by tunnelling the SIP header in the MIME bodies. This SIP tunnelling for protection of SIP header will create additional overhead.

2) If SIP tunnelling is used, the usage of TCP is recommended because of the larger message size. This reduces our choice for transport protocol.

3) S/MIME requires certificates and private keys to be used. Lack of a prevalent public key infrastructure will create serious problems. If self-signed certificates are used, the key exchange mechanisms are susceptible to man-in-the-middle attacks whereby an attacker can potentially inspect and modify S/MIME bodies. The attacker needs to intercept the first exchange of keys between the two parties in a dialog, remove the existing signatures from the request and response, and insert a different signature containing a certificate supplied by the attacker. Each party will think they have exchanged keys with the other, when in fact each has the public key of the attacker RFC 3261 [35]. It is however not known if this PKI infrastructure will be available if in case the transit network is untrusted.

## 8.5 Non-SIP security mechanisms

### 8.5.1 ECS mechanisms for security

The most obvious non-SIP mechanism is TLS. RFC 3261 [35] mandates the usage of TLS for proxies, redirect servers and registrars. Methods for use of TLS are already defined in IETF.

#### 8.5.1.1 ECN mechanisms for security

The most obvious ECN mechanism to apply is IPsec and in 3GPP the SEG function covers the requirement. The calling party domain and the called party domain may deploy SEG at the edge of their networks.

## 8.6 RTP security

The PES should protect the data traffic in order to provide assurance that the security in the IP link is equivalent to that provided in each of the connected ISUP domains. In trusted networks, RTP traffic can be either end-to-end/end-to-middle encrypted. However, if there are many transit networks, repeated encryption and decryption might affect real-time traffic. No solution has been identified in scope of NGN Release 1.

Trust for the data traffic may be provided by authentication. The RTP traffic (which was initially converted from TDM), should include security mechanisms which provide integrity, confidentiality and authentication. Security for the data plane could be provided either at application level or at IP level.

## 8.7 Conclusions

If many operators with transit networks are involved, they should mutually trust each other.

Trust in the SIP/SIP-I network may be provided by mutual authentication of the SIP-agents.

The only way to protect SIP headers using S/MIME is by tunnelling the SIP header in the MIME body. This SIP tunnelling for the protection of SIP headers will create additional overhead. In addition, S/MIME requires certificates and private keys to be used.

The PES should protect the data traffic in order to provide assurance that the security in the IP link is equivalent to that provided in each of the connected ISUP domains. No solution has been identified in scope of NGN Release 1.

# 9 Summary of conclusions

The findings presented in the preesent document are that in a small number of areas further standardization work is required to ensure that the PES is able to satisfy the requirements set by regulation or by current practice to ensure seamless transition for PSTN/ISDN consumers to PES.

Further work is required in the areas of:

- Bearer support (clause 5.1.1.1).
- Number Portability (clause 5.2.3).
- Call Completion to Busy Subscriber (CCBS) (clause 5.3.17).
- Security analysis and provision (clause 8).
- Clarification of the interpretation of missing specifications to clauses of ITU-T Recommendation H.248.1 [29].

The scope of the additional standards work is identified in the clauses shown.

# 10 Recommendations

## 10.1 Media not supported by EN 383 001

Because of the complexity of multiple timeslot assignments, there are few, if any, standards-based implementations of multi-rate bearer services in existing public networks. It is, therefore, recommended that multi-rate bearer services be not offered in the NGN Release 1 PSDN/ISDN Emulation Service.

## 10.2 Number Portability (NP)

As the procedures according to annex A of EN 302 097 [8] are only conditionally incompatible with the specifications for NGN Release 1, it is recommended that the procedures in annex A are not deployed in the NGN Release 1 PSDN/ISDN Emulation Service.

As the procedures according to annex B of EN 302 097 [8] are completely incompatible with the specifications for NGN Release 1, it is recommended that the procedures in annex B are not deployed in the NGN Release 1 PSDN/ISDN Emulation Service.

As onward routing may lead to undesirable multiple transcoding situations, it is recommended that the QoR (query on release) method according to annex C of EN 302 097 [8] be deployed in the NGN Release 1 PSDN/ISDN Emulation Service.

## 10.3 CCBS and CCNR supplementary services

Because of its complexity, there are, in fact, few standards-based implementations of CCBS in existing public networks. Consequently, it is probably unnecessary to spend any significant effort in specifying the use of CCBS in the NGN PES. It is recommended to await the specification of a genuine NGN CCBS service which could be used directly in the interworking of ISUP CCBS with PES, PSS, and IMS.

## 10.4 Profiles to ITU-T Recommendation H.248.1

To avoid interpretation conflict, it is recommended to amend both profiles by indicating explicitly the non-applicability of clauses of ITU-T Recommendation H.248.1 [29] at the next revision of the present document.

## 10.5 Security analysis and provision

The use of S/MIME [32] to protect ISUP messages contained in the body of SIP messages is NOT recommended for the following reasons:

- Untrusted networks between in-coming and out-going Interworking units (NNI interface) require that the PKI CA problems can be adequately resolved.

- Usage of S/MIME is inefficient when SIP headers have to be protected.

The use of HTTP-Digest is NOT recommended as it offers no real cryptographic strength to the payload.

The use of TLS or IPsec satisfies the requirements for protecting ISUP over SIP-I. As the security is not in SIP plane, the scenario should ensure the provision of security.

No additional security mechanisms need to be defined in PES for ISUP encapsulation in SIP-I. The data plane protection needs further work. The RTP security can be scoped as a post Release-1 issue.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | December 2005 | Publication |
| | | |
| | | |
| | | |
| | | |