ETSI TR 124 969 V12.0.0 (2015-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Business Trunking;
NGCN-NGN Interfaces Implementation Guide
(3GPP TR 24.969 version 12.0.0 Release 12)

Reference
DTR/TSGC-0124969vc00

Keywords
LTE,UMTS

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

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://ipr.etsi.org).

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 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The purpose of the present document is to give an implementation guide to the relevant Common IMS specifications and functions used in the interconnection of a Next Generation Corporate Network site (NGCN site) to the NGN.

The present document addresses control plane signalling (usage of SIP and SDP protocols, required SIP headers) as well as other interconnecting aspects like security, numbering/naming/addressing and user plane issues such as transport protocol, media and codecs actually covered in a widespread set of 3GPP and ETSI TISPAN specifications, as seen from the perspective of an NGCN site.

Advice-of-charge aspects are addressed as far as SIP signalling is concerned.

The present document is based on 3GPP TS 24.229 [12].

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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

[2] 3GPP TS 22.519: "; Business communication requirements, stage 1".

[3] 3GPP TS 24.525: "Business trunking; Architecture and functional description".

[4] 3GPP TS 24.523: "Core and enterprise NGN interaction scenarios; Architecture and functional description".

[5] IETF RFC 2976 (2000): "The SIP INFO Method".

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

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

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

[9] IETF RFC 6665 (2012): "Session Initiation Protocol (SIP) Specific Event Notification".

[10] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[11] IETF RFC 3903: "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[12] 3GPP TS 24.229: " Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 ".

[13] IETF RFC 791 (1981): "DARPA Internet Program Protocol Specification".

[14] IETF RFC 2460 (1998): "Internet Protocol, Version 6 (IPv6) Specification".

[15] Void.

[16] ETSI ES 282 001 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[17] 3GPPTS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".

[18] IETF RFC 3966 (2004): "The tel URI for Telephone Numbers".

[19] IETF RFC 3860 (2004): "Common Profile for Instant Messaging (CPIM)".

[20] IETF RFC 3859 (2004): "Common Profile for Presence (CPP)".

[21] 3GPP TS 29.162: "Interworking between IM CN Sub-system and IP networks".

[22] ECMA TR/96 "NGCN-Identity: "Next Generation Corporate Networks (NGCN) - Identification and routing".

[23] IETF RFC 3841 (2004): "Caller Preferences for the Session Initiation Protocol (SIP)".

[24] IETF RFC 6442 (December 2011): "Location Conveyance for the Session Initiation Protocol".

[25] IETF RFC 7044 (2014): "An Extension to the Session Initiation Protocol (SIP) for Request History Information".

[26] IETF RFC 3911 (2004): "The Session Initiation Protocol (SIP) "Join" Header".

[27] IETF RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

[28] IETF RFC 7315 (2014): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

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

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

[31] IETF RFC 3326 (2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[32] IETF RFC 3329 (2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[33] IETF RFC 3892 (2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[34] IETF RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[35] IETF RFC 5002 (2007): "The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)".

[36] IETF RFC 4457 (2006): "The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-header)".

[37] IETF RFC 3313 (2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[38] IETF RFC 5009 (2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[39] IETF RFC 3891 (2004): "The Session Initiation Protocol (SIP) "Replaces" Header".

[40] IETF RFC 4412 (2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[41] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

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

[43] IETF RFC 3856 (2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[44] IETF RFC 4662 (2006): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

[45] IETF RFC 3680 (2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[46] IETF RFC 5628 (October 2009): "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs)".

[47] IETF RFC 3857 (2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[48] IETF RFC 5875 (May 2010): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".

[49] IETF RFC 4575 (2006): "A Session Initiation Protocol (SIP) Event Package for Conference State".

[50] IETF RFC 3842 (2004) "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)".

[51] IETF RFC 4354 (2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".

[52] 3GPP TS 33.203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services ".

[53] IETF RFC 5393 (2008): "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies".

[54] IETF RFC 3312 (2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[55] IETF RFC 4032 (2005): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

[56] IETF RFC 3327 (2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[57] IETF RFC 3608 (2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[58] IETF RFC 3581 (2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[59] IETF RFC 3840 (2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[60] IETF RFC 5079 (December 2007): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".

[61] IETF RFC 4320 (2006): "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction".

[62] IETF RFC 5031 (2008): "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[63] IETF RFC 5627 (2009): "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)".

[64] Void.[65] IETF RFC 5626 (2009): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

[66] IETF RFC 4964 (2007): "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular".

[67] IETF RFC 4733 (2006): "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals".

[68] IETF RFC 3388 (2002): "Grouping of Media Lines in the Session Description Protocol (SDP)".

[69] IETF RFC 3524 (2003): "Mapping of Media Streams to Resource Reservation Flows".

[70] IETF RFC 3556 (2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[71] IETF RFC 4145 (2005): "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[72] IETF RFC 5245 (2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[73] IETF RFC 4583 (2006): "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams".

[74] IETF RFC 4585 (2006): " Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)".

[75] IETF RFC 5939 (2010): "Session Description Protocol (SDP) Capability Negotiation".

[76] IETF RFC 4566 (2006): "SDP: Session Description Protocol".

[77] IETF RFC 7316 (2014): "The Session Initiation Protocol (SIP) P-Private-Network-Indication Private-Header (P-Header)".

[78] IETF RFC 4119 (2005): "A Presence-based GEOPRIV Location Object Format".

[79] ETSI TS 181 005 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[80] 3GPP TS 24.647: "Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem".

[81] IETF RFC 6086 (October 2009): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

[82] IETF RFC 3324 (2002): "Short Term Requirements for Network Asserted Identity".

[83] Void.

[84] Void.

[85] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

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

[87] IETF RFC 5621 (2009): "Message Body Handling in the Session Initiation Protocol (SIP)".

[88] ECMA TR/100: "Next Generation Corporate Networks (NGCN) - Security of Session-based Communications".

[89] ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".

[90] 3GPP TS 124 173: "IMS Multimedia telephony service and supplementary services; Stage 3".

[91] RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP)".

[92] IETF Draft-dawes-sipping-debug-02 (February 2010): "Private Extension to the Session Initiation Protocol (SIP) for Debugging".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[93] Void.

[94] 3GPP TR 23.812: "3rd Generation Partnership Project (3GPP), Feasibility Study on IMS Evolution".

[95] TR-69: "CPE WAN Management Protocol v1.1".

[96] TR-104: "DSLHome™ Provisioning Parameters for VoIP CPE".

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

[98] IETF RFC 6228 (2011): "Response Code for Indication of Terminated Dialog".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 180 000 [85], 3GPP TS 22.519 [2], 3GPP TS 24.525 [3] and the following apply:

NGCN Attachment Point: SIP entity inside the NGCN with a direct SIP interface to the NGN

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 180 000 [85], 3GPP TS 22.519 [2] and 3GPP TS 24.525 [3] apply.

4 Overview

4.1 Business Trunking architecture and protocols

Business trunking refers to an architecture where corporate networks appear to the NGN as an NGCN.

3GPP TS 24.525 [3] and 3GPP TS 22.519 [2] provide architecture and functional requirements for business trunking making use of IMS and foresee two main interconnection models: the subscription based approach, where the entry point to the IMS is the P-CSCF, and the peering based approach, where the entry point to the IMS is the IBCF.

In both arrangement scenarios, aiming to support business trunking, protocol interconnection has to occur between NGCN and NGN:

- at a control plane level, in order that IMS procedures can be supported;
- at a user plane level, where media streams are exchanged.

The management of IP multimedia sessions is achieved using SIP. The transport mechanism for both SIP session signalling and media is UDP or TCP over IPv4 (RFC 791 [13]) or IPv6 (RFC 2460 [14]); for signalling optionally also TLS over TCP.

The protocol behaviour of the NGN functional entities involved in the signalling plane interconnection (IBCF, P-CSCF) is specified in 3GPP TS 24.229 [12].

The protocol behaviour of the NGCN is also expected to follow 3GPP TS 24.229 [12], subject to the applicable interconnection scenario:

- for the subscription-based approach the behaviour is based on the rules for a UE;
- for the peering-based approach the NGCN site appears to the NGN as if it were an IBCF complying with the requirements identified in 3GPPTS 24.229 [12], subclause 4.1 for this functional entity.

The present document presents guidelines for NGCNs connecting to an NGN for the purpose of business trunking.

NOTE: A given NGCN can have multiple business trunking arrangements with the same NGN or with different NGNs, some using the subscription-based approach and others using the peering-based approach.

4.2 Roadmap to relevant specifications

The following specifications are relevant for the implementation of the NGCN-NGN interface:

- 3GPP TS 22.519 [2] provides Business Communication Requirements.
- 3GPP TS 24.523 [4] provides architecture and functional description of Core and enterprise NGN interaction scenarios.
- 3GPP TS 24.525 [3] gives architecture and functional description of Business trunking.
- 3GPP TS 24.229 [12] defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

4.3 Specification methodology

4.3.1 General

Clauses 5, 6 and 7 of the present document describe the various aspects of an NGN-NGCN interconnection, including a description of SIP and SDP procedures, and the SIP methods and header fields to be supported, in the form of a series of tables and description.

Aspects common to both the subscription-based and the peering-based scenario are described in clause 5. Considerations for a particular scenario are covered in clauses 6 and 7 respectively.

The tables summarize key aspects of IMS SIP used in business trunking and are aligned with similar tables available in annex A of 3GPP TS 24.229 [12]. Each of the tables in the present document include two "Status" columns, one for the sending side, one for the receiving side. The status entries represent the requirements on an NGCN acting as sender / as receiver of a SIP message. The present document is an informative document and as such does not specify any changes to SIP described in 3GPP TS 24.229 [12].

NOTE: The present document in some cases selects options from the baseline specifications. As an example, if the "status" column in the baseline specification indicates a condition for supporting a particular header field and that condition is always met by the implementation of the interface to an NGCN site then the "profile status" column for this header field is marked "mandatory" rather than "optional" or "conditionally mandatory" in the present document. Similarly if the "status" column in the baseline specification indicates that support of a particular header field is optional and the implementation of the interface to an NGCN site always require it then the "profile status" column for this header field is marked "mandatory" rather than "optional".

The notation for status codes is explained in subclause 4.3.2.

There are cases where the status of a method or a header field depends on capabilities supported at the NGCN-NGN interface. In such a case, the status indicated in the tables depends on the status of the respective capability, as described in subclause 4.4.

4.3.2 Notation for status codes

The following notations, defined in ISO/IEC 9646-7 [41], are used for the status column:

- m: mandatory - the capability is required to be supported.
- o: optional - the capability may be supported or not.
- n/a: not applicable - in the given context, it is impossible to use the capability.
- x: prohibited (excluded) - there is a requirement not to use this capability in the given context.

- o.i: qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer, which identifies a unique group of related optional items and the logic of their selection, which is defined immediately following the table.

- ci: conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "i" is an integer identifying a unique conditional status expression which is defined immediately following the table.

In the status columns of tables within subsequent sections, status codes m, o, c, x and n/a have the following meanings, as specified in the base standards, with the following qualifications:

- Conformance requirements are indicated in static terms, meaning that a behaviour indicated as mandatory shall be observed when the implementation is placed in conditions in which the conformance requirements of the reference specification compel it to do so. For instance, if the support for a header field in a sent message is indicated as mandatory, it does not mean that the NGCN shall always include that header field when sending the message concerned, but that the NGCN shall include that header field in the message concerned in circumstances specified in the reference specification.

- If support for a particular behaviour is required, there is no requirement for every SIP-capable entity within the NGCN to support that behaviour, but at least one element involved shall support that behaviour. For instance, if the support for a header field in a sent message is indicated as mandatory, it does not mean that all NGCN entities involved in handling the message to be sent shall support inclusion of that header field, but at least one NGCN entity shall be able to insert that header field such that it appears in the resulting message sent to the NGN.

- When appearing in a column relating to sending by an NGCN, the notation 'm' means that an NGCN shall support this capability when sending a message.

- When appearing in a column relating to receiving by an NGCN, the notation 'm' means that an NGCN shall support this capability when present in a received message.

- The notation 'o' means that the capability may or may not be supported by an NGCN, this being an implementation choice.

- When appearing in a column relating to sending by an NGCN, the notation 'n/a' means that there is no requirement for an NGCN to support this capability when sending a message.

- When appearing in a column relating to receiving by an NGCN, the notation 'n/a' means that there is no requirement for an NGCN to support this capability when present in a received message.

- When appearing in a column relating to sending by an NGCN, the notation 'x' means that an NGCN shall not use this capability when sending a message.

- When appearing in a column relating to receiving by an NGCN, the notation 'x' means that an NGCN shall ignore this capability when present in a received message.

4.4 Major capabilities at the NGCN-NGN interface

4.4.1 Service capabilities

Table 4.1 describes the Service Capabilities supported by NGCN at the NGCN-NGN interface.

Table 4.1: Major capabilities supported by NGCN at the NGCN-NGN interface

Item	Does the implementation support	Reference	Status
1	Advice of Charge as a Client	3GPP TS 24.525 [3], subclause 6.1.12	O
2	Multimedia telephony service	ETSI TS 124 173 [90]	O

4.4.2 Protocol capabilities

4.4.2.1 General

The NGCN is expected to support the following SIP capabilities under the stated circumstances.

4.4.2.2 Basic requirements

Session control: The support of INVITE initiated dialogs is mandatory if media sessions are supported across the NGCN - NGN interface where media can be any mix of audio, video, and application data. In subscription-based approach both UAC and UAS side procedures are applicable; in peering-based approach proxy procedures may apply as well.

Registration, client side: Mandatory when working in subscription mode, not applicable in peering mode.

Event notification framework: SUBSCRIBE/NOTIFY support is mandatory if any SIP event package is supported. Depending on the package the NGCN will act as subscriber or as notifier.

Event state publication: Support of the PUBLISH method is optional.

Messaging: Support of the MESSAGE method is mandatory if instant messages are supported. There is no specific use case specified in 3GPP TS 24.525 [3] that requires an NGCN to send the MESSAGE method.
See table 5.1 for details on the support of the MESSAGE method on sending and receiving sides. In 3GPP TS 23.228 [17] it is only specified for a UE to support Messaging, that implies that it is mandatory in the case of Subscription based approach.

UA-UA Authentication (Digest) (see [1], subclause 22.2): mandatory for REPLACES or JOIN else optional.

UA-Proxy Authentication (Digest) (see [1], subclause 20.28, 22.3): optional.

4.4.2.3 Extensions for session control

The following bullets list a number of SIP extensions and their status for the NGCN-NGN interface. The list is not exhaustive but contains all items relevant to the NGCN-NGN interface.

- Fixes for non-INVITE transactions (see [61]): mandatory.
- Fork-loop fixes (see [53]): mandatory if forking in NGCN is possible else not applicable.
- Reliable provisional responses (PRACK) (see [6]): mandatory if using session preconditions else optional.
- INFO method (see [5]): optional; required for AoC.
- REFER method, Referred-by header field (see [7], [33]): both optional.
- UPDATE method (see [8]): optional.
- Session Preconditions (for QoS) (see [54], [55]): mandatory if initiating a session requiring resource reservation else optional.
- Symmetric response routing (see [58]): optional.
- Caller preferences (see [23]): optional.
- Callee capabilities (see [59]): optional.
- Replaces (see [39]): optional.
- Join (see [26]): optional.
- P-Asserted-Identity (see [29]): mandatory.
- Privacy (see [30]): mandatory (privacy value 'id').

- P-Called-Party-ID (see [28]): optional; not applicable for peering mode.
- P-Access-Network-Info (see [28]): mandatory for GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN access types and optional for the others.
- Session timer (see [27]): optional.
- UA-UA and UA-Proxy Authentication (Digest) (see [1]): both optional.
- History-Info and privacy of history info (see [25]): optional.
- GRUUs (see [63]): optional.
- ICE (see [72]): optional.
- SIP Outbound (see [65]): optional.
- Location conveyance (see [24]): optional.
- Service URNs (e.g. 'sos') (see [62]): mandatory.
- Private Network Traffic (see [77]): optional.
- Authorization of Early Media (see [38]): optional.
- Identification of communication services extension (P-Preferred-Service) (see [34]): optional in the subscription-based approach, not applicable in the peering based approach.
- SIP extensions for media authorization ([37]): optional

4.4.2.4 Extensions for registration (subscription based approach only)

The following bullets list a number of SIP extensions and their status for the NGCN-NGN interface. The list is not exhaustive but contains all items relevant to the NGCN-NGN interface.

- **UA-Registrar Authentication** (see [1]): mandatory.
- **Session initiation protocol extension header field for registering non-adjacent contacts (Path header field)** (see [56]): mandatory. The support of the extension is indicated in the Supported header field sent by the NGCN. It is up to the NGCN whether it uses the Path header field received in the 200 OK response.
- **Reg-event package** (see [45]): mandatory.

Subscription to the reg-event package provided by the NGN enables the NGN with the following capabilities:

- informing the NGCN about the implicitly registered public user identities;
- informing the NGCN about the registration state of all explicitly and implicitly registered public user identities;
- forcing the NGCN at any time to perform re-registration after a NGN determined time (network initiated re-registration);
- network initiated de-registration of one or more registered public user identities of the NGCN.

NOTE 1: 3GPP TS 24.229 [12] mandates the support of the 'reg' event package. In particular the last two capabilities above are needed by the NGN operator e.g. in cases when the network wants to re-authenticate the user (network initiated re-registration) or when the S-CSCF needs to shut down for maintenance purposes and the user should register newly at a different S-CSCF (network initiated de-registration).

- **Session initiation protocol extension header field for service route discovery during registration (Service-Route header field)** (see [57]): mandatory. If the UE does not set the content of the Service-Route received during the last successful registration or re-registration, in a Route header field of an outgoing SIP Request, the P-CSCF may reject this request.

- **The P-Associated-URI header extension (P-Associated-URI header field)** (see [29]): mandatory.

NOTE 2: TS 24.229 [12] mandates the support of the P-Associated-URI header field to enable the NGN to provide to the UE the implicitly registered public user identities. There is no requirement in TS 24.525 [3] to use this header field inside the NGCN site.

- **Security mechanism agreement** (see [32]): mandatory if SIP Digest with TLS or IMS AKA plus IPsec ESP is used to secure the signalling exchange between the UE and the network else optional (see TS 24.229 [12], subclause 5.1.1.5, TS 33.203 [52], clause 6 and TS 33.203 [52], annexes N and O).

- **SIP extensions for media authorization** (see [37]): mandatory if initiating session and GPRS else n/a.

5 Common guidelines

5.1 Reference model for interconnection

The reference model for interconnection is scenario specific; refer to subclause 6.1 for the subscription-based approach and to subclause 7.1 for the peering based method of interconnection.

5.2 Control plane interconnection

5.2.1 SIP procedures

5.2.1.1 Outgoing requests from NGCN site

5.2.1.1.1 General

The following subclauses provide guidance on the expected NGCN site behaviour when sending a request to the NGN and receiving a response from the NGN. Allowed formats for URIs are listed in subclause 5.4, but other formats may possibly be used by agreement between enterprise and NGN.

The terms **trust**, **trusted by** and **trust domain** in the following subclauses are used as defined in RFC 3324 [82] and relate only to the handling of P-Asserted-Identity and Privacy:id header fields as specified in RFC 3325 [29]. RFC 3324 [82] defines Spec (T) as the set of specifications and configuration settings that are used to ensure trust.

The trust relationship between NGCN sites and NGN is a matter of an SLA between enterprise and NGN operator. If according to the SLA the NGN and NGCN form part of the same trust domain, the SLA includes a Spec (T) applicable to the interconnection of NGCN and NGN. In this case the NGN trusts the NGCN site and vice versa (as described in RFC 3324 [82]). On the other hand the NGCN site may trust the NGN even if the NGCN site is not in the trust domain of the NGN.

NOTE 1: TS 24.525 [3] talks about trust only in the context of the NGN trusting the NGCN regarding the SIP header fields P-Asserted-Identity and related Privacy provided by the NGCN in a SIP request or SIP response.

NOTE 2: According to RFC 3324 [82], for an NGCN site outside the trust domain, trusting the NGN implies both secured signalling and knowledge that the peer NGN entity belongs to a recognized trust domain. As a consequence signalling that is not secured is equivalent to not trusting the NGN

NOTE 3: Trust is required if privacy applies; for identities that are not subject to privacy it is a matter of policy whether they are passed to a non-trusted node.

5.2.1.1.2 Calling and connected identifiers

When sending a request to the NGN the NGCN site can include a calling party identity in the P-Asserted-Identity header field in accordance with RFC 3325 [29].

NOTE 1: If included, the asserted identity is in addition to the identity provided by the calling party in the From header field.

The NGCN site can provide two P-Asserted-Identity header fields, one containing a SIP URI and the other containing a TEL URI, in order to provide alias identities for the calling party (see TS 22.519 [2]).

The handling of the P-Asserted-Identity header field(s) by the NGN depends on whether the NGN trusts the NGCN or not and on the scenario (subscription based or peering).

NOTE 2: If the NGN trusts the NGCN site it will accept a P-Asserted-Identity received from the NGCN.

A calling identifier in a From or P-Asserted-Identity header field is expected to comply with the formats listed in subclause 5.4 where an entity internal to the NGCN site is identified.

The NGCN site may receive a connected party identity in the P-Asserted-Identity header field in a 18x or 2xx final response depending on NGN policy and the trust relationship between NGN and NGCN.

5.2.1.1.3 Privacy

If the NGCN site requires privacy for the calling party identity it will include a Privacy:id header field when sending a request to the NGN.

NOTE 1: This header field asks the NGN not to send a P-Asserted-Identity to a recipient outside its trust domain.

NOTE 2: The calling party will also put an anonymous SIP URI into the From header field if privacy is required.

The NGCN site may insert a P-Asserted-Identity header field in addition to Privacy:id if it trusts the NGN. If the NGCN site does not trust the NGN the NGCN site will not include a P-Asserted-Identity for which privacy is required.

5.2.1.1.4 Called identifier

The To header field may contain any URI format. The Request-URI has to be in a format supported by the NGN for the request to be accepted. TS 24.229 [12] subclause 5.1.2A.1.2 gives information on the format of the Request-UR

5.2.1.2 Incoming requests to NGCN site

5.2.1.2.1 General

The following subclauses provide guidance on the common aspects of expected NGCN site behaviour when receiving a request from the NGN.

The text from subclause 5.2.1.1.1 on trust also applies here.

The supported URI formats are listed in subclause 5.4.

5.2.1.2.2 Calling identity

The NGCN site can receive a user provided calling identity in the From header field and an asserted calling identity in the P-Asserted-Identity header field. The P-Asserted-Identity can be accompanied by a Privacy:id header field if presentation of this identity is restricted and the NGN trusts the NGCN.

Conditions under which the NGN will send such identities depend on the availability of the information and on privacy requirements as specified in TS 24.525 [3] and TS 24.229 [12], and are also subject to an SLA between NGN and NGCN.

5.2.1.2.3 Called identity

The NGCN site may return a called party identity, which may or may not be one of the public user identities allocated to the NGCN site, in form of a P-Asserted-Identity header field in a 18x or 2xx response, as specified in TS 24.525 [3].

5.2.1.2.4 Request-URI

For an initial or standalone request the Request-URI will normally contain a public user identity assigned to the NGCN; an exception will be an initial call to a globally routable contact address, e.g. in the case of an emergency call-back.

NOTE: For a mid-dialog request the Request-URI will contain the target URI learned from the respective Contact header field at dialog establishment time or through the most recent target refreshment.

5.2.2 SIP protocol elements

5.2.2.1 General

NOTE: The status of some header fields and parameters described in this subclause may not be applicable in case of private network traffic. Further study is required to identify the list of header fields that must be supported to ensure proper handling of private traffic in the IMS.

5.2.2.2 Methods

Table 5.1 provides information on the SIP methods to be supported by the NGCN site for the connection to the NGN.

It is based on tables A.5 and A.163 of TS 24.229 [12] and considering Business Trunking specific requirements as described in TS 24.525 [3].

Table 5.1: Supported methods

Item	PDU	Sending		Receiving	
		Ref.	Profile Status	Ref.	Profile Status
1	ACK request	[1] 13	c2	[1] 13	c2
2	BYE request	[1] 15.1	c2	[1] 15.1	c2
3	BYE response	[1] 15.1	c2	[1] 15.1	c2
4	CANCEL request	[1] 9	m (note 3)	[1] 9	m (note 3)
5	CANCEL response	[1] 9	m (note 3)	[1] 9	m (note 3)
8	INVITE request	[1] 13	c2	[1] 13	c2
9	INVITE response	[1] 13	c2	[1] 13	c2
9A	MESSAGE request	[10]	M (note 5)	[10]	m (note 4)
9B	MESSAGE response	[10]	m (note 4)	[10]	m (note 5)
12	OPTIONS request	[5]	m	[5]	m
13	OPTIONS response	[5]	m	[5]	m
14	PRACK request	[6]	o	[6]	o
15	PRACK response	[6]	o	[6]	o
15A	PUBLISH request	[11]	o (note 2)	[11]	o (note 2)
15B	PUBLISH response	[11]	o (note 2)	[11]	o (note 2)
16	REFER request	[7]	o (note 1)	[7]	o (note 1)
17	REFER response	[7]	o (note 1)	[7]	o (note 1)
22	UPDATE request	[8]	o	[8]	o
23	UPDATE response	[8]	o	[8]	o
24	INFO request	[5]	c1	[5]	c1
24	INFO response	[5]	c1	[5]	c1
c1:	IF 4.1/1 THEN m ELSE o - AoC.				
c2:	IF the NGCN site supports session based services THEN m ELSE n/a.				
NOTE 1:	Use of the REFER method is expected to be in conjunction with call transfer or conference, for example, when exposed at the NGCN-NGN interface.				
NOTE 2:	Use of the PUBLISH method is expected to be in conjunction with presence, for example, when exposed at the NGCN-NGN interface.				
NOTE 3:	TS 24.229 [12] mandates the support of the CANCEL request but the use of this request is linked to the use of the INVITE request which status is conditional. The status should be "c2".				
NOTE 4:	TS 23.228 [17], subclause 5.4.9.0 requires AS or S-CSCF to be able to send information to UEs using SIP based messages.				
NOTE 5:	There is no mandated circumstance requiring that an NGCN site needs to send a MESSAGE request unless it supports IM or unless retargeting causes a received MESSAGE request to be redirected back to the NGN.				

According to subclause 21.5.2 of [1] if the NGCN site receives unknown SIP method from the NGN, it answers with a 501 (Not implemented) response.

5.2.2.3 Responses

The NGCN site has to be prepared to send and receive SIP responses listed in TS 24.229 [12], annex A, as described in table 5.2.

Table 5.2: Supported response codes

Item	Header	Ref.	Sending	Receiving	Comments
1	100 (Trying)	[1] 21.1.1	o	m	
2	180 (Ringing)	[1] 21.1.2	o	m	Only applicable for INVITE response.
3	181 (Call Is Being Forwarded)	[1] 21.1.3	o	m	Only applicable for INVITE response.
4	182 (Queued)	[1] 21.1.4	o	m	Only applicable for INVITE response.
5	183 (Session Progress)	[1] 21.1.5	o (see note)	m	Only applicable for INVITE response.
5A	199 (Early Dialog Terminated)	[yy] 11.1	m	m	Only applicable for INVITE response.
6	200 (OK)	[1] 21.2.1	m	m	
7	202 (Accepted)	[9] 8.3.1	c1	c1	
8	300 (Multiple Choices)	[1] 21.3.1	m	m	
9	301 (Moved Permanently)	[1] 21.3.2	m	m	
10	302 (Moved Temporarily)	[1] 21.3.3	m	m	
11	305 (Use Proxy)	[1] 21.3.4	m	m	Not commonly used by NGCNs.
12	380 (Alternative Service)	[1] 21.3.5	m	m	Not commonly used by NGCNs.
13	400 (Bad Request)	[1] 21.4.1	m	m	
14	401 (Unauthorized)	[1] 21.4.2	o	m	
15	402 (Payment Required)	[1] 21.4.3	n/a	n/a	
16	403 (Forbidden)	[1] 21.4.4	m	m	
17	404 (Not Found)	[1] 21.4.5	m	m	
18	405 (Method Not Allowed)	[1] 21.4.6	m	m	
19	406 (Not Acceptable)	[1] 21.4.7	m	m	
20	407 (Proxy Authentication Required)	[1] 21.4.8	o	m	
21	408 (Request Timeout)	[1] 21.4.9	o	m	Optionally sent in an INVITE response.
22	410 (Gone)	[1] 21.4.10	m	m	
22A	412 (Conditional Request Failed)	[11] 11.2.1	c2	c2	
23	413 (Request Entity Too Large)	[1] 21.4.11	m	m	
24	414 (Request-URI Too Large)	[1] 21.4.12	m	m	
25	415 (Unsupported Media Type)	[1] 21.4.13	m	m	
26	416 (Unsupported URI Scheme)	[1] 21.4.14	m	m	
27	420 (Bad Extension)	[1] 21.4.15	m	m	
28	421 (Extension Required)	[1] 21.4.16	o	m	
28A	422 (Session Interval Too Small)	[27] 6	c 3	c 3	
29	423 (Interval Too Brief)	[1] 21.4.17	c4	c4	
29A	424 (Bad Location Information)	[24] 3.3	c 5	c5	
29B	429 (Provide Referrer Identity)	[33] 5	c6	c7	
29C	430 (Flow Failed)	[65] 11	n/a	c8	
29D	433 (Anonymity Disallowed)	[60] 4	c9	o	ACR currently not required by TS 24.525 [3] stage 2.
30	480 (Temporarily Unavailable)	[1] 21.4.18	m	m	
31	481 (Call/Transaction Does Not Exist)	[1] 21.4.19	m	m	
32	482 (Loop Detected)	[1] 21.4.20	m	m	
33	483 (Too Many Hops)	[1] 21.4.21	m	m	
34	484 (Address Incomplete)	[1] 21.4.22	o	m	
35	485 (Ambiguous)	[1] 21.4.23	o	m	
36	486 (Busy Here)	[1] 21.4.24	m	m	
37	487 (Request Terminated)	[1] 21.4.25	m	m	
38	488 (Not Acceptable Here)	[1] 21.4.26	m	m	
39	489 (Bad Event)	[9] 7.3.2	c10	c10	
40	491 (Request Pending)	[1] 21.4.27	m	m	
41	493 (Undecipherable)	[1] 21.4.28	m	m	
41A	494 (Security Agreement Required)	[32] 2	n/a	c 11	
42	500 (Internal Server Error)	[1] 21.5.1	m	m	
43	501 (Not Implemented)	[1] 21.5.2	m	m	
44	502 (Bad Gateway)	[1] 21.5.3	o	m	

Item	Header	Ref.	Sending	Receiving	Comments
45	503 (Service Unavailable)	[1] 21.5.4	m	m	
46	504 (Server Time-out)	[1] 21.5.5	m	m	
47	505 (Version not supported)	[1] 21.5.6	m	m	
48	513 (Message Too Large)	[1] 21.5.7	m	m	
49	580 (Precondition Failure)	[54] 8	o	o	.
50	600 (Busy Everywhere)	[1] 21.6.1	m	m	
51	603 (Decline)	[1] 21.6.2	c 12	m	
52	604 (Does Not Exist Anywhere)	[1] 21.6.3	m)	m	
53	606 (Not Acceptable)	[1] 21.6.4	m	m	
c1:	If SUBSCRIBE or REFER then m else o.				
c2:	If PUBLISH then m else n/a.				
c3:	If session-timer then m else n/a.				
c4:	If REGISTER or SUBSCRIBE then m else n/a.				
c5:	If location-conveyance then m else n/a.				
c6:	If REFER and referred-by then o else n/a.				
c7:	If REFER and referred-by then m else n/a.				
c8:	If outbound then m else n/a.				
c9:	If ACR then m else n/a.				
c10:	If SUBSCRIBE or NOTIFY then m else n/a.				
c11:	If security-agreement then m else n/a.				
c12:	If INVITE/replaces then m else o.				
NOTE:	The sending of this response code is needed in case of initiating a session which requires local and/or remote resource reservation (Session Preconditions for QoS).				

5.2.2.4 Header fields

5.2.2.4.1 General

The following subclauses list header fields with a specific relevance in a business trunking context. The usage of these header fields follows normal SIP rules, with some additional qualifications as described below.

5.2.2.4.2 Accept

As specified in TS 24.525 [3], if the agreement between the NGN and the NGCN specifies that an NGCN site receives advice of charge information, this header field indicates the support of MIME bodies of type "application/vnd.etsaoc+xml" defined in TS 24.647 [80].

5.2.2.4.3 Allow

As specified in TS 24.525 [3], if the agreement between the NGN and the NGCN specifies that an NGCN site receives advice of charge information, this header field indicates the support of the INFO method.

5.2.2.4.4 Contact

In an outgoing dialog initiating or target refresh request this header field contains the target URI within the NGCN (which can be different from the public user identities assigned to the NGCN site) for receiving subsequent mid-dialog requests. This URI may also be suitable for receiving future out-of-dialog requests.

In a 2xx final response to an incoming dialog initiating or target refresh request this header field contains the target URI within the NGCN (which can be different from the public user identities assigned to the NGCN site) for receiving subsequent mid-dialog requests. This URI may also be suitable for receiving future out-of-dialog requests.

5.2.2.4.5 Max-Breadth

As an NGCN site may comprise multiple SIP entities, the Max-Breadth header field can prevent loops by limiting forking within the NGCN site.

5.2.2.4.6 Max-Forwards

As an NGCN site may comprise multiple SIP entities, the Max-Forwards header field can prevent loops by limiting the number of nodes that can forward the request within the NGCN site.

5.2.2.4.7 P-Private-Network-Indication

As stated in TS 24.525 [3], the NGN can include a Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [77] in an initial request or standalone request to the NGCN site, and the NGCN site can include this header field in an initial request or standalone request to the NGN.

5.2.2.4.8 Record-Route

As an NGCN site may comprise multiple SIP entities, this header field may be populated by entities within the NGCN site

- in a dialog initiating request sent to the NGN;
- in a response to a dialog initiating request received from the NGN.

When internally received by the NGCN attachment point, this header field has to be passed on by the attachment point and the attachment point can also add its own Record-Route header field.

5.2.2.4.9 Route

As an NGCN site may comprise multiple SIP entities, the header field may contain additional URIs addressing nodes within the NGCN site in a request received from the NGN.

NOTE: The NGN may know the route set within the NGCN site from a Record-Route received earlier on the same dialog, through configuration, or from a Path header field received during registration when working in subscription mode.

5.2.2.4.10 Via

As an NGCN site may comprise multiple SIP entities, this header field may be populated by multiple entities within the NGCN site in an outgoing request to the NGN.

5.2.2.4.11 Summary of message headers

The following tables provide information on the SIP header fields to be supported by the NGCN site for the interconnection to the NGN.

As per the procedures specified in RFC 3261 [1], the NGCN site shall ignore received unknown SIP header fields and unknown header field parameters and continue processing the request or response where they were contained.

The tables below are based on clause A.2 of TS 24.229 [12] and considering Business Trunking specific requirements as described in TS 24.525 [3].

Table 5.3: Supported headers within the ACK request

Item	Header	Ref.	Sending	Receiving	Content / Comment
1	Accept-Contact	[23] 9.2	c5	c6	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authorization	[1] 20.7	c3	c3	
4	Call-ID	[1] 20.8	m	m	
6	Content-Disposition	[1] 20.11	o	m	
7	Content-Encoding	[1] 20.12	o	m	
8	Content-Language	[1] 20.13	o	m	
9	Content-Length	[1] 20.14	m	m	
10	Content-Type	[1] 20.15	m	m	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	From	[1] 20.20	m	m	
13A	Max-Breadth	[53] 5.8	o	c1	
14	Max-Forwards	[1] 20.22	m	c2	
15	MIME-Version	[1] 20.24	o	m	
15A	Privacy	[30] 4.2	n/a	n/a	
16	Proxy-Authorization	[1] 20.28	c4	n/a	
17	Proxy-Require	[1] 20.29	n/a	n/a	
17A	Reason	[31] 2	o	o	
17B	Reject-Contact	[23] 9.2	c5	c6	
17C	Request-Disposition	[23]] 9.1	c5	c6	
18	Require	[1] 20.32	n/a	n/a	
19	Route	[1] 20.34	m	c2	
20	Timestamp	[1] 20.38	o	m	
21	To	[1] 20.39	m	m	
22	User-Agent	[1] 20.41	o	o	
23	Via	[1] 20.42	m	m	
c1:	IF forking is possible within the NGCN THEN m ELSE n/a.				
c2:	IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.				
c3:	IF UA-UA Authentication is used THEN m ELSE o.				
c4:	IF UA-Proxy Authentication is used THEN m ELSE o.				
c5:	IF Caller Preferences extension is supported THEN o ELSE n/a.				
c6:	IF Caller Preferences extension is supported THEN m ELSE n/a.				

Table 5.4: Supported headers within the BYE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
1A	Accept-Contact	[23] 9.2	c7	c8 (see note)	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
3A	Allow	[1] 20.5	o	m	
4	Allow-Events	[9] 7.2.2	o	m	
5	Authorization	[1] 20.7	c3	c3	
6	Call-ID	[1] 20.8	m	m	
7	Content-Disposition	[1] 20.11	o	m	
8	Content-Encoding	[1] 20.12	o	m	
9	Content-Language	[1] 20.13	o	m	
10	Content-Length	[1] 20.14	m	m	
11	Content-Type	[1] 20.15	m	m	
12	Cseq	[1] 20.16	m	m	
13	Date	[1] 20.17	o	m	
14	From	[1] 20.20	m	m	
14A	Geolocation	[24] 3.2	o	o	
14B	Max-Breadth	[53] 5.8	o	c1	
15	Max-Forwards	[1] 20.22	m	c5	
16	MIME-Version	[1] 20.24	o	m	
16A	P-Access-Network-Info	[28] 4.4	c2	n/a	
16B	P-Asserted-Identity	[29] 9.1	c6	o	This header is part of the SLA between the enterprise and the operator (on the support or not of a trusted connection).
16C	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
16D	P-Charging-Vector	[8] 4.6	n/a	n/a	
16E	P-Preferred-Identity	[29] 9.2	n/a	n/a	
16F	Privacy	[30] 4.2	o	c12	(See note 2).
17	Proxy-Authorization	[1] 20.28	c4	n/a	
18	Proxy-Require	[1] 20.29	o	m	Values equal to those in NVITE request.
18A	Reason	[31] 2	o	o	
19	Record-Route	[1] 20.30	n/a	n/a	
19A	Referred-By	[33] 3	c9	c10	
19B	Reject-Contact	[23] 9.2	c7	c8 (see note 1)	
19C	Request-Disposition	[23] 9.1	c7	c8 (see note 1)	
20	Require	[1] 20.32	m	m	Values equal to those in INVITE request.
21	Route	[1] 20.34	m	c5	
22	Supported	[1] 20.37	m	m	
23	Timestamp	[1] 20.38	o	m	
24	To	[1] 20.39	m	m	
25	User-Agent	[1] 20.41	o	o	
26	Via	[1] 20.42	m	m	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF the access type is GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN THEN m ELSE o.
c3: IF UA-UA Authentication is used THEN m ELSE o.
c4: IF SIP digest is used THEN m ELSE o.
c5: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c6: IF the NGCN site can be deployed in an environment where it is trusted THEN o ELSE n/a.
c7: IF Caller Preferences extension is supported THEN o ELSE n/a.
c8: IF Caller Preferences extension is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN m ELSE n/a.
c10: IF Referred-By mechanism is supported THEN o ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.

NOTE 1: There is no use case for receiving Accept-Contact, Reject-Contact and Request-Disposition headers in BYE request.
NOTE 2: Privacy is for further study in TS 24.525 [3].

Table 5.5: Supported headers within the 200 OK response to the BYE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authentication-Info	[1] 20.6	o	m	
4	Call-ID	[1] 20.8	m	m	
5	Content-Disposition	[1] 20.11	o	m	
6	Content-Encoding	[1] 20.12	o	m	
7	Content-Language	[1] 20.13	o	m	
8	Content-Length	[1] 20.14	m	m	
9	Content-Type	[1] 20.15	m	m	
10	Cseq	[1] 20.16	m	m	
11	Date	[1] 20.17	o	o	
12	From	[1] 20.20	m	m	
14	MIME-Version	[1] 20.24	o	m	
15	P-Access-Network-Info	[28] 4.4	c2	c2	
16	P-Asserted-Identity	[29] 9.1	n/a	c1	
17	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
18	P-Charging-Vector	[28] 4.6	n/a	n/a	
19	P-Preferred-Identity	[30] 9.2	n/a	n/a	
20	Privacy	[31] 4.2	o	c3	(See note)
21	Require	[1] 20.32	m	m	
22	Server	[1] 20.35	o	o	
23	Supported	[1] 20.37	m	m	
24	Timestamp	[1] 20.38	m	o	
25	To	[1] 20.39	m	m	
26	User-Agent	[1] 20.41	o	o	
27	Via	[1] 20.42	m	m	
28	Warning	[1] 20.43	o	o	
c1: IF the NGCN site can be deployed in an environment where it is trusted THEN "o" ELSE "n/a".					
c2: IF the access type is GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN THEN "m" ELSE "o".					
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.					
NOTE: Privacy is for further study.					

Table 5.6: Supported headers within the CANCEL request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept-Contact	[23] 9.2	c3	c4	
5	Authorization	[1] 20.7	o	o	
6	Call-ID	[1] 20.8	m	m	
8	Content-Length	[1] 20.14	m	m	
9	Cseq	[1] 20.16	m	m	
10	Date	[1] 20.17	o	m	
11	From	[1] 20.20	m	m	
11A	Max-Breadth	[53] 5.8	o	c2	Upon reception of Max-Breadth header in a CANCEL request, no special behaviour is required (header field is ignored).
12	Max-Forwards	[1] 20.22	m	c2	
14	Privacy	[30] 4.2	n/a	n/a	(See note)
15	Reason	[31] 2	o	o	
16	Record-Route	[1] 20.30	n/a	n/a	
17	Reject-Contact	[23] 9.2	c3	c4	
17A	Request-Disposition	[23] 9.1	c3	c4	
18	Route	[1] 20.34	m	c2	
19	Supported	[1] 20.37	m	m	
20	Timestamp	[1] 20.38	o	m	
21	To	[1] 20.39	m	m	
22	User-Agent	[1] 20.41	o	o	
23	Via	[1] 20.42	m	m	
c2: IF there are more than one SIP node within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a. c3: IF Caller Preferences extension is supported THEN o ELSE n/a. c4: IF Caller Preferences extension is supported THEN m ELSE n/a.					
NOTE: Privacy is for further study.					

Table 5.7: Supported headers within the 200 OK response to the CANCEL request

Item	Header	Ref.	Sending	Receiving	Comment
1	Call-ID	[1] 20.8	m	m	
2	Content-Length	[1] 20.14	m	m	
3	Cseq	[1] 20.16	m	m	
4	Date	[1] 20.17	o	o	
5	From	[1] 20.20	m	m	
6	Privacy	[30] 4.2	n/a	n/a	(See note)
7	Record-Route	[1] 20.30	n/a	n/a	
8	Supported	[1] 20.37	m	m	
9	Timestamp	[1] 20.38	m	o	
10	To	[1] 20.39	m	m	
11	User-Agent	[1] 20.41	o	o	
12	Via	[1] 20.42	m	m	
13	Warning	[1] 20.43	o	o	
NOTE: Privacy is for further study.					

Table 5.8: Supported headers within the INFO request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Allow	[1] 20.5	o	m	
5	Allow-Events	[9] 7.2.2	o	m	
6	Authorization	[1] 20.7	o	o	
7	Call-ID	[1] 20.8	m	m	
7A	Call-Info	[1] 20.9	o	o	
8	Contact	[1] 20.10	n/a	n/a	
9	Content-Disposition	[1] 20.11	o	m	
10	Content-Encoding	[1] 20.12	o	m	
11	Content-Language	[1] 20.13	o	m	
12	Content-Length	[1] 20.14	m	m	
13	Content-Type	[1] 20.15	m	m	
14	Cseq	[1] 20.16	m	m	
15	Date	[1] 20.17	o	m	
16	From	[1] 20.20	m	m	
17	Geolocation	[24] 3.2	o	o	
19	Max-Breadth	[53] 5.8	o	c1	
20	Max-Forwards	[1] 20.22	m	c2	
21	MIME-Version	[1] 20.24	o	m	
23	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
24	P-Charging-Vector	[28] 4.6	n/a	n/a	
25	P-Debug-ID	[92]	o	o	
26	Privacy	[30] 4.2	o	c6	
27	Proxy-Authorization	[1] 20.28	c5	n/a	
28	Proxy-Require	[1] 20.29	n/a	n/a	
29	Reason	[31] 2	o	o	
30	Record-Route	[1] 20.30	n/a	n/a	
31	Referred-By	[33] 3	c3	c4	
33	Request-Disposition	[23] 9.1	o	o	
34	Require	[1] 20.32	m	m	
35	Resource-Priority	[40] 3.1	o	o	
36	Route	[1] 20.34	m	c2	
39	Subject	[1] 20.35	o	o	
40	Supported	[1] 20.37	m	m	
41	Timestamp	[1] 20.38	o	m	
42	To	[1] 20.39	m	m	
43	User-Agent	[1] 20.41	o	o	
44	Via	[1] 20.42	m	m	
c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a. c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a. c3: IF Referred-By mechanism is supported THEN m ELSE n/a. c4: IF Referred-By mechanism is supported THEN o ELSE n/a. c5: IF UA-Proxy Authentication is used THEN m ELSE o. c6: IF the NGCN site can be deployed in an environment where it is trustedTHEN m ELSE o.					

Table 5.9: Supported headers within the 200 OK response to the INFO request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Accept-Resource-Priority	[40] 3.2	o	o	
5	Allow	[1] 20.5	o	m	
6	Allow-Events	[9] 7.2.2	o	m	
7	Authentication-Info	[1] 20.6	o	m	
8	Call-ID	[1] 20.8	m	m	

Item	Header	Ref.	Sending	Receiving	Comment
9	Call-Info	[1] 20.9	o	o	
10	Content-Disposition	[1] 20.11	o	m	
11	Content-Encoding	[1] 20.12	o	m	
12	Content-Language	[1] 20.13	o	m	
13	Content-Length	[1] 20.14	m	m	
14	Content-Type	[1] 20.15	m	m	
15	Cseq	[1] 20.16	m	m	
16	Date	[1] 20.17	o	m	
17	From	[1] 20.20	m	m	
19	MIME-Version	[1] 20.24	o	m	
20	Organization	[1] 20.25	o	o	
22	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
23	P-Charging-Vector	[28] 4.6	n/a	n/a	
25	Privacy	[30] 4.2	o	c1	
27	Require	[1] 20.32	o	m	
28	Supported	[1] 20.37	o	m	
29	Server	[1] 20.35	o	o	
30	Timestamp	[1] 20.38	m	o	
31	To	[1] 20.39	m	m	
32	User-Agent	[1] 20.41	o	o	
33	Via	[1] 20.42	m	m	
34	Warning	[1] 20.43	o	o	
c1:	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				

Table 5.10: Supported headers within the INVITE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	c1	m	Indicates the support of the MIME type for the AOC information: "application/vnd.etsaoc+xml".
1A	Accept-Contact	[23] 9.2	c5	c6	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Alert-Info	[1] 20.4	o	o	Contains the URL of the media to be played.
5	Allow	[1] 20.5, [1] 5.1	c1	m	May indicates the support of the INFO method for the AoC service.
6	Allow-Events	[9] 7.2.2	c11	c11	For subscription based approach, the S-CSCF (notifier) indicates at least the support of the reg event package.
8	Authorization	[1] 20.7	o	o	
9	Call-ID	[1] 20.8	m	m	
10	Call-Info	[1] 20.9	o	o	
11	Contact	[1] 20.10	m	m	
12	Content-Disposition	[1] 20.11	o	m	
13	Content-Encoding	[1] 20.12	o	m	
14	Content-Language	[1] 20.13	o	m	
15	Content-Length	[1] 20.14	m	m	
16	Content-Type	[1] 20.15	m	m	
17	Cseq	[1] 20.16	m	m	
18	Date	[1] 20.17	o	m	
19	Expires	[1] 20.19	o	o	
20	From	[1] 20.20	m	m	
20A	Geolocation	[24] 3.2	o	o	In case of an emergency call, the NGCN site will normally identify it as an emergency call and provide a geolocation in conjunction with such calls, using the procedures of [24].
20B	History-Info	[25] 4.1	c13	c13	
21	In-Reply-To	[1] 20.21	o	o	
21A	Join	[26] 7.1	c14	c14	
21B	Max-Breadth	[53] 5.8	o	c9	
22	Max-Forwards	[1] 20.22	m	c10	
23	MIME-Version	[1] 20.24	o	m	
23A	Min-SE	[27] 5	c2	c3	
24	Organization	[1] 20.25	o	o	
24B	P-Asserted-Identity	[29] 9.1	c4	o (see note 1)	This header is part of the SLA between the enterprise and the operator (on the support or not of a trusted connection).
24C	P-Asserted-Service	[34] 4.1	x	x	
24E	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
24F	P-Charging-Vector	[28] 4.6	n/a	n/a	
24G	P-Early-Media	[38] 8	c7	c7	
25C	P-Profile-Key	[35] 5	n/a	n/a	
25D	P-User-Database	[36] 4	n/a	n/a	
25E	P-Visited-Network-ID	[28] 4.3	x	n/a	
26	Priority	[1] 20.26	o	o	
26A	Privacy	[30] 4.2	o	c12	
26B	Private-Network-Indicator	[77]	o	o	The use of this header is subject to agreement between the operator and the enterprise customer. It should be mandatory in case of private network traffic.
27	Proxy-Authorization	[1] 20.28	c17	n/a	
28	Proxy-Require	[1] 20.29	o	n/a	
28A	Reason	[31] 2	o	o	
29	Record-Route	[1] 20.30	o	m	
30	Referred-By	[33] 3	c8	c9	
31	Reject-Contact	[23] 9.2	c5	c6	

Item	Header	Ref.	Sending	Receiving	Comment
31A	Replaces	[39] 6.1	c15	c15	
31B	Reply-To	[1] 20.31	o	o	
31B	Request-Disposition	[23] 9.1	c5	c6	
32	Require	[1] 20.32	m	m	
33	Route	[1] 20.34	m	c10	
33C	Session-Expires	[27] 4	c16	c16	
34	Subject	[1] 20.36	o	o	
35	Supported	[1] 20.37	m	m	This header may contain the option-tag "100Rel" in the receiving side.
36	Timestamp	[1] 20.38	o	m	
37	To	[1] 20.39	m	m	
38	User-Agent	[1] 20.41	o	o	
39	Via	[1] 20.42	m	m	

c1: IF 4.1/1 is supported OR initiating a session THEN m ELSE o - - Advice of Charge (INFO method), initiating a session.
c2: IF SIP session timer extension is supported THEN o else n/a.
c3: IF SIP session timer extension is supported THEN m else n/a.
c4: IF the NGCN site can be deployed in an environment where it is trusted THEN "o" ELSE "n/a".
c5: IF Caller Preferences extension is supported THEN o else n/a.
c6: IF Caller Preferences extension is supported THEN m else n/ac9: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c7: IF P-Early-Media private header extension is supported THEN m ELSE n/a.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c10: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m else n/a.
c11: IF there is a notifier beyond the NGCN attachment point THEN m ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.
c13: IF History-Info extension is supported THEN m else n/a.
c14: IF Join extension is supported THEN m else n/a.
c15: IF SIP "Replaces" header extension is supported THEN m ELSE n/a.
c16: IF SIP session timer extension is supported THEN m ELSE n/a.
c17: IF UA-Proxy Authentication is used THEN "m" ELSE "no".

NOTE 1: The use of this header is subject to Spec T.

Table 5.11: Supported headers within the 200 OK response to the INVITE

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Allow	[1] 20.5	m	m	
5	Allow-Events	[9] 7.2.2	o	m	
6	Authentication-Info	[1] 20.6	o	m	
7	Call-ID	[1] 20.8	m	m	
8	Call-Info	[1] 20.9	o	o	
9	Contact	[1] 20.10	m	m	
10	Content-Disposition	[1] 20.11	o	m	
11	Content-Encoding	[1] 20.12	o	m	
12	Content-Language	[1] 20.13	o	m	
13	Content-Length	[1] 20.14	m	m	
14	Content-Type	[1] 20.15	m	m	
15	Cseq	[1] 20.16	m	m	
16	Date	[1] 20.17	o	o	
17	Expires	[1] 20.19	o	o	
18	From	[1] 20.20	m	m	
20	History-Info	[25] 4.1	c13	c13	
21	MIME-Version	[1] 20.24	o	m	
22	Organization	[1] 20.25	o	o	
23	P-Answer-State	[66]	n/a	n/a	
24	P-Asserted-Identity	[29] 9.1	o	o	
25	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
26	P-Charging-Vector	[28] 4.6	n/a	n/a	
26A	P-Preferred-Identity	[29] 9.2	x	n/a	
29	Privacy	[30] 4.2	o	c2	
30	Record-Route	[1] 20.30	m	m	
31	Reply-To	[1] 20.31	o	o	
32	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in 200 OK response to INVITE.
33	Server	[1] 20.35	o	o	
34	Session-Expires	[27] 4	c1	c1	
35	Supported	[1] 20.37	m	m	
36	Timestamp	[1] 20.38	m	o	
37	To	[1] 20.39	m	m	
38	User-Agent	[1] 20.41	o	o	
39	Via	[1] 20.42	m	m	
40	Warning	[1] 20.43	o	o	
c1: IF SIP session timer extension is supported THEN m ELSE n/a. c2: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o. c13: IF History-Info extension is supported THEN m else n/a.					

NOTE: Table 5.11 gives hint on the headers' status for all the remaining possible responses to the INVITE request.

Table 5.12: Supported headers within the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept-Contact	[23] 9.2	c5	c6	
1A	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authorization	[1] 20.7	o	o	
4	Call-ID	[1] 20.8	m	m	
5	Call-Info	[1] 20.9	o	o	
6	Content-Disposition	[1] 20.11	o	m	
7	Content-Encoding	[1] 20.12	o	m	
8	Content-Language	[1] 20.13	o	m	
9	Content-Length	[1] 20.14	o	m	
10	Content-Type	[1] 20.15	m	m	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	Expires	[1] 20.19	o	o	
14	From	[1] 20.20	m	m	
14A	Geolocation	[24] 3.2	o	o	
14B	History-Info	[25] 4.1	c13	c13	
15	In-Reply-To	[1] 20.21	o	o	
15A	Max-Breadth	[53] 5.8	o	c1	
16	Max-Forwards	[1] 20.22	m	c2	
17	MIME-Version	[1] 20.24	o	m	
18	Organization	[1] 20.25	o	o	
18B	P-Asserted-Identity	[29] 9.1	c3	o	When sending this header is part of the SLA between the enterprise and the operator (on the support or not of a trusted relationship).
18E	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
18F	P-Charging-Vector	[28] 4.6	n/a	n/a	
18I	P-Profile-Key	[35] 5	n/a	n/a	
18J	P-User-Database	[36] 4	n/a	n/a	
18K	P-Visited-Network-ID	[28] 4.3	x	n/a	
19	Priority	[1] 20.26	o	o	
19A	Privacy	[30] 4.2	o	c12	
20	Proxy-Authorization	[1] 20.28	c7	n/a	
21	Proxy-Require	[1] 20.29	n/a	n/a	
21A	Reason	[31] 2	o	o	
22	Record-Route	[1] 20.30	n/a	n/a	
22A	Referred-By	[33] 3	c8	c9	
23	Reject-Contact	[23] 9.2	c5	c6	
23A	Reply-To	[1] 20.31	o	o	
23B	Request-Disposition	[23] 9.1	c5	c6	
24	Require	[1] 20.32	o	m	
25	Route	[1] 20.34	m	c4	
26	Subject	[1] 20.35	o	o	
27	Supported	[1] 20.37	m	m	
28	Timestamp	[1] 20.38	o	m	
29	To	[1] 20.39	m	m	
30	User-Agent	[1] 20.41	o	o	
31	Via	[1] 20.42	m	m	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN "o" ELSE "n/a".
c4: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c5: IF Caller Preferences extension is supported THEN o else n/a.
c6: IF Caller Preferences extension is supported THEN m else n/a.
c7: IF UA-Proxy Authentication is used THEN m ELSE o.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.
c13: IF History-Info extension is supported THEN m ELSE n/a.

Table 5.13: Supported headers within the 2xx response to the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authentication-Info	[1] 20.6	o	m	
4	Call-ID	[1] 20.8	m	m	
5	Call-Info	[1] 20.9	o	o	
6	Content-Disposition	[1] 20.11	x	n/a	
7	Content-Encoding	[1] 20.12	x	n/a	
8	Content-Language	[1] 20.13	x	n/a	
9	Content-Length	[1] 20.14	x	n/a	
10	Content-Type	[1] 20.15	x	n/a	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	Expires	[1] 20.19	o	o	
14	From	[1] 20.20	m	m	
16	History-Info	[25] 4.1	c13	c13	
17	MIME-Version	[1] 20.24	x	n/a	
18	Organization	[1] 20.25	o	o	
19	P-Asserted-Identity	[29] 9.1	o	o	
20	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
21	P-Charging-Vector	[28] 4.6	n/a	n/a	
22	P-Preferred-Identity	[29] 9.2	x	n/a	
23	Privacy	[30] 4.2	o	c1	
24	Reply-To	[1] 20.31	o	o	
25	Require	[1] 20.32	o	m	
26	Server	[1] 20.35	o	o	
27	Supported	[1] 20.37	o	m	
28	Timestamp	[1] 20.38	m	o	
29	To	[1] 20.39	m	m	
31	User-Agent	[1] 20.41	o	o	
32	Via	[1] 20.42	m	m	
33	Warning	[1] 20.43	o	o	
c1: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o. c13: IF History-Info extension is supported THEN m else n/a.					

Table 5.14: Supported headers within the NOTIFY request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
1A	Accept-Contact	[23] 9.2	c5	c6	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
3A	Allow	[1] 20.5	o	m	
4	Allow-Events	[9] 7.2.2	o	m	
5	Authorization	[1] 20.7	o	o	
6	Call-ID	[1] 20.8	m	m	
6A	Call-Info	[1] 20.9	o		
6B	Contact	[1] 20.10	m	m	
7	Content-Disposition	[1] 20.11	o	m	
8	Content-Encoding	[1] 20.12	o	m	
9	Content-Language	[1] 20.13	o	m	
10	Content-Length	[1] 20.14	m	m	
11	Content-Type	[1] 20.15	m	m	
12	Cseq	[1] 20.16	m	m	
13	Date	[1] 20.17	o	m	
14	Event	[9] 7.2.1	m	m	
15	From	[1] 20.20	m	m	
15A	Geolocation	[24] 3.2	o	o	
15B	History-Info	[25] 4.1	c13	c13	
15C	Max-Breadth	[53] 5.8	o	c1	
16	Max-Forwards	[1] 20.22	m	c2	
17	MIME-Version	[1] 20.24	o	m	
17B	P-Asserted-Identity	[29] 9.1	c3	o	When sending this header is part of the SLA between the enterprise and the operator (on the support or not of a trusted relationship).
17C	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
17D	P-Charging-Vector	[28] 4.6	n/a	n/a	
17E	P-Preferred-Identity	[29] 9.2	x	n/a	
17F	Privacy	[30] 4.2	o	c12	
18	Proxy-Authorization	[1] 20.28	c7	n/a	
19	Proxy-Require	[1] 20.29	n/a	n/a	
19A	Reason	[31] 2	o	o	
20	Record-Route	[1] 20.30	o	m	
20A	Referred-By	[33] 3	c8	c9	
20B	Reject-Contact	[23] 9.2	c5	c6	
20C	Request-Disposition	[23] 9.1	c5	c6	
21	Require	[1] 20.32	o	m	
22	Route	[1] 20.34	m		
23	Subscription-State	[9] 8.2.3	m	m	
24	Supported	[1] 20.37	o	m	
25	Timestamp	[1] 20.38	o	m	
26	To	[1] 20.39	m	m	
27	User-Agent	[1] 20.41	o	o	
28	Via	[1] 20.42	m	m	
29	Warning	[1] 20.43	o	o	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m else n/a.
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN "o" ELSE "n/a".
c5: IF Caller Preferences extension is supported THEN o else n/a.
c6: IF Caller Preferences extension is supported THEN m else n/a.
c7: IF UA-Proxy Authentication is used THEN m ELSE o.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.
c13: IF History-Info extension is supported THEN m else n/a.

Table 5.15: Supported headers within the 200 OK response to NOTIFY

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authentication-Info	[1] 20.6	o	m	
4	Call-ID	[1] 20.8	m	m	
5	Contact	[1] 20.10	o	m	
6	Content-Disposition	[1] 20.11	o	m	
7	Content-Encoding	[1] 20.12	o	m	
8	Content-Language	[1] 20.13	o	m	
9	Content-Length	[1] 20.14	m	m	
10	Content-Type	[1] 20.15	m	m	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	From	[1] 20.20	m	m	
15	MIME-Version	[1] 20.24	o	m	
16	P-Asserted-Identity	[29] 9.1	o	o	
17	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
18	P-Charging-Vector	[28] 4.6	n/a	n/a	
19	P-Preferred-Identity	[29] 9.2	x	n/a	
20	Privacy	[30] 4.2	o	c1	
21	Record-Route	[1] 20.30	o	o	
22	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in 200 OK response to NOTIFY.
23	Server	[1] 20.35	o	o	
24	Supported	[1] 20.37	m	m	
25	Timestamp	[1] 20.38	m	o	
26	To	[1] 20.39	m	m	
27	User-Agent	[1] 20.41	o	o	
28	Via	[1] 20.42	m	m	
29	Warning	[1] 20.43	o	o	
c1:	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				

Table 5.16: Supported headers within the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	m	m	
1A	Accept-Contact	[23] 9.2	c4	c5	
2	Accept-Encoding	[1] 20.2	m	m	
3	Accept-Language	[1] 20.3	m	m	
3A	Allow	[1] 20.5	o	m	
4	Allow-Events	[9] 7.2.2	o	m	
5	Authorization	[1] 20.7	o	o	
6	Call-ID	[1] 20.8	m	m	
7	Call-Info	[1] 20.9	o	o	
8	Contact	[1] 20.10	o	o	
9	Content-Disposition	[1] 20.11	o	m	
10	Content-Encoding	[1] 20.12	o	m	
11	Content-Language	[1] 20.13	o	m	
12	Content-Length	[1] 20.14	m	m	
13	Content-Type	[1] 20.15	m	m	
14	Cseq	[1] 20.16	m	m	
15	Date	[1] 20.17	o	m	
16	From	[1] 20.20	m	m	
16A	Geolocation	[24] 3.2	o	o	
16B	History-Info	[25] 4.1	c13	c13	
16C	Max-Breadth	[53] 5.8	o	c1	
17	Max-Forwards	[1] 20.22	m	c2	
18	MIME-Version	[1] 20.24	o	m	
19	Organization	[1] 20.25	o	o	
19A	P-Access-Network-Info	[28] 4.4	c3	n/a	
19B	P-Asserted-Identity	[29] 9.1	c6	o (see note)	This header is part of the SLA between the enterprise and the operator (on the support or not of a trusted connection).
19E	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
19F	P-Charging-Vector	[28] 4.6	n/a	n/a	
19G	P-Preferred-Identity	[29] 9.2	o	n/a	
19I	P-Profile-Key	[35] 5	n/a	n/a	
19J	P-User-Database	[36] 4	n/a	n/a	
19K	P-Visited-Network-ID	[28] 4.3	x	n/a	
19L	Privacy	[30] 4.2	o	c12	
19M	Private-Network-Indicator	[77]	o	o	The use of this header is subject to agreement between the operator and the enterprise customer. It should be mandatory in case of private network traffic.
20	Proxy-Authorization	[1] 20.28	c7	n/a	
21	Proxy-Require	[1] 20.29	o	n/a	
21A	Reason	[31] 2	o	o	
22	Record-Route	[1] 20.30	n/a	n/a	
22A	Referred-By	[33] 3	c8	c9	
22B	Reject-Contact	[23] 9.2	c4	c5	
22C	Request-Disposition	[23] 9.1	c4	c5	
23	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in OPTIONS request.
24	Route	[1] 20.34	m	n/a	
26	Timestamp	[1] 20.38	o	m	
27	To	[1] 20.39	m	m	
28	User-Agent	[1] 20.41	o	o	
29	Via	[1] 20.42	m	m	

Item	Header	Ref.	Sending	Receiving	Comment
c1:	IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.				
c2:	IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.				
c3:	IF the access type is GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN THEN m ELSE o.				
c4:	IF Caller Preferences extension is supported THEN o else n/a.				
c5:	IF Caller Preferences extension is supported THEN m else n/a.				
c6:	IF the NGCN site can be deployed in an environment where it is trusted THEN o ELSE n/a.				
c7:	IF UA-Proxy Authentication is used THEN m ELSE o.				
c8:	IF Referred-By mechanism is supported THEN m ELSE n/a.				
c9:	IF Referred-By mechanism is supported THEN o ELSE n/a.				
c12	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				
c13:	IF History-Info extension is supported THEN m else n/a.				
NOTE:	The use of this header is subject to Spec T.				

Table 5.17: Supported headers within the 200 OK response to the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	m	m	
2	Accept-Encoding	[1] 20.2	m	m	
3	Accept-Language	[1] 20.3	m	m	
4	Allow	[1] 20.5	m	m	
5	Allow-Events	[9] 7.2.2	o	m	
6	Authentication-Info	[1] 20.6	o	m	
7	Call-ID	[1] 20.8	m	m	
8	Call-Info	[1] 20.9	o	o	
9	Contact	[1] 20.10	n/a	n/a	
10	Content-Disposition	[1] 20.11	o	m	
11	Content-Encoding	[1] 20.12	o	m	
12	Content-Language	[1] 20.13	o	m	
13	Content-Length	[1] 20.14	m	m	
14	Content-Type	[1] 20.15	m	m	
15	Cseq	[1] 20.16	m	m	
16	Date	[1] 20.17	o	m	
17	From	[1] 20.20	m	m	
19	History-Info	[25] 4.1	c13	c13	
20	MIME-Version	[1] 20.24	o	m	
21	Organization	[1] 20.25	o	o	
23	P-Asserted-Identity	[29] 9.1	o	o	
24	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
25	P-Charging-Vector	[28] 4.6	n/a	n/a	
26	P-Preferred-Identity	[29] 9.2	o	n/a	
27	Privacy	[30] 4.2	o	c1	
28	Require	[1] 20.32	m	m	
29	Server	[1] 20.35	o	o	
30	Supported	[1] 20.37	m	m	
31	Timestamp	[1] 20.38	m	o	
32	To	[1] 20.39	m	m	
33	User-Agent	[1] 20.41	o	o	
34	Via	[1] 20.42	m	m	
35	Warning	[1] 20.43	o	o	
c1:	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				
c13:	IF History-Info extension is supported THEN m else n/a.				

Table 5.18: Supported headers within the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
1A	Accept-Contact	[23] 9.2	c5	c6	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
3A	Allow	[1] 20.5	o	m	
4	Allow-Events	[9] 7.2.2	o	m	
5	Authorization	[1] 20.7	c3	c3	
6	Call-ID	[1] 20.8	m	m	
7	Content-Disposition	[1] 20.11	o	m	
8	Content-Encoding	[1] 20.12	o	m	
9	Content-Language	[1] 20.13	o	m	
10	Content-Length	[1] 20.14	m	m	
11	Content-Type	[1] 20.15	m	m	
12	Cseq	[1] 20.16	m	m	
13	Date	[1] 20.17	o	m	
14	From	[1] 20.20	m	m	
14A	Max-Breadth	[53] 5.8	o	c1	
15	Max-Forwards	[1] 20.22	m	c2	
16	MIME-Version	[1] 20.24	o	m	
16B	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
16C	P-Charging-Vector	[28] 4.6	n/a	n/a	
16CA	P-Early-Media	[38] 8	c7	c7	
16D	Privacy	[30] 4.2	n/a	n/a	
17	Proxy-Authorization	[1] 20.28	c4	n/a	
18	Proxy-Require	[1] 20.29	o	m	Values equal to those in INVITE request.
19	Rack	[6] 7.2	m	m	
19A	Reason	[31] 2	o	o	
20	Record-Route	[1] 20.30	n/a	n/a	
20A	Referred-By	[33] 3	c8	c9	
20B	Reject-Contact	[23] 9.2	c5	c6	
20C	Request-Disposition	[23] 9.1	c5	c6	
21	Require	[1] 20.32	m	m	Values equal to those in INVITE request.
22	Route	[1] 20.34	m	c2	
23	Supported	[1] 20.37	m	m	
24	Timestamp	[1] 20.38	o	m	
25	To	[1] 20.39	m	m	
26	User-Agent	[1] 20.41	o	o	
27	Via	[1] 20.42	m	m	
c1:	IF forking is possible within the NGCN THEN m ELSE n/a.				
c2:	IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.				
c3:	IF UA-UA Authentication is used THEN m ELSE o.				
c4:	IF UA-Proxy Authentication is used THEN m ELSE o.				
c5:	IF Caller Preferences extension is supported THEN o ELSE n/a.				
c6:	IF Caller Preferences extension is supported THEN m ELSE n/a.				
c7:	IF P-Early-Media private header extension is supported THEN m ELSE n/a.				
c8:	IF Referred-By mechanism is supported THEN m ELSE n/a.				
c9:	IF Referred-By mechanism is supported THEN o ELSE n/a.				

Table 5.19: Supported headers within the 200 OK response to the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow-Events	[9] 7.2.2	o	m	
2	Authentication-Info	[1] 20.6	o	o	
3	Call-ID	[1] 20.8	m	m	
4	Content-Disposition	[1] 20.11	o	m	
5	Content-Encoding	[1] 20.12	o	m	
6	Content-Language	[1] 20.13	o	m	
7	Content-Length	[1] 20.14	m	m	
8	Content-Type	[1] 20.15	m	m	
9	Cseq	[1] 20.16	m	m	
10	Date	[1] 20.17	o	m	
11	From	[1] 20.20	m	m	
12	MIME-Version	[1] 20.24	o	m	
14	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
15	P-Charging-Vector	[28] 4.6	n/a	n/a	
16	P-Early-Media	[38] 8	c1	c1	
17	Privacy	[30] 4.2	n/a	n/a	
18	Require	[1] 20.32	m	m	
19	Server	[1] 20.35	o	o	
20	Supported	[1] 20.37	m	m	
21	Timestamp	[1] 20.38	m	o	
22	To	[1] 20.39	m	m	
23	User-Agent	[1] 20.41	o	o	
24	Via	[1] 20.42	m	m	
25	Warning	[1] 20.43	o	o	

c1: IF P-Early-Media private header extension is supported THEN m ELSE n/a.

Table 5.20: Supported headers within the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept-Contact	[23] 9.2	c4	c5	
2	Allow	[1] 20.5	o	m	
3	Allow-Events	[1] 7.2.2	o	m	
4	Authorization	[1] 20.7	o	o	
5	Call-ID	[1] 20.8	m	m	
6	Call-Info	[1] 20.9	o	o	
7	Content-Disposition	[1] 20.11	o	m	
8	Content-Encoding	[1] 20.12	o	m	
9	Content-Language	[1] 20.13	o	m	
10	Content-Length	[1] 20.14	m	m	
11	Content-Type	[1] 20.15	m	m	
12	Cseq	[1] 20.16	m	m	
13	Date	[1] 20.17	o	m	
14	Event	[11] 4, 6	m	m	
15	Expires	[1] 20.19, [11] 4, 5, 6	o	m	
16	From	[1] 20.20	m	m	
16A	History-Info	[25] 4.1	c13	c13	
17	In-Reply-To	[1] 20.21	o	o	
17A	Max-Breadth	[53] 5.8	o	c1	
18	Max-Forwards	[1] 20.22	m	c2	
19	MIME-Version	[1] 20.24	o	m	
20	Organization	[1] 20.25	o	o	
22	P-Asserted-Identity	[29] 9.1	c3	o	
24	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
25	P-Charging-Vector	[28] 4.6	n/a	n/a	
26B	P-Profile-Key	[35] 5	n/a	n/a	
26C	P-User-Database	[36] 4	n/a	n/a	
27	P-Visited-Network-ID	[28] 4.3	x	n/a	
28	Priority	[1] 20.26	o	o	
29	Privacy	[30] 4.2	o	c12	
30	Proxy-Authorization	[1] 20.28	c7	n/a	
31	Proxy-Require	[1] 20.29	n/a	n/a	
32	Reason	[31] 2	o	o	
33	Reject-Contact	[23] 9.2	c4	c5	
33A	Referred-By	[33] 3	c8	c9	
34	Request-Disposition	[23] 9.1	c4	c5	
35	Reply-To	[1] 20.31	o	o	
36	Require	[1] 20.32	o	m	
37	Route	[1] 20.34	m	n/a	
40	SIP-If-Match	[11] 11.3.2	o	m	
41	Subject	[1] 20.36	o	o	
42	Supported	[1] 20.37, [1] 7.1	o	m	
43	Timestamp	[1] 20.38	o	m	
44	To	[1] 20.39	m	m	
45	User-Agent	[1] 20.41	o	o	
46	Via	[1] 20.42	m	m	

c1: IF forking is possible within the NGCN THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN o ELSE n/a.
c4: IF Caller Preferences extension is supported THEN o else n/a.
c5: IF Caller Preferences extension is supported THEN m else n/a.
c7: IF UA-Proxy Authentication is used THEN m ELSE o.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.
c13: IF History-Info extension is supported THEN m else n/a.

Table 5.21: Supported headers within the 2xx response to the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Authentication-Info	[1] 20.6	o	m	
3	Call-ID	[1] 20.8	m	m	
4	Call-Info	[1] 24.9	o	m	
5	Content-Disposition	[1] 20.11	o	m	
6	Content-Encoding	[1] 20.12	o	m	
7	Content-Language	[1] 20.13	o	m	
8	Content-Length	[1] 20.14	m	m	
9	Content-Type	[1] 20.15	m	m	
10	Cseq	[1] 20.16	m	m	
11	Date	[1] 20.17	o	m	
12	Expires	[1] 20.19, [11] 4, 5, 6	m	m	
13	From	[1] 20.20	m	m	
14	History-Info	[25] 4.1	o	o	
15	MIME-Version	[1] 20.24	o	m	
16	Organization	[1] 20.25	o	o	
18	P-Asserted-Identity	[29] 9.1	o	o	
19	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
20	P-Charging-Vector	[28] 4.6	n/a	n/a	
21	P-Preferred-Identity	[29] 9.2	x	n/a	
22	Privacy	[30] 4.2	o	c1	
23	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in 2xx response to PUBLISH.
24	Server	[1] 20.35	o	o	
25	SIP-Etag	[11] 11.3.1	m	m	
26	Supported	[1] 20.37	m	m	
27	Timestamp	[1] 20.38	m	o	
28	To	[1] 20.39	m	m	
29	User-Agent	[1] 20.41	o	o	
30	Via	[1] 20.42	m	m	
31	Warning	[1] 20.43	o	o	
c1:	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				

Table 5.22: Supported headers within the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
0A	Accept	[1] 20.1	o	m	
0B	Accept-Contact	[23] 9.2	c5	c6	
0C	Accept-Encoding	[1] 20.2	o	m	
1	Accept-Language	[1] 20.3	o	m	
1A	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authorization	[1] 20.7	o	o	
4	Call-ID	[1] 20.8	m	m	
5	Contact	[1] 20.10	m	m	
5A	Content-Disposition	[1] 20.11	o	m	
5B	Content-Encoding	[1] 20.12	o	m	
5C	Content-Language	[1] 20.13	o	m	
6	Content-Length	[1] 20.14	m	m	
7	Content-Type	[1] 20.15	m	m	
8	Cseq	[1] 20.16	m	m	
9	Date	[1] 20.17	o	m	
10	Expires	[1] 20.19	o	o	
11	From	[1] 20.20	m	m	
11A	Geolocation	[24] 3.2	o	o	
11B	History-Info	[25] 4.1	c13	c13	
11C	Max-Breadth	[53] 5.8	o	c1	
12	Max-Forwards	[1] 20.22	m	c2	
13	MIME-Version	[1] 20.24	o	m	
14	Organization	[1] 20.25	o	o	
14B	P-Asserted-Identity	[29] 9.1	c3	o	When sending this header is part of the SLA between the enterprise and the operator (on the support or not of a trusted relationship).
14E	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
14F	P-Charging-Vector	[28] 4.6	n/a	n/a	
14I	P-Profile-Key	[35] 5	n/a	n/a	
14J	P-User-Database	[36] 4	n/a	n/a	
14K	P-Visited-Network-ID	[28] 4.3	x	n/a	
14L	Privacy	[30] 4.2	o	c12	
15	Proxy-Authorization	[1] 20.28	c7	n/a	
16	Proxy-Require	[1] 20.29	n/a	n/a	
16A	Reason	[31] 2	o	o	
17	Record-Route	[1] 20.30	o	m	
18	Refer-To	[35] 3	m	m	
18A	Referred-By	[33] 3	c8	c8	
18B	Reject-Contact	[23] 9.2	c5	c6	
18C	Request-Disposition	[23] 9.1	c5	c6	
19	Require	[1] 20.32	o	m	
20	Route	[1] 20.34	m	c4	
21	Supported	[1] 20.37, [1] 7.1	o	m	
22	Timestamp	[1] 20.38	o	m	
23	To	[1] 20.39	m	m	
24	User-Agent	[1] 20.41	o	o	
25	Via	[1] 20.42	m	m	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m else n/a.
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN "o" ELSE "n/a".
c4: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m else n/a.
c5: IF Caller Preferences extension is supported THEN o else n/a.
c6: IF Caller Preferences extension is supported THEN m else n/a.
c7: IF UA-Proxy Authentication is used THEN m ELSE oc8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.
c13: IF History-Info extension is supported THEN m else n/a.

Table 5.23: Supported headers within the 2xx response to the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authentication-Info	[1] 20.6	o	m	
4	Call-ID	[1] 20.8	m	m	
5	Contact	[1] 20.10	m	m	
6	Content-Disposition	[1] 20.11	o	m	
7	Content-Encoding	[1] 20.12	o	m	
8	Content-Language	[1] 20.13	o	m	
9	Content-Length	[1] 20.14	m	m	
10	Content-Type	[1] 20.15	m	m	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	From	[1] 20.20	m	m	
15	History-Info	[25] 4.1	c13	c13	
16	MIME-Version	[1] 20.24	o	m	
17	Organization	[1] 20.25	o	o	
18	P-Asserted-Identity	[29] 9.1	o	o	
19	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
20	P-Charging-Vector	[28] 4.6	n/a	n/a	
21	P-Preferred-Identity	[29] 9.2	x	n/a	
22	Privacy	[30] 4.2	o	c1	
23	Record-Route	[1] 20.30	m	m	
24	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in 2xx response to REFER.
25	Server	[1] 20.35	o	o	
26	Supported	[1] 20.37	m	m	
27	Timestamp	[1] 20.38	m	o	
28	To	[1] 20.39	m	m	
29	User-Agent	[1] 20.41	o	o	
30	Via	[1] 20.42	m	m	
31	Warning	[1] 20.43	o	o	
c1: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o. c13: IF History-Info extension is supported THEN m else n/a.					
NOTE: The use of this header is subject to Spec T.					

Table 5.24: Supported headers within the SUBSCRIBE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
1A	Accept-Contact	[23] 9.2	c5	c6	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
3A	Allow	[1] 20.5	o	m	
4	Allow-Events	[9] 7.2.2	o	m	
5	Authorization	[1] 20.7	o	o	
6	Call-ID	[1] 20.8	m	m	
6A	Contact	[1] 20.10	m	m	
7	Content-Disposition	[1] 20.11	o	m	
8	Content-Encoding	[1] 20.12	o	m	
9	Content-Language	[1] 20.13	o	m	
10	Content-Length	[1] 20.14	m	m	
11	Content-Type	[1] 20.15	m	m	
12	Cseq	[1] 20.16	m	m	
13	Date	[1] 20.17	o	m	
14	Event	[9] 7.2.1	m	m	
15	Expires	[1] 20.19	o	m	
16	From	[1] 20.20	m	m	
16A	Geolocation	[24] 3.2	o	o	
16B	History-Info	[25] 4.1	c13	c13	
16C	Max-Breadth	[53] 5.8	o	c1	
17	Max-Forwards	[1] 20.22	m	c2	
18	MIME-Version	[1] 20.24	o	m	
18A	Organization	[1] 20.25	o	o	
18C	P-Asserted-Identity	[29] 9.1	c3	o	When sending this header is part of the SLA between the enterprise and the operator (on the support or not of a trusted relationship).
18F	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
18G	P-Charging-Vector	[28] 4.6	n/a	n/a	
18J	P-Profile-Key	[35] 5	n/a	n/a	
18K	P-User-Database	[36] 4	n/a	n/a	
18L	P-Visited-Network-ID	[28] 4.3	x	n/a	
18M	Privacy	[30] 4.2	o	c12	
19	Proxy-Authorization	[1] 20.28	c7	n/a	
20	Proxy-Require	[1] 20.29	n/a	n/a	
20A	Reason	[31] 2	o	o	
21	Record-Route	[1] 20.30	o	m	
21A	Referred-By	[33] 3	c8	c9	
21B	Reject-Contact	[23] 9.2	c5	c6	
21C	Request-Disposition	[23] 9.1	c5	c6	
22	Require	[1] 20.32	o	m	
23	Route	[1] 20.34	m	c4	
24	Supported	[1] 20.37	o	m	
25	Timestamp	[1] 20.38	o	m	
26	To	[1] 20.39	m	m	
27	User-Agent	[1] 20.41	o	o	
28	Via	[1] 20.42	m	m	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c3: IF the NGCN site can be deployed in an environment where it is trusted THEN o ELSE n/a.
c4: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c5: IF Caller Preferences extension is supported THEN o ELSE n/a.
c6: IF Caller Preferences extension is supported THEN m ELSE n/a.
c7: IF UA-Proxy Authentication is used THEN m ELSE o.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c12: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.

Item	Header	Ref.	Sending	Receiving	Comment
c13:	IF History-Info extension is supported THEN m ELSE n/a.				

Table 5.25: Supported headers within the 2xx response to SUBSCRIBE

Item	Header	Ref.	Sending	Receiving	Comment
1	Allow	[1] 20.5	o	m	
2	Allow-Events	[9] 7.2.2	o	m	
3	Authentication-Info	[1] 20.6	o	m	
4	Call-ID	[1] 20.8	m	m	
5	Contact	[1] 20.10	m	m	
6	Content-Disposition	[1] 20.11	o	m	
7	Content-Encoding	[1] 20.12	o	m	
8	Content-Language	[1] 20.13	o	m	
9	Content-Length	[1] 20.14	m	m	
10	Content-Type	[1] 20.15	m	m	
11	Cseq	[1] 20.16	m	m	
12	Date	[1] 20.17	o	m	
13	Expires	[1] 20.19	m	m	
14	From	[1] 20.20	m	m	
16	History-Info	[25] 4.1	c13	c13	
17	MIME-Version	[1] 20.24	o	m	
18	Organization	[1] 20.25	o	o	
20	P-Asserted-Identity	[29] 9.1	o	o	
21	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
22	P-Charging-Vector	[28] 4.6	n/a	n/a	
23	P-Preferred-Identity	[29] 9.2	x	n/a	
24	Privacy	[30] 4.2	o	c1	
25	Record-Route	[1] 20.30	m	m	
26	Require	[1] 20.32	m	m	Although TS 24.229 [12] indicates that the ability to send this header field is mandatory, there is no business trunking requirement to send this header field in 2xx response to SUBSCRIBE.
27	Server	[1] 20.35	o	o	
28	Supported	[1] 20.37	m	m	
29	Timestamp	[1] 20.38	m	o	
30	To	[1] 20.39	m	m	
31	User-Agent	[1] 20.41	o	o	
32	Via	[1] 20.42	m	m	
33	Warning	[1] 20.43	o	o	
c1:	IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.				
c13:	IF History-Info extension is supported THEN m else n/a.				

Table 5.26: Supported headers within the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
1A	Accept-Contact	[23] 9.2	c3	c4	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Allow	[1] 20.5	o	m	
5	Allow-Events	[9] 7.2.2	o	m	
6	Authorization	[1] 20.7	o	o	
7	Call-ID	[1] 20.8	m	m	
8	Call-Info	[1] 20.9	o	o	
9	Contact	[1] 20.10	m	m	
10	Content-Disposition	[1] 20.11	o	m	
11	Content-Encoding	[1] 20.12	o	m	
12	Content-Language	[1] 20.13	o	m	
13	Content-Length	[1] 20.14	m	m	
14	Content-Type	[1] 20.15	m	m	
15	Cseq	[1] 20.16	m	m	
16	Date	[1] 20.17	o	m	
17	From	[1] 20.20	m	m	
17A	Geolocation	[24] 3.2	o	o	
17B	Max-Breadth	[53] 5.8	o	c1	
18	Max-Forwards	[1] 20.22	m	c2	
19	MIME-Version	[1] 20.24	o	m	
19A	Min-SE	[27] 5	c5	c5	
20	Organization	[1] 20.25	o	o	
20B	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
20C	P-Charging-Vector	[28] 4.6	n/a	n/a	
20D	P-Early-Media	[38] 8	c7	c7	
20E	Privacy	[30] 4.2	n/a	n/a	
21	Proxy-Authorization	[1] 20.28	c6	n/a	
22	Proxy-Require	[1] 20.29	n/a	n/a	
22A	Reason	[31] 2	o	o	
23	Record-Route	[1] 20.30	n/a	n/a	
23A	Referred-By	[33] 3	c8	c9	
23B	Reject-Contact	[23] 9.2	c3	c4	
23C	Request-Disposition	[23] 9.1	c3	c4	
24	Require	[1] 20.32	o	m	
25	Route	[1] 20.34	m	c2	
25C	Session-Expires	[27] 4	c10	c10	
26	Supported	[1] 20.37	o	m	
27	Timestamp	[1] 20.38	o	m	
28	To	[1] 20.39	m	m	
29	User-Agent	[1] 20.41	o	o	
30	Via	[1] 20.42	m	m	

c1: IF forking is possible beyond the NGCN attachment point THEN m ELSE n/a.
c2: IF there are more than one SIP entity within the NGCN (including the attachment point to the NGN) THEN m ELSE n/a.
c3: IF Caller Preferences extension is supported THEN o ELSE n/a.
c4: IF Caller Preferences extension is supported THEN m ELSE n/a.
c5: IF SIP session timer extension is supported THEN m ELSE n/a.
c6: IF UA-Proxy Authentication is used THEN o ELSE n/a.
c7: IF P-Early-Media private header extension is supported THEN m ELSE n/a.
c8: IF Referred-By mechanism is supported THEN m ELSE n/a.
c9: IF Referred-By mechanism is supported THEN o ELSE n/a.
c10: IF SIP session timer extension is supported THEN m ELSE n/a.

Table 5.27: Supported headers within the 200 OK response to the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	m	
2	Accept-Encoding	[1] 20.2	o	m	
3	Accept-Language	[1] 20.3	o	m	
4	Allow	[1] 20.5	o	m	
5	Allow-Events	[9] 7.2.2	o	m	
6	Authentication-Info	[1] 20.6	o	o	
7	Call-ID	[1] 20.8	m	m	
8	Call-Info	[1] 20.9	o	o	
9	Contact	[1] 20.10	m	m	
10	Content-Disposition	[1] 20.11	o	m	
11	Content-Encoding	[1] 20.12	o	m	
12	Content-Language	[1] 20.13	o	m	
13	Content-Length	[1] 20.14	m	m	
14	Content-Type	[1] 20.15	m	m	
15	Cseq	[1] 20.16	m	m	
16	Date	[1] 20.17	o	m	
17	From	[1] 20.20	m	m	
19	MIME-Version	[1] 20.24	o	m	
20	Organization	[1] 20.25	o	o	
22	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
23	P-Charging-Vector	[28] 4.6	n/a	n/a	
24	P-Early-Media	[38] 8	c1	c1	
25	Privacy	[30] 4.2	o	c3	
26	Require	[1] 20.31	m	m	
27	Server	[1] 20.35	o	o	
28	Session-Expires	[27]	c2	c2	
29	Supported	[1] 20.37	m	m	
30	Timestamp	[1] 20.38	o	o	
31	To	[1] 20.39	m	m	
32	User-Agent	[1] 20.41	o	o	
33	Via	[1] 20.42	m	m	
34	Warning	[1] 20.43	o	o	
c1: IF P-Early-Media private header extension is supported THEN m ELSE n/a. c2: IF SIP session timer extension is supported THEN m ELSE n/a. c3: IF the NGCN site can be deployed in an environment where it is trusted THEN m ELSE o.					

5.2.2.5 Supported Message bodies

According to TS 24.229 [12] SIP message body handling follows the rules of RFC 5621 [87]; see item 82 of table A.4 (for a UE) and item 92 of table 162 (for a proxy). These rules require that a UE supports 'multipart/mixed' and 'multipart/alternative' body types; for a proxy support is optional (dependent on whether the proxy will examine body contents).

If the NGCN supports conditions under which two or more body parts will have to be included in a single SIP message (for example SDP and location information) it has to be prepared to send and receive a 'multipart/mixed' or 'multipart/alternative' body in appropriate SIP messages.

Besides that the NGCN site is expected to support the message body types listed below:

- application/sdp: mandatory for both receiving and sending side
- application/vnd.etsaoc+xml for the Advice of Charge service: as specified in subclause 6.1.12 of TS 24.525 [3] mandatory for the receiving side if advice of charge is supported, not applicable otherwise.
- application/pidf+xml in accordance with RFC 4119 [78] and draft-ietf-sip-location-conveyance [24]:
  - mandatory for the sending side if geographical location has to be sent (unless location information is sent by reference) as specified in subclause 5.1.6.8 of TS 24.229 [12] or if NGCN has to act as a presentity (presence service);

- mandatory for the receiving side if NGCN has to act as a presence watcher or if the NGCN supports location based services.

Further body types may be allowed across the NGN-NGCN interface, e.g. under a service level agreement.

NOTE: Conditions for supporting pidf+xml for basic presence services require further studies as well as the conditions for supporting multipart bodies.

5.2.2.6 Event packages

The NGCN site supported event packages are listed below:

Table 5.28: Supported event packages

Item	Does the implementation support	Ref.	Subscriber	Notifier
2	refer package?	[7] 3	o	o
3	presence package?	[43] 6	o	o
4	eventlist with underlying presence package?	[44], [43] 6	o	o
5	presence.winfo template-package?	[47] 4	o	o
6	ua-profile package?	[48] 3	o	o
7	conference package?	[49] 3	o	o
8	message-summary package?	[50]	o	o
9	poc-settings package	[51]	n/a	n/a

5.2.3 SDP protocol

5.2.3 SDP protocol

For the NGCN the provisions of clause 6 of TS 24.229 [12] and TS 24.525 [3], for a UE apply with the following qualifications:

- At a minimum the NGCN is expected to support SDP offer / answer exchanges as described RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP) [91].

- Reliable provisional responses and the PRACK method are optional, and neither side must depend on SDP carried in a 18x response or a PRACK message. The NGCN site shall not require reliable provisional responses (i.e. 100rel option in Require header field) on outgoing INVITE requests

- If the UPDATE method is supported it can be used for SDP offer/answer exchange before and after the call has been answered.

- TS 24.229 [12] requires inclusion of a bandwidth parameter for audio and video media lines.

- According to TS 24.229 [12] an offer-answer cycle should result in a single codec per media type; if this is not the case a further offer should be issued to eliminate all codecs except the selected one.

The support of SDP extensions is detailed in table 5.29.

Table 5.29: Major capabilities

Item	Does the implementation support capabilities within main protocol extensions	Reference	Status	Comment
22	integration of resource management and SIP?	[54], [55]	o	
23	grouping of media lines?	[68]	c2	
24	mapping of media streams to resource reservation flows?	[69]	c3	
25	SDP bandwidth modifiers for RTCP bandwidth?	[70]	o (see note)	
26	TCP-based media transport in the session description protocol?	[71]	o	
27	interactive connectivity establishment?	[72]	o	
28	session description protocol format for binary floor control protocol streams?	[73]	o	
29	extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)?	[74]	o	
30	SDP capability negotiation?	[75]	c1	
c1:	IF 4.1/2 THEN m ELSE o - - multimedia telephony service			
c2:	IF 6.30/24 THEN m ELSE o - - mapping of media streams to resource reservation flows.			
c3:	IF there are access specific procedures as used in TS 24.229 [12] which the NGCN is using THEN m ELSE o.			
NOTE:	For "video" and "audio" media types that utilise RTP/RTCP, if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [70], then it shall be specified. For other media types, it may be specified.			

The following table provide information on the SDP protocol to be supported by the NGCN site for the interconnection to the NGN.

It is based on tables A.317, A.318 and A.319 of TS 24.229 [12] and considering Business Trunking specific requirements as described in TS 24.525 [3].

Table 5.30: SDP types

Item	Type	Reference	Sending	Receiving
	Session level description			
1	v= (protocol version)	[76] 5.1	m	m
2	o= (owner/creator and session identifier)	[76] 5.2	m	m
3	s= (session name)	[76] 5.3	m	m
4	i= (session information)	[76] 5.4	o	m
5	u= (URI of description)	[76] 5.5	n/a	n/a
6	e= (email address)	[76] 5.6	n/a	n/a
7	p= (phone number)	[76] 5.6	n/a	n/a
8	c= (connection information)	[76] 5.7	m.1	m
9	b= (bandwidth information)	[76] 5.8	o (see note)	m
	Time description (one or more per description)			
10	t= (time the session is active)	[76] 5.9	m	m
11	r= (zero or more repeat times)	[76] 5.10	n/a	n/a
	Session level description (continued)			
12	z= (time zone adjustments)	[76] 5.11	n/a	n/a
13	k= (encryption key)	[76] 5.12	x	n/a
14	a= (zero or more session attribute lines)	[76] 5.13	o	m
	Media description (zero or more per description)			
15	m= (media name and transport address)	[76] 5.14	m	m
16	i= (media title)	[76] 5.4	o	m
17	c= (connection information)	[76] 5.7	m.1	m
18	b= (bandwidth information)	[76] 5.8	o (see note)	m
19	k= (encryption key)	[76] 5.12	x	n/a
20	a= (zero or more media attribute lines)	[76] 5.13	o	m
m.1:	At least one of the parameters mandatory.			
NOTE:	For "video" and "audio" media types that utilise RTP/RTCP, it is specified. For other media types, it may be specified.			

5.2.4 Control plane transport

This depends on the method of interconnection; see subclause 6.2.4 for the subscription-based and subclause 7.2.4 for the peering-based method.

5.3 User plane interconnection

5.3.1 Media and Codec

5.3.1.1 DTMF

As specified in TS 24.229 [12], an NGCN site shall include the MIME subtype "telephone-event" in the media description in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733 [67].

If the MIME subtype "telephone-event" is not supported by the remote party, the NGCN site should be able to send and receive DTMF in the media flow using a suitable audio codec negotiated in the offer/answer exchange.

5.3.1.2 Codecs

TS 181 005 [79] specifies principles for the use of codecs in the NGN. Specifically TS 181 005 [79] mandates that the "NGN shall allow end to end negotiation of any codec between NGN entities (terminal, network elements)". Although no direct requirement is placed on entities within the NGCN; by merit of the fact that SIP is used as the protocol for the interconnect it is clear that the NGCN-NGN interconnection interface shall allow end to end negotiation of any codec between NGCN and NGCN/NGN entities.

If the NGCN supports narrow band voice services then, as specified in TS 181 005 [79], in order to enable interworking for narrow band voice services for public traffic, the NGCN shall be capable of sending and receiving ITU-T Recommendation G.711 [89] coded speech with a packetization size of 20 ms.

5.3.1.3 Modification of media session parameters

As specified in 3GPP TS 24.229 [12], modifications of the characteristics of the media session) can be issued by the NGCN site or by the NGN by sending a re-INVITE request. The ability to support modifications of early dialogs depends on the support of the UPDATE and PRACK methods (see table 5.1).

5.4 Numbering, naming and addressing

The following URI formats in SIP messages apply at the NGCN-NGN interconnection as standardized in 3GPP TS 24.229 [12] in order to provide business trunking services:

- SIP URI as defined in RFC 3261 [1], with the following qualifications:
  - The SIP URI can be either based on an E.164 number or a private number or it can be an e-mail style SIP URI, including device identifiers such as GRUUs.
  - Dial strings are not present on the NGCN-NGN interface.
  - As specified in [1], the ";user=phone" parameter is present in SIP URIs in which the user part is a telephone-subscriber string.
  - As specified in [1], the ";user=phone" parameter is not present in SIP URIs in which the user part is not a telephone-subscriber string in compliance with the tel URI definition of RFC 3966 [18]. According to this requirement, the phone-context parameter is mandatory when the user part of a SIP URI with a ";user=phone" parameter is not a global number.
- Tel URI defined in RFC 3966 [18] and according to the requirements defined in ECMA TR/96 [22]:
  - In accordance with RFC 3966 [18], the phone-context parameter is mandatory when the tel URI contains a private number.

In addition, the following URI formats in SIP Request-URIs may be applied at the NGCN-NGN interconnection as standardized in TS 24.229 [12] for the support of presence and instant messaging:

- IM URI defined in RFC 3860 [19];
- PRES URI defined in RFC 3859 [20].

Other URI formats may also be supported over the NGCN-NGN interconnection depending on the NGN operator and its customer agreements.

NOTE: The NGN behaviour in case of URIs that do not comply with the specified formats is outside the scope of the present document.

5.5 IP Version

The network elements interconnected on the NGCN-NGN Interconnection may support IPv4 only, IPv6 only or both.

The support of one or both of the IP versions is an option and should be based on bilateral agreement.

The control plane and the user plane may use different IP addresses and different IP versions.

In case IPv4 and IPv6 networks are interconnected, as specified in TS 24.229 [12], annex G and TS 29.162 [21], the involved P-CSCF shall apply the IP version interworking procedures for NA(P)-T-PT.

5.6 Security

5.6.1 Authentication

The authentication mechanism used on the NGCN-NGN interconnection should be part of the Service Level Agreement (SLA) between the operator and the enterprise.

It is expected that different mechanisms will apply for the two methods of interconnection; see subclause 6.6.1 for the subscription based approach and subclause 7.6.1 for the peering-based method.

6 Specific guidelines for the subscription based approach

6.1 Reference model for interconnection

6.1.1 General

The architectural split of the service layer and transport layer (used in the description below) is defined in ES 282 001 [16].

Clause 5.2 of TS 24.525 [3] describes the architectural requirements for the connection of an Next Generation Corporate Network site (NGCN site) to the NGN using the P-CSCF as an entry point at the service layer.

Clause 8.3 of TS 24.523 [4] shows the arrangement of the involved functional entities.

6.1.2 Functionalities performed by entities at the service layer

6.1.2.1 P-CSCF, S-CSCF

According to TS 24.525 [3], for the subscription based scenario the P-CSCF is the first contact point for the NGCN site within the IM subsystem (IMS). The NGCN site attaches to the P-CSCF at the Gm reference point.

The S-CSCF provides home server functions for the NGCN site, making use of the HSS as necessary.

Further definition of the P-CSCF and S-CSCF is provided in TS 23.228 [17] as modified by ES 282 007 [42].

6.1.2.2 AS

Business trunking may involve a dedicated application server that provides business trunking specific capabilities and may need to access the HSS for that purpose.

NOTE: If P-CSCF and S-CSCF together provide all business trunking related functions then no AS is needed.

6.1.2.3 NGCN

The NGCN site appears to the NGN like a UE attached to the P-CSCF at the Gm reference point.

6.1.3 Functionalities performed by entities at the transport layer

6.1.3.1 C-BGF

According to TS 24.525 [3], the main functional entity that is used at the transport layer to realise subscription-based business trunking and that is involved on the NGN-NGCN interface is the Core Border Gateway Function (C-BGF).

The C-BGF sits at the boundary between an access network and a core network and provides the interface between two IP-transport domains. Further definition of the C-BGF is provided in ES 282 001 [16].

6.1.4 Connectivity Access Network

As described in TS 24.525 [3], NGCN sites may be connected to any IP-CAN valid for TISPAN NGN. The present document assumes the following types of IP-CANs: xDSL and Ethernet LAN although it may be applicable to other types of IP-CANs.

Clause 9.2.1 of TS 24.229 [12] and TS 24.525 [3] subclause 7.1.1 specify methods for getting a P-CSCF SIP server domain name or IP address:

- P-CSCF SIP server domain name or IP address is received from the NASS (e. the NACF representing a DHCP server). In this case the P-CSCF address/port are found in DHCP Option 120 (for xDSL access).
- P-CSCF address provisioned through an O&M interface.
- P-CSCF SIP server domain name or IP address received using the TR-69 [95] CWMP. In this case the P-CSCF address/port are found in the ProxyServer (ProxyServerPort) field or the OuboundProxy (OutboundProxyPort) field defined in TR-104 [96].

Additionally, subclause 9.2.1. and related access technology specific annexes of TS 24.229 [12] specify methods of obtaining the P-CSCF address for all access technologies.

6.2 Control plane interconnection

6.2.1 SIP procedures

6.2.1.1 Outgoing requests from NGCN site

6.2.1.1.1 General

Procedures for outgoing requests are specified in TS 24.525 [3], subclause 6.1.4. The following subclauses provide further guidance on the expected NGCN site behaviour for the subscription based case in addition to subclause 5.2.1.1.

6.2.1.1.2 Calling and connected identifiers

Clause 5.2.1.1.2 applies with the addition that a calling party identity may be sent in a P-Preferred-Identity instead of a P-Asserted-Identity header field in accordance with RFC 3325 [29].

NOTE: If the NGN does not trust the NGCN site it will generate its own P-Asserted-Identity header field, which may take an NGCN-provided P-Asserted-Identity or P-Preferred-Identity into account or may be a default identity for the NGCN site. NGN will use a provided PAI or PPI if that matches one of the registered public user identities.

6.2.1.1.3 Privacy

See subclause 5.2.1.1.3.

In addition, a Privacy:id header field can also accompany a P-Preferred-Identity header field sent by the NGCN site.

6.2.1.1.4 Called identifier

See subclause 5.2.1.1.4.

6.2.1.1.5 SDP offer

NOTE: TS 24.229 [12] currently requires a UE to include an SDP offer when submitting an INVITE request. There is an issue with subscription-based business trunking if in certain situations the NGCN site is unable to include an SDP offer in the INVITE request.

6.2.1.2 Incoming requests to NGCN site

6.2.1.2.1 General

Procedures for incoming requests are specified in TS 24.525 [3], subclause 6.1.5. The following subclauses provide further guidance on the expected NGCN site behaviour for the subscription based case in addition to 5.2.1.2.

6.2.1.2.2 Calling identity

See subclause 5.2.1.2.2.

6.2.1.2.3 Called identity

See subclause 5.2.1.2.3.

6.2.1.2.4 Request-URI

As specified in TS 24.525 [3], if a loose-route indicator is configured for the NGCN site the Request-URI of a SIP request received from the NGN will convey the actual destination inside the NGCN (as specified in subclause 5.2.1.2.4), and the Route header field will contain the registered contact of the NGCN site.

If no loose-route indicator is configured in the NGCN site profile the Request-URI of a SIP request received from the NGN will contain the registered contact of the NGCN site, and the public user identity of the actual destination inside the NGCN is conveyed in the P-Called-Party-ID header field.

NOTE: The non-loose-route procedure may not be adequate for NGCN URIs that are not assigned public user identities, e.g. private GRUUs. This issue requires further study.

6.2.1.3 Registration

In the subscription based mode the NGCN site will register to the NGN as described in TS 24.525 [3] subclause 6.1.3, using a public user identity and a private user identity that represent the NGCN site as a whole. As specified in TS 24.229 [12] for UE"s, the NGCN site includes a Supported:path header field in the REGISTER request.

When using SIP Digest, in addition to the procedures specified in RFC3261, the initial REGISTER includes an Authorization header field with the private user identity, as specified in TS 24.229 [12] subclause 5.1.

NOTE 1: This procedure implicitly registers all other public user identities assigned to the NGCN site as individual or wildcarded identities.

NOTE 2: If provisioned in the user profile associated with the NGCN site the loose route indication will be stored by the S-CSCF at registration time.

If present in the REGISTER response the P-Associated-URI header field contains the set of implicitly registered identities.

Successful registration will result in an association between the NGCN site and the P-CSCF used for registration, based on mutual authentication between NGCN site and S-CSCF. The NGCN should be prepared to receive signalling traffic from the NGN over this association and in turn is expected to use this association when sending signalling messages to the NGN. An association may be a security association, a TLS session or a relationship between public user identity and port number (see subclause 6.6.1).

As specified in TS 24.229 [12] for UE"s, the NGCN site subscribes to the reg-event package in order to get notified of status changes regarding its registration (refer to subclause 4.4.2.4).

6.2.2 SIP protocol elements

6.2.2.1 General

See subclause 5.2.2.1.

6.2.2.2 Methods

In addition to table 5.1, the methods listed in table 6.1 apply in the context of the subscription based scenario.

Table 6.1: Additional supported methods for subscription based scenario

Item	PDU	Sending		Receiving	
		Ref.	Profile Status	Ref.	Profile Status
10	NOTIFY request	[9]	o	[9]	m (see note)
11	NOTIFY response	[9]	m (see note)	[9]	o
18	REGISTER request	[1] 10	m	[1] 10	x
19	REGISTER response	[1] 10	x	[1] 10	m
20	SUBSCRIBE request	[9]	m (see note)	[9]	o
21	SUBSCRIBE response	[9]	o	[9]	m (see note)
NOTE: See subclause 4.4.2.4 (reg-event package).					

6.2.2.3 Responses

See subclause 5.2.2.3.

6.2.2.4 Header fields

In addition to subclause 5.2.2.4, the following header fields apply for the following methods.

Table 6.2: Void

Table 6.3: Supported headers within the BYE request

Item	Header	Ref.	Sending	Receiving	Comment
21A	Security-Client	[32] 2.3.1	c2	n/a	
21B	Security-Verify	[32] 2.3.1	c3	n/a	
c2: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a c3: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a					

Table 6.4: Void

Table 6.5: Void

Table 6.6: Void

Table 6.7: Supported headers within the INFO request

Item	Header	Ref.	Sending	Receiving	Comment
22	P-Access-Network-Info	[28] 4.4	c15	n/a	
37	Security-Client	[32] 2.3.1	c4	n/a	
38	Security-Verify	[32] 2.3.1	c5	n/a	
c4: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c5: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.8: Supported headers within the 200 OK response to the INFO request

Item	Header	Ref.	Sending	Receiving	Comment
21	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.9: Supported headers within the INVITE request

Item	Header	Ref.	Sending	Receiving	Comment
24A	P-Access-Network-Info	[28] 4.4	c1	n/a	
24C	P-Asserted-Service	[34] 4.1	n/a	c4	
24D	P-Called-Party-ID	[28] 4.2	x	c2	
25	P-Media-Authorization	[37] 5.1	n/a	o	
25A	P-Preferred-Identity	[29] 9.2	o	n/a	
25B	P-Preferred-Service	[34] 4.2	c3	n/a	
33A	Security-Client	[32] 2.3.1	c7	n/a	
33B	Security-Verify	[32] 2.3.1	c8	n/a	
c1: IF the access type is GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN AND IF P-Access-Network-Info extension is supported THEN "m" ELSE "o".					
c2: IF P-Called-Party-ID extension is supported THEN o ELSE n/a.					
c3: IF identification of communication services extension is supported THEN o ELSE n/a.					
c4: IF identification of communication services extension is supported THEN m ELSE n/a.					
c7: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c8: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					

Table 6.10: Supported headers within the 200 OK response to the INVITE

Item	Header	Ref.	Sending	Receiving	Comment
23	P-Access-Network-Info	[28] 4.4	c1	n/a	
27	P-Media-Authorization	[37] 5.1	n/a	o	
c1 IF GPRS, 3GPP2, I-WLAN and DOCSIS IP-CAN access types are used THEN m ELSE o.					

NOTE: Table 6.10 gives hint on the headers' status for all the remaining possible responses to the INVITE request.

Table 6.11: Supported headers within the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
18A	P-Access-Network-Info	[28] 4.4	c15	n/a	
18C	P-Asserted-Service	[34] 4.1	n/a	c3	
18D	P-Called-Party-ID	[28] 4.2	x	c1	
18G	P-Preferred-Identity	[29] 9.2	o	n/a	
18H	P-Preferred-Service	[34] 4.2	c2	n/a	
25A	Security-Client	[32] 2.3.1	c6	n/a	
25B	Security-Verify	[32] 2.3.1	c7	n/a	
c1: IF P-Called-Party-ID extension is supported THEN o ELSE n/a.					
c2: IF identification of communication services extension is supported THEN o ELSE n/a.					
c3: IF identification of communication services extension is supported THEN m ELSE n/a.					
c6: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c7: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.12: Supported headers within the 2xx response to the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
12A	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.13: Supported headers within the NOTIFY request

Item	Header	Ref.	Sending	Receiving	Comment
17A	P-Access-Network-Info	[28] 4.4	c15	n/a	
22A	Security-Client	[32] 2.3.1	c4	n/a	
22B	Security-Verify	[32] 2.3.1	c5	n/a	
c4: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c5: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.14: Supported headers within the 200 OK response to NOTIFY

Item	Header	Ref.	Sending	Receiving	Comment
1	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.15: Supported headers within the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
19C	P-Asserted-Service	[34] 4.1	n/a	c6	
19D	P-Called-Party-ID	[28] 4.2	x	c1	
19H	P-Preferred-Service	[34] 4.2	c2	n/a	
24A	Security-Client	[32] 2.3.1	c4	n/a	
24B	Security-Verify	[32] 2.3.1	c5	n/a	
25	Supported	[1] 20.37	m	m	
c1: IF P-Called-Party-ID extension is supported THEN o ELSE n/a.					
c2: IF identification of communication services extension is supported THEN o ELSE n/a.					
c4: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c5: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c6: IF identification of communication services extension is supported THEN m ELSE n/a.					

Table 6.16: Supported headers within the 200 OK response to the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
22	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.17: Supported headers within the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
16A	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.18: Supported headers within the 200 OK response to the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
13	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.19: Supported headers within the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
22A	P-Asserted-Service	[34] 4.1	n/a	c3	
21	P-Access-Network-Info	[28] 4.4	c15	n/a	
23	P-Called-Party-ID	[28] 4.2	x	c1	
26	P-Preferred-Identity	[29] 9.2	o	n/a	
26A	P-Preferred-Service	[34] 4.2	c2	n/a	
38	Security-Client	[32] 2.3.1	c5	n/a	
39	Security-Verify	[32] 2.3.1	c6	n/a	
c1: IF P-Called-Party-ID extension is supported THEN o ELSE n/a.					
c2: IF identification of communication services extension is supported THEN o ELSE n/a.					
c3: IF identification of communication services extension is supported THEN m ELSE n/a.					
c5: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c6: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.20: Supported headers within the 2xx response to the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
17	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.21: Supported headers within the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
14A	P-Access-Network-Info	[28] 4.4	c15	n/a	
14C	P-Asserted-Service	[34] 4.1	n/a	c3	
14D	P-Called-Party-ID	[28] 4.2	x	c1	
14G	P-Preferred-Identity	[29] 9.2	o	n/a	
14H	P-Preferred-Service	[34] 4.2	c2	n/a	
20A	Security-Client	[32] 2.3.1	c6	n/a	
20B	Security-Verify	[32] 2.3.1	c7	n/a	
c1 IF P-Called-Party-ID extension is supported THEN o ELSE n/a.					
c2: IF identification of communication services extension is supported THEN o ELSE n/a.					
c3: IF identification of communication services extension is supported THEN m ELSE n/a.					
c6: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.					
c7: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.					
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.22: Supported headers within the 2xx response to the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
10A	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.23: Supported headers within the REGISTER request

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	o	n/a	
2	Accept-Encoding	[1] 20.2	o	n/a	
3	Accept-Language	[1] 20.3	o	n/a	
3A	Allow	[1] 20.5	o	n/a	
4	Allow-Events	[9] 7.2.2	o	n/a	
5	Authorization	[1] 20.7	m	n/a	
6	Call-ID	[1] 20.8	m	n/a	
7	Call-Info	[1] 20.9	o	n/a	
8	Contact	[1] 20.10	m	n/a	
9	Content-Disposition	[1] 20.11	o	n/a	
10	Content-Encoding	[1] 20.12	o	n/a	
11	Content-Language	[1] 20.13	o	n/a	
12	Content-Length	[1] 20.14	m	n/a	
13	Content-Type	[1] 20.15	m	n/a	
14	Cseq	[1] 20.16	m	n/a	
15	Date	[1] 20.17	o	n/a	
16	Expires	[1] 20.19	o	n/a	
17	From	[1] 20.20	m	n/a	
17A	Geolocation	[24] 3.2	o	n/a	
17B	History-Info	[25] 4.1	o	n/a	
17C	Max-Breadth	[53] 5.8	n/a	n/a	
18	Max-Forwards	[1] 20.22	m	n/a	
19	MIME-Version	[1] 20.24	o	n/a	
20	Organization	[1] 20.25	o	n/a	
20A	P-Access-Network-Info	[28] 4.4	c15	n/a	
20B	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
20C	P-Charging-Vector	[28] 4.6	n/a	n/a	
20D	P-User-Database	[36] 4	n/a	n/a	
20E	P-Visited-Network-ID	[28] 4.3	x	n/a	
20FE	Path	[56] 4	x	n/a	
20GF	Privacy	[30] 4.2	n/a	n/a	
21	Proxy-Authorization	[1] 20.28	o	n/a	
22	Proxy-Require	[1] 20.29	o	n/a	
22A	Reason	[31] 2	o	n/a	
22B	Referred-By	[33] 3	n/a	n/a	
22C	Request-Disposition	[23] 9.1	n/a	n/a	
23	Require	[1] 20.32	o	n/a	
24	Route	[1] 20.34	n/a	n/a	
24A	Security-Client	[32] 2.3.1	c1	n/a	
24B	Security-Verify	[32] 2.3.1	c1	n/a	
25	Supported	[1] 20.37	m	n/a	Contains the option-tag "path" and if GRUU is supported the option-tag "gruu".
26	Timestamp	[1] 20.38	o	n/a	
27	To	[1] 20.39	m	n/a	
28	User-Agent	[1] 20.41	o	n/a	
29	Via	[1] 20.42	m	n/a	
c1: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is supported as security mechanism THEN m ELSE n/a. c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.24: Supported headers within the 200 OK response to the REGISTER

Item	Header	Ref.	Sending	Receiving	Comment
1	Accept	[1] 20.1	n/a	m	
2	Accept-Encoding	[1] 20.2	n/a	m	
3	Accept-Language	[1] 20.3	n/a	m	
4	Allow	[1] 20.5	n/a	m	
5	Allow-Events	[9] 7.2.2	n/a	m	
6	Authentication-Info	[1] 20.6	n/a	m	
7	Call-ID	[1] 20.8	n/a	m	
8	Call-Info	[1] 20.9	n/a	o	
9	Contact	[1] 20.10	n/a	m	
10	Content-Disposition	[1] 20.11	n/a	m	
11	Content-Encoding	[1] 20.12	n/a	m	
12	Content-Language	[1] 20.13	n/a	m	
13	Content-Length	[1] 20.14	n/a	m	
14	Content-Type	[1] 20.15	n/a	m	
15	Cseq	[1] 20.16	n/a	m	
16	Date	[1] 20.17	n/a	m	
17	Flow-Timer	[65] 11	n/a	o	
18	From	[1] 20.20	n/a	m	
19	Geolocation	[24] 3.2	n/a	n/a	
20	History-Info	[25] 4.1	n/a	o	
21	MIME-Version	[1] 20.24	n/a	m	
22	Organization	[1] 20.25	n/a	o	
23	P-Access-Network-Info	[28] 4.4	n/a	n/a	
24	P-Associated-URI	[28] 4.1	n/a	m	See subclause 4.4.2.4.
25	Path	[56] 4	n/a	o	
26	P-Charging-Function-Addresses	[28] 4.5	n/a	n/a	
27	P-Charging-Vector	[28] 4.6	n/a	n/a	
28	Privacy	[30] 4.2	n/a	n/a	
29	Require	[1] 20.32	n/a	m	
30	Server	[1] 20.35	n/a	o	
31	Service-Route	[37] 5	n/a	m	See subclause 4.4.2.4.
32	Supported	[1] 20.37	n/a	m	
33	Timestamp	[1] 20.38	n/a	m	
34	To	[1] 20.39	n/a	m	
35	User-Agent	[1] 20.41	n/a	o	
36	Via	[1] 20.42	n/a	m	
37	Warning	[1] 20.43	n/a	o	

Table 6.25: Supported headers within the SUBSCRIBE request

Item	Header	Ref.	Sending	Receiving	Comment
18B	P-Access-Network-Info	[28] 4.4	c15	n/a	
18D	P-Asserted-Service	[28] 4.1	n/a	c3	
18E	P-Called-Party-ID	[28] 4.2	x	c1	
18H	P-Preferred-Identity	[29] 9.2	o	n/a	
18I	P-Preferred-Service	[34] 4.2	c2	n/a	
23A	Security-Client	[32] 2.3.1	c6	n/a	
23B	Security-Verify	[32] 2.3.1	c7	n/a	

c1: IF P-Called-Party-ID extension is supported THEN o ELSE n/a.
c2: IF identification of communication services extension is supported THEN o ELSE n/a.
c3: IF identification of communication services extension is supported THEN m ELSE n/a.
c6: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a.
c7: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a.
c15: IF P-Access-Network-Info extension is supported THEN m ELSE n/a.

Table 6.26: Supported headers within the 2xx response to SUBSCRIBE

Item	Header	Ref.	Sending	Receiving	Comment
19	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m ELSE n/a.					

Table 6.27: Supported headers within the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
20A	P-Access-Network-Info	[28] 4.4	c15	n/a	
25A	Security-Client	[32] 2.3.1	c4	n/a	
25B	Security-Verify	[32] 2.3.1	c5	n/a	
c4: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN o ELSE n/a. c5: IF IMS AKA plus IPsec ESP or SIP Digest with TLS is used for authentication THEN m ELSE n/a. c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

Table 6.28: Supported headers within the 200 OK response to the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
21	P-Access-Network-Info	[28] 4.4	c15	n/a	
c15: IF P-Access-Network-Info extension is supported THEN m else n/a.					

6.2.2.5 Supported message bodies

See subclause 5.2.2.5.

6.2.2.6 Event packages

In addition to subclause 5.2.2.6 the event packages in the following table apply:

Table 6.29: Supported event packages

Item	Does the implementation support	Ref.	Subscriber	Notifier
1	reg event package?	[45]	M (see note)	n/a
1A	reg event package extension for GRUUs?	[46]	o	n/a
NOTE: See subclause 4.4.2.4.				

6.2.3 SDP protocol

See subclause 5.2.3.

6.2.4 Control plane transport

The control plane transport of the NGCN-NGN Interconnection interface in the subscription based approach complies with the provisions in subclause 4.2A of TS 24.229 [12] applicable to a UE and a P-CSCF with modifications as described in the following subclauses.

A security gateway may exist with IPv4 and IPv6 interfaces between the NGCN and the NGN.

NOTE: Need statement concerning behaviour when two SIP entities within an NGCN site are both capable of registering through the P-CSCF, either on a cold or hot standby basis or on a load sharing basis.

6.2.4.1 Keep alive mechanism

TS 24.229 [12] provides two solutions to keep a connection alive depending on the NAT traversal mechanism: When SIP outbound, as specified in annex K is used the SIP-outbound keep-alive mechanism applies. When the hosted NAT

traversal mechanism defined in annex F is used, the keep-alive mechanism based on short registrations or the SIP-outbound keep-alive mechanism can be used as described in subclause F.4.2 of 3GPP TS 24.229.

NOTE: Use of alternative mechanisms (e.g. OPTIONS method) is outside the scope of the present document.

6.2.4.2 P-CSCF redundancy

Clause 6.1.4 describes several methods enabling an NGCN site to obtain the IP address or the SIP server domain name of the P-CSCF. If a SIP server domain name of the P-CSCF is obtained, RFC 3263 [86] procedures as specified in TS 24.229 [12], subclause E.2.2.1 can be applied to obtain from the DNS the IP address of the P-CSCF, including backup addresses for use in case of failure of the preferred choice.

NOTE 1: 3GPP TR 23.812 [94] may provide solutions for including load status information in the DNS (e.g. setting the weight field in SRV records based on the actual server load). However this will not affect the NGCN-NGN interface but rather the DNS behaviour.

NOTE 2: Business Trunking specific redundancy mechanisms are for further study in 3GPP TS 24.525 [3].

6.3 User plane interconnection

6.3.1 Media and Codec

6.3.1.1 DTMF

See subclause 5.3.1.1.

6.3.1.2 Codecs

See subclause 5.3.1.2.

6.3.1.3 Modification of media session parameters

See subclause 5.3.1.3.

6.4 Numbering, naming and addressing

See subclause 5.4.

6.5 IP Version

See subclause 5.5.

6.6 Security

6.6.1 Authentication

The NGCN site can connect to the NGN using one of the following authentication mechanisms between NGN and NGCN site as specified in TS 24.229 [12], subclause 5.1.1.5:

- IMS AKA with IPSec;
- SIP digest over TLS;
- SIP digest without TLS.

NOTE: When SIP Digest is used without TLS, the NGCN site may need to provide authentication credentials in all requests, as specified in 3GPP TS 33.203 [52] annex N, unless a check on the source address/port of the messages sent by the NGCN site is considered sufficiently secure by the NGN.

Which of these authentication mechanisms are applicable is part of an SLA between NGN and NGCN.

An NGCN has to support at least one of the above mechanisms and should allow configuration of the authentication mechanism to be used if it supports more than one. For the mechanisms TLS and IMS AKA support of the security agreement extension of SIP is mandatory.

Irrespective of the mechanism used, the NGCN site is authenticated as a whole as part of the registration process. If TLS or IMS AKA is in use, non-REGISTER requests from the NGCN are implicitly authenticated by being sent within the security context established between NGN and NGCN during registration, but non-REGISTER requests may be challenged by the NGN if SIP Digest without TLS is in use. Individual NGCN entities beyond the NGCN attachment point are never subject to being challenged by the NGN.

In addition, if allowed by the SLA, implicit authentication may also be used. This does not require any specific action from the NGCN site and relies on the NASS bundled authentication procedure at the NGN side.

NOTE: The authentication mechanism discussed above is different from NGCN-internal authentication mechanisms between entities inside the NGCN; refer to draft ECMA-TR/100 [88] for more information. NGCN-specific authentication information may traverse the NGN if exchanged between NGCN sites connected by the NGN.

7 Specific guidelines for the peering-based approach

7.1 Reference model for interconnection

7.1.1 General

7.1.2 Functionalities performed by entities at the service layer

7.1.2.1 Interconnection Border Control Function (IBCF)

According to 3GPP TS 24.525 [3], for the peering based scenario the IBCF is the contact point for the NGCN site within the IM subsystem (IMS). The NGCN site attaches to the IBCF at the Ic reference point.

Further definition of the IBCF is provided in 3GPP TS 23.228 [17] as modified by ETSI ES 282 007 [42].

7.1.2.2 NGCN

The NGCN site appears to the NGN like an IBCF attached to the (NGN's) IBCF at the Ic reference point.

7.2 Control plane interconnection

7.2.1 SIP procedures

7.2.1.1 Outgoing requests from NGCN site

Procedures for outgoing requests are specified in 3GPP TS 24.525 [3], subsubclause 6.2.4 for the peering based case. The peering based scenario has no further requirements in addition to 5.2.1.1.

NOTE: If the NGN does not trust the NGCN site it will remove a P-Asserted-Identity header field provided by the NGCN site, e. the message will proceed without a P-Asserted-Identity.

7.2.1.2 Incoming requests to NGCN site

Procedures for incoming requests are specified in 3GPP TS 24.525 [3], subsubclause 6.2.5 for the peering based case. The peering based scenario has no further requirements in addition to 5.2.1.2.

7.2.1.3 Registration

Not applicable.

7.2.2 SIP protocol elements

7.2.2.1 General

7.2.2.2 Methods

See subclause 5.2.2.2.

In addition to table 5.1, the methods listed in table 7.1 apply in the context of the peering based scenario.

Table 7.1: Supported methods

Item	PDU	Sending		Receiving	
		Ref.	Profile Status	Ref.	Profile Status
10	NOTIFY request	[9]	o	[9]	o
11	NOTIFY response	[9]	o	[9]	o
20	SUBSCRIBE request	[9]	o	[9]	o
21	SUBSCRIBE response	[9]	o	[9]	o

7.2.2.3 Responses

See subclause 5.2.2.3.

7.2.2.4 Header fields

In addition to 5.2.2.4, the following header fields apply for the following methods.

Table 7.2: Void

Table 7.3: Supported headers within the BYE request

Item	Header	Ref.	Sending	Receiving	Comment
21A	Security-Client	[32] 2.3.1	n/a	n/a	
21B	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.4: Void

Table 7.5: Void

Table 7.6: Void

Table 7.7: Supported headers within the INFO request (peering based approach)

Item	Header	Ref.	Sending	Receiving	Comment
22	P-Access-Network-Info	[28] 4.4	n/a	n/a	
37	Security-Client	[32] 2.3.1	n/a	n/a	
38	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.8: Supported headers within the 200 OK response to the INFO request

Item	Header	Ref.	Sending	Receiving	Comment
21	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.9: Supported headers within the INVITE request

Item	Header	Ref.	Sending	Receiving	Comment
24A	P-Access-Network-Info	[28] 4.4	n/a	n/a	
24C	P-Asserted-Service	[34] 4.1	n/a	n/a	
24D	P-Called-Party-ID	[28] 4.2	x	n/a	
25	P-Media-Authorization	[37] 5.1	n/a	n/a	
25A	P-Preferred-Identity	[29] 9.2	n/a	n/a	
25B	P-Preferred-Service	[34] 4.2	n/a	n/a	
33A	Security-Client	[32] 2.3.1	n/a	n/a	
33B	Security-Verify	[32] 2.3.1	n/a	n/a	
NOTE: The use of this header is subject to Spec T.					

Table 7.10: Supported headers within the 200 OK response to the INVITE request

Item	Header	Ref.	Sending	Receiving	Comment
23	P-Access-Network-Info	[28] 4.4	n/a	n/a	
27	P-Media-Authorization	[37] 5.1	x	n/a	

Table 7.11: Supported headers within the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
18A	P-Access-Network-Info	[28] 4.4	n/a	n/a	
18C	P-Asserted-Service	[34] 4.1	n/a	n/a	
18D	P-Called-Party-ID	[28] 4.2	x	n/a	
18G	P-Preferred-Identity	[29] 9.2	n/a	n/a	
18H	P-Preferred-Service	[34] 4.2	n/a	n/a	
25A	Security-Client	[32] 2.3.1	n/a	n/a	
25B	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.12: Supported headers within the 2xx response to the MESSAGE request

Item	Header	Ref.	Sending	Receiving	Comment
12A	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.13: Supported headers within the NOTIFY request

Item	Header	Ref.	Sending	Receiving	Comment
17A	P-Access-Network-Info	[28] 4.4	n/a	n/a	
22A	Security-Client	[32] 2.3.1	n/a	n/a	
22B	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.14: Supported headers within the 200 OK response to NOTIFY

Item	Header	Ref.	Sending	Receiving	Comment
1	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.15: Supported headers within the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
19C	P-Asserted-Service	[34] 4.1	n/a	n/a	
19D	P-Called-Party-ID	[28] 4.2	x	n/a	
19H	P-Preferred-Service	[34] 4.2	n/a	n/a	
24A	Security-Client	[32] 2.3.1	n/a	n/a	
24B	Security-Verify	[32] 2.3.1	n/a	n/a	
25	Supported	[1] 20.37	o	m	
NOTE: The use of this header is subject to Spec T.					

Table 7.16: Supported headers within the 200 OK response to the OPTIONS request

Item	Header	Ref.	Sending	Receiving	Comment
22	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.17: Supported headers within the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
16A	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.18: Supported headers within the 200 OK response to the PRACK request

Item	Header	Ref.	Sending	Receiving	Comment
13	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.19: Supported headers within the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
22A	P-Asserted-Service	[34] 4.1	n/a	n/a	
21	P-Access-Network-Info	[28] 4.4	n/a	n/a	
23	P-Called-Party-ID	[28] 4.2	x	n/a	
26	P-Preferred-Identity	[29] 9.2	n/a	n/a	
26A	P-Preferred-Service	[34] 4.2	n/a	n/a	
38	Security-Client	[32] 2.3.1	n/a	n/a	
39	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.20: Supported headers within the 2xx response to the PUBLISH request

Item	Header	Ref.	Sending	Receiving	Comment
17	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.21: Supported headers within the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
14A	P-Access-Network-Info	[28] 4.4	n/a	n/a	
14C	P-Asserted-Service	[34] 4.1	n/a	n/a	
14D	P-Called-Party-ID	[28] 4.2	x	n/a	
14G	P-Preferred-Identity	[29] 9.2	x	n/a	
14H	P-Preferred-Service	[34] 4.2	n/a	n/a	
20A	Security-Client	[32] 2.3.1	n/a	n/a	
20B	Security-Verify	[32] 2.3.1	n/a		

Table 7.22: Supported headers within the 2xx response to the REFER request

Item	Header	Ref.	Sending	Receiving	Comment
10A	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.23: Supported headers within the SUBSCRIBE request

Item	Header	Ref.	Sending	Receiving	Comment
18B	P-Access-Network-Info	[28] 4.4	n/a	n/a	
18D	P-Asserted-Service	[28] 4.1	n/a	n/a	
18E	P-Called-Party-ID	[28] 4.2	x	n/a	
18H	P-Preferred-Identity	[29] 9.2	n/a	n/a	
18I	P-Preferred-Service	[34] 4.2	n/a	n/a	
23A	Security-Client	[32] 2.3.1	n/a	n/a	
23B	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.24: Supported headers within the 2xx response to SUBSCRIBE

Item	Header	Ref.	Sending	Receiving	Comment
19	P-Access-Network-Info	[28] 4.4	n/a	n/a	

Table 7.25: Supported headers within the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
20A	P-Access-Network-Info	[28] 4.4	n/a	n/a	
25A	Security-Client	[32] 2.3.1	n/a	n/a	
25B	Security-Verify	[32] 2.3.1	n/a	n/a	

Table 7.26: Supported headers within the 200 OK response to the UPDATE request

Item	Header	Ref.	Sending	Receiving	Comment
21	P-Access-Network-Info	[28] 4.4	n/a	n/a	

7.2.2.5 Supported message bodies

See subclause 5.2.2.5.

7.2.2.6 Event packages

See subclause 5.2.2.6.

7.2.3 SDP protocol

See subclause 5.2.3.

7.3 User plane interconnection

7.3.1 Media and Codec

7.3.1.1 DTMF

See subclause 5.3.1.1.

7.3.1.2 Codecs

See subclause 5.3.1.2.

7.3.1.3 Modification of media session parameters

See subclause 5.3.1.3.

7.4 Numbering, naming and addressing

See subclause 5.4.

7.5 IP Version

See subclause 5.5.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
14/07/2014					Version for input to 3GPP CT1#88		0.0.1
09-2014	CT-65	CP-140628			Version 1.0.0 presented for information at CT plenary	0.0.1	1.0.0
10-2014	C1-88bis					1.0.0	1.1.0
12-2014	CT-66	CP-140810			Version 2.0.0 presented for approval at CT plenary	1.1.0	2.0.0
12-2014	CT-66				Version 12.0.0 created after approval at CT plenary	2.0.0	12.0.0

History

Document history		
V12.0.0	January 2015	Publication