ETSI TS 124 525 V15.0.0 (2018-06)

Universal Mobile Telecommunications System (UMTS);
LTE;
Business trunking;
Architecture and functional description
(3GPP TS 24.525 version 15.0.0 Release 15)

Reference
RTS/TSGC-0124525vf00

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) 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**", "**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 Specification 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 present document provides architecture and functional requirements for business trunking for the Next Generation Network (NGN).

The present document also specifies the protocol requirements for the Next Generation Corporate Networks (NGCNs) to attach to the NGN (in particular the IM CN subsystem) and also any protocol requirements relation to application servers provided in support of business trunking.

Business trunking is a set of NGN capabilities that may be applied to communications between NGCNs using the NGN as a transit.

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] 3GPP TS 22.519: "Business Communication Requirements".

[2] ETSI ES 282 001 (V3.4.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[3] ETSI ES 282 004 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[4] ETSI ES 282 007 (V2.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);IP Multimedia Subsystem (IMS);Functional architecture".

[5] Void.

[6] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[7] 3GPP TS 24.523: "Core and enterprise NGN interaction scenarios; Architecture and functional description".

[8] 3GPP TS 24.611: "Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[9] ETSI TS 183 019 (V.2.3.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

[10] 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[11] ETSI ES 283 035 (V.2.6.2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[12] 3GPP TS 24.647: "Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem".

[13] 3GPP TS 29.658: "SIP Transfer of IP Multimedia Service Tariff Information; Protocol specification".

[14] ETSI TS 183 065 (V3.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Customer Network Gateway Configuration Function; e3 Interface based upon CWMP".

[15] ETSI TS 185 003 (V2.3.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points".

[16] 3GPP TS 33.203: "3G security; Access security for IP-based services".

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

[18] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[19] Void.

[20] ETSI TR 102 634 (V1.1.1): "Next Generation Corporate Networks (NGCN) - Identification and Routing".

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

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

[23] Void.

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

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

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

[27] ETSI TS 181 005 (V3.3.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

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

[29] IETF RFC 5626 (October 2009): "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)".

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

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

[32] 3GPP TS 23.003: "Numbering, addressing and identification".

[33] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[34] ETSI TR 183 069 (V2.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Trunking; NGCN-NGN Interfaces Implementation Guide".

[35] 3GPP TS 29.165: "Inter-IMS Network to Network Interface (NNI)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.519 [1], ETSI ES 282 004 [3], 3GPP TS 23.228 [17], 3GPP TS 23.003 [32] and 3GPP TS 23.218 [33] apply.

3.2 Abbreviations

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

AOR	Address Of Record
AS	Application Server
B2BUA	Back-to-Back User Agent
CNG	Customer Network Gateway
CNGCF	Customer Network Gateway Control Function
CSCF	Call Session Control Function
DNS	Domain Name System
DSL	Digital Subscriber Line
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IWF	Interworking Function
LAN	Local Area Network
NASS	Network Attachment SubSystem
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
P-CSCF	Proxy CSCF
PNP	Private Numbering Plan
S-CSCF	Serving-CSCF
SIP	Session Initiation Protocol
SLA	Service Level Agreement
UE	User Equipment
URI	Uniform Resource Identifier

4 Overview

4.1 General principles

Business trunking refers to an architecture where corporate networks appear to the NGN as an NGCN. Although the interface between an NGCN and an NGN is IP-based, this does not preclude the existence of non-IP-based elements within the NGCN but not visible to the NGN. The NGCN appears to the NGN as a black box.

4.2 Access network interconnection

NGCN sites may be connected to any IP-connectivity Access Network (IP-CAN) valid for TISPAN NGN using a Customer Network Gateway (CNG), as defined in ETSI ES 282 001 [2] or connected to an NGN core network via an edge router of the enterprise.

Connection to an IP-CAN includes the case where the NGCN site incorporates a CNG as defined in ETSI TS 185 003 [15], connected to a DSL-based access network (see figure 4.1) as well as the case where the NGCN site comprises a corporate LAN with one or more edge routers playing the role of a CNG connected to access nodes in the operator's access network (see figure 4.2).

NOTE 1: Use of the "SIP Proxy/B2BUA" function within the CNG, as defined in ETSI TS 185 003 [15], is not applicable to the present release of the present document.

NOTE 2: Within an NGCN site, the CNG functionality may be collocated with an NGCN host or a stand-alone equipment unit.

Towards an access network, the NGCN site acts as a UE. For further details see clause 7.

Towards the IM CN subsystem, the entry point / exit point entity is dependent on the approach adopted and is described further in clause 6.

An NGCN connects a multiplicity of endpoints to the network, each of which may be an IP device or a legacy phone. The NGN does not need to have any knowledge on the individual endpoints connected to the NGCN.

With the subscription based approach, for each NGCN site, the Home Subscriber Server (HSS) stores a single public user identity and a single associated user profile enabling triggering of network-based services beyond those provided by the NGCN itself. A set of telephone numbers and/or SIP URIs are also associated with each NGCN site. The former could be expressed in the form of number ranges and the latter using wildcards in the user or host part.

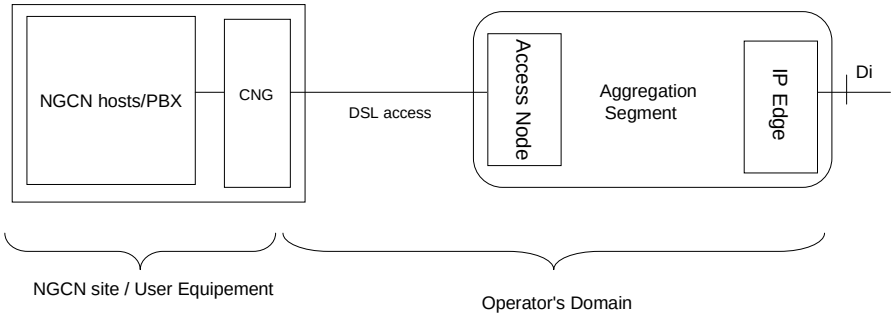

Figure 4.1: DSL access

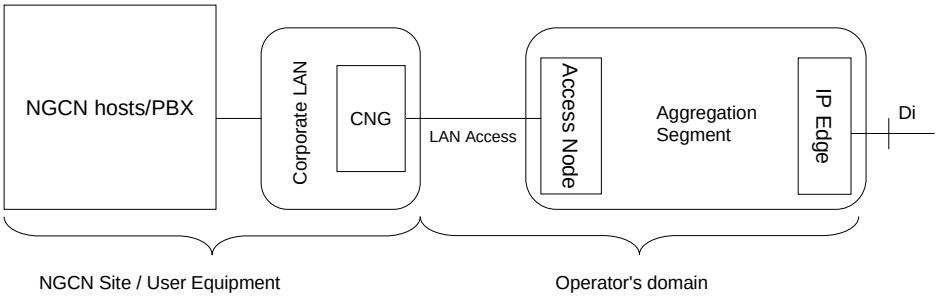

Figure 4.2: Corporate LAN access

Identifiers based on private numbers shall be handled in accordance with ETSI TR 102 634 [20].

4.3 Service level layer interconnection

The service level layer interconnection makes use of IMS. Two main interconnection arrangements are provided:

- Interconnection of the NGN and NGCN where the entry point to the IMS is the P-CSCF. This is known as the subscription-based approach. This is represented by scenario 5 in subclause 8.3 of 3GPP TS 24.523 [7]. In this case each site of the NGCN has a service subscription to the IMS, with an appropriate entry in the HSS. An AS is used to provide business trunking applications, e.g. those defined in 3GPP TS 22.519 [1], subclause 4.4. If such capabilities are not required, then the AS is not included in any request processing. The service level capabilities of this scenario are described further in subclause 6.1.

- Interconnection of the NGN and NGCN where the entry point to the IMS is the IBCF. This is known as the peering-based approach. This is represented by scenario 6 in subclause 8.4 of 3GPP TS 24.523 [7]. In this case there is no dynamic registration to the IMS of individual NGCN-users or NGCN-sites. However, the absence of such dynamic registrations in an HSS does not preclude the NGN to host enterprise specific data in an HSS. The service level capabilities of this scenario are described further in subclause 6.2.

The second of these arrangements is called the peering-based approach due to the similarity of the arrangement to the mechanism by which the IMS in two NGNs interconnect. The provision of the business trunking applications (e.g. those defined in 3GPP TS 22.519 [1], subclause 4.4) is realized by an intelligent routeing function, which may involve an AS depending on the actual enterprise specific data.

In none of the arrangements do the private extensions behind the NGCN need their own service subscription within the NGN, since they are owned and managed by the NGCN. The private extensions register with the NGCN, and the NGCN provides the individual services to the private extensions.

An architecturally similar case to the peering-based approach is represented by scenario 3 in subclause 7.1 of 3GPP TS 24.523 [7]. In this case, SIP requests at one entry point are always routed to the same exit point, and no business trunking applications are provided. The service level capabilities of this scenario are described further in subclause 6.3 of the present document. This scenario carries private network traffic only.

5 Functional architecture

5.1 General

The architectural split of the service layer and transport layer (used in the description below) is defined in ETSI ES 282 001 [2].

5.2 Subscription based business trunking

5.2.1 General

This describes the architectural requirements for the connection of an NGCN site to the NGN using the P-CSCF as an entry point at the service layer.

Subclause 8.3 of 3GPP TS 24.523 [7] shows the arrangement of the involved functional entities.

5.2.2 Used functional entities at the service layer

The main functional entities from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise subscription-based business trunking arrangements are as follows:

- P-CSCF;
- S-CSCF;
- AS (in case a business trunking application is required); and
- HSS.

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, e.g. I-CSCF, are not listed.

Within the AS, the additional services can be provided by the home network operator, or can be provided by a third party service provider. It is also possible that the enterprise itself provides the services, by providing equipment that acts as an application server beyond an ISC gateway function.

A description of specific procedures executed to provide subscription-based business trunking can be found in subclause 6.1.

5.2.3 Used reference points at the service layer

The main reference points from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise subscription-based business trunking arrangements are as follows:

- Gm (this reference point forms the point of interconnection between the NGCN site and the NGN at the service layer);
- Mw;

- Cx;
- ISC (in case a business trunking application is required);
- Sh (in case a business trunking application is required);
- e2; and
- Gq'.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.2.4 Used functional entities at the transport layer

The main functional entities from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise subscription-based business trunking arrangements are as follows:

- BGF (whether an I-BGF or a C-BGF performs this function requires further study).

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, are not listed.

5.2.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise subscription-based business trunking arrangements are as follows:

- none identified.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.3 Peering-based business trunking

5.3.1 General

This describes the architectural requirements for the connection of an NGCN site to the NGN using the IBCF as an entry point at the service layer.

Subclause 8.4 of 3GPP TS 24.523 [7] shows the arrangement of the involved functional entities.

Optionally an AS may be used to provide business trunking applications, e.g. those defined in clause 4.4 of 3GPP TS 22.519 [1]. One mechanism to support such functionality is to use an AS attached to a transit function (see 3GPP TS 23.218 [33]) using the ISC interface. Based on an SLA with the NGCN concerned this option is administrated in the related subscriber profile in an HSS.

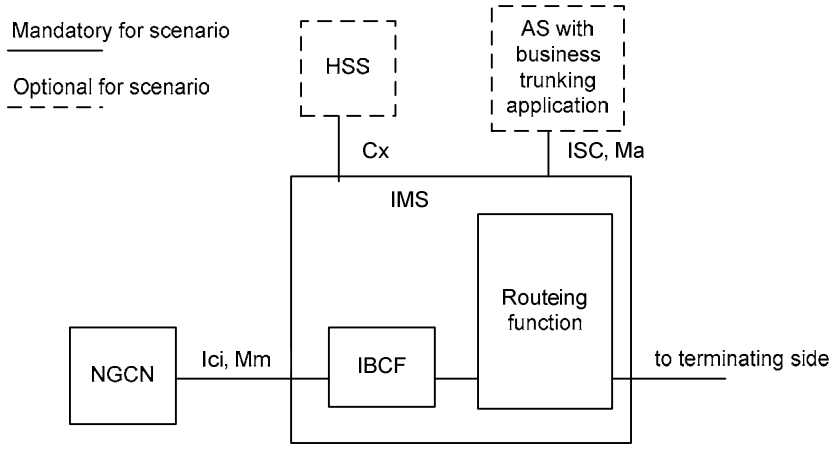

Figure 5.1: Originating Side with AS and HSS

Because the routeing function in the originating scenario has to behave like a CSCF performing originating procedures, the IBCF provokes this by insertion of an originate-indication in the forwarded request (e.g. "orig" parameter in the related Route header field).

NOTE: The IBCF capability to invoke originating services is added in 3GPP TS 23.228 [17].

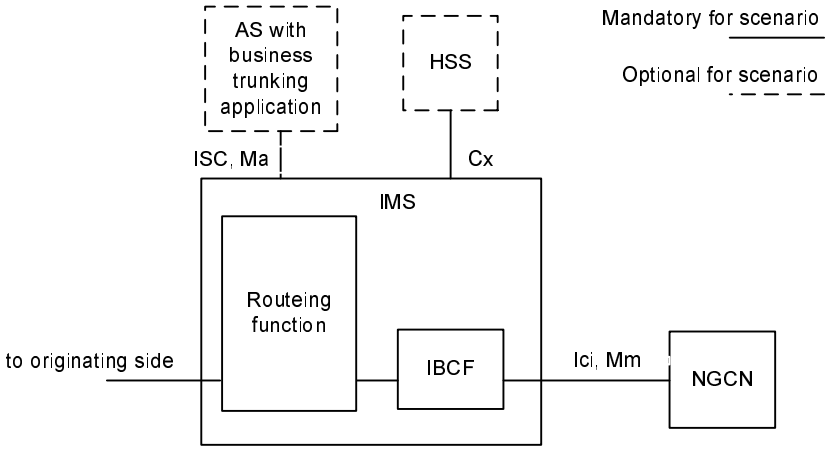

Figure 5.2: Terminating Side with AS and HSS

If business trunking applications are to be provided to the destination NGCN, the CSCF routeing capabilities of the routeing function invoke the AS based on the related NGCN specific data in the HSS.

5.3.2 Used functional entities at the service layer

The main functional entities from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise peering-based business trunking arrangements are as follows:

- routeing function;
- IBCF;
- if business applications are to be provided (e.g. those defined in subclause 4.4 of 3GPP TS 22.519 [1]): HSS containing NGCN specific data; and
- if business applications are to be provided (e.g. those defined in subclause 4.4 of 3GPP TS 22.519 [1]): AS.

The routeing function represents the routeing capabilities available in IMS entities. In basic scenarios the routeing capabilities of the Transit Function defined in 3GPP TS 23.228 [17], subclause 5.19 are sufficient while in more

advanced scenarios where Application Servers have to be involved to provide enhanced functionality, the routeing capabilities of one or more CSCF are required.

On the originating side the IBCF is capable of indicating whether an incoming SIP request is to be handled as an originating request by subsequent nodes in the IMS (see 3GPP TS 23.228 [17], subclause 4.14).

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, e.g. BGCF, are not listed.

A description of specific procedures executed to provide peering-based business trunking can be found in subclause 6.2.

5.3.3 Used reference points at the service layer

The main reference points from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise peering-based business trunking arrangements are as follows:

- e2;
- Gq';
- Ici or Mm;

NOTE 1: If the NGCN network appears as another IMS then Ici applies. Otherwise Mm applies.

NOTE 2: If Ici applies then there may be an inconsistency between 3GPP TS 29.165 [35] and ETSI TR 183 069 (Implementors guide for NGCN) [34].

- Mx;
- Cx (in case business trunking applications are to be provided);
- Sh (in case business trunking applications are to be provided); and
- ISC or Ma (in case business trunking applications are to be provided).

NOTE 3: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.3.4 Used functional entities at the transport layer

The main functional entities from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise peering-based business trunking arrangements are as follows:

- BGF (whether an I-BGF or a C-BGF performs this function requires further study).

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, are not listed.

5.3.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise peering-based business trunking arrangements are as follows:

- none identified.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.4 Session-level virtual leased line

5.4.1 General

This describes the architectural requirements for the connection of an NGCN site to the NGN using the IBCF as an entry point at the service layer and where only leased line type capabilities are provided.

Subclause 7.1 of 3GPP TS 24.523 [7] shows the arrangement of the involved functional entities.

5.4.2 Used functional entities at the service layer

The main functional entities from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise session-level virtual leased line arrangements are as follows:

- routeing function; and
- IBCF.

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, e.g. I-CSCF, are not listed.

A description of specific procedures executed to provide session-level virtual leased line can be found in subclause 6.3.

5.4.3 Used reference points at the service layer

The main reference points from the IMS service layer as specified in ETSI ES 282 007 [4] that are used to realise session-level virtual leased line arrangements are as follows:

- Mx;
- Ici or Mm;

NOTE 1: If the NGCN network appears as another IMS then Ici applies. Otherwise Mm applies.

NOTE 2: If Ici applies then there may be an inconsistency between 3GPP TS 29.165 [35] and ETSI TR 183 069 (Implementors guide for NGCN) [34].

- e2; and
- Gq'.

5.4.4 Used functional entities at the transport layer

The main functional entities from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise session-level leased line arrangements are as follows:

- BGF (whether an I-BGF or a C-BGF performs this function requires further study).

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, are not listed.

5.4.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise session-level virtual leased line arrangements are as follows:

- none identified.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.5 Support for roaming NGCN user

5.5.1 General

This describes the architectural requirements for the connection of an NGCN site to the IMS using to allow NGCN users to roam into that IMS.

Subclause 9.1 of 3GPP TS 24.523 [7] shows the arrangement of the involved functional entities.

5.5.2 Used functional entities at the service layer

A list of the main functional entities from the IMS service layer as specified in ES 282 007 [4] used to realise roaming for NGCN users in NGN:

- P-CSCF; and
- IBCF.

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, e.g. I-CSCF, are not listed.

A description of specific procedures executed to provide NGCN user roaming into NGN can be found in subclause 6.4.

5.5.3 Used reference points at the service layer

A list of the main reference points from the IMS service layer as specified in ETSI ES 282 007 [4] used to realise roaming for NGCN users in NGN:

- Gm;
- Mx;
- e2; and
- Gq'.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.5.4 Used functional entities at the transport layer

The main functional entities from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise NGCN user roaming in NGN arrangements are as follows:

- BGF (whether an I-BGF or a C-BGF performs this function requires further study).

NOTE: The above list includes only those entities where specific functionality is applied to realise business communication in this scenario. Entities which otherwise transport, but apply no special processing, are not listed.

5.5.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in ETSI ES 282 007 [4] that are used to realise NGCN user roaming in NGN arrangements are as follows:

- none identified.

NOTE: The above list includes only those interfaces where specific protocol is applied to realise business communication in this scenario.

5.6 Support for roaming NGN user

Not applicable.

6 Procedures

6.1 Subscription based business trunking

6.1.1 Introduction

In addition to the procedures specified in the subclause 6.1, the NGCN site shall comply with the requirements identified in 3GPP TS 24.229 [18], subclause 4.1 for a UE, and specifically for a UE performing the functions of an external attached network.

In addition to the procedures specified in the subclause 6.1, all functional IMS entities shall support the procedures appropriate for these entities specified in 3GPP TS 24.229 [18] and in 3GPP TS 24.628 [10].

6.1.2 Identification

Each NGCN site is allocated a pair of private and public user identities. This public user identity is also known as the NGCN site identifier; this public user identity has to be a valid corporate network user identifier.

NGCN user identifiers are owned and managed by the enterprise. NGCN user identifiers are not stored in the HSS.

To be able to support routeing to NGCN users registered in an NGCN, through the connection with a specific NGCN site, an NGN shall support implicit registration of one or more wildcarded public user identities in addition to the implicit registration of one or more distinct public user identities. The implicitly registered identities associated with the registration of a particular NGCN site shall be determined by agreement between the NGCN and NGN.

NOTE: The wildcarded public user identity consists of a delimited regular expression located in the telephone-subscriber portion of a tel URI (e.g. tel: +3314529! [0-9]{4}!) or in the user portion of a SIP URI (e.g. sip:!.*!@example.com). The wildcarded public user identity is configured in the HSS as part of the implicit registration set of the subscription for a corporate network identifier.

A specific public user identifier is referred to as an NGCN user identifier if it matches a distinct public user identifier or a wildcarded public user identifier that is contained in the implicit registration set associated with an NGCN site identifier.

The NGN shall support implicit registration of NGCN user identifiers (specific or wildcarded) where the domain belongs to an enterprise.

For the purpose of processing incoming and outgoing calls the identity of each NGCN user behind an NGCN site is handled as a distinct public user identity possibly within a public user identity range or subdomain.

6.1.3 Registration

Registration of the NGCN site in the IMS is required. Registration shall rely on standard registration procedures for the IM CN subsystem, based on the pair of private user identity and public user identity representing the NGCN site as a whole.

NOTE 1: For NGCN sites that do not support IMS registration procedure, approaches like surrogate registration or configuration can be used as a fallback. The details of such approaches are out of scope of the present document.

Upon successful registration an implicit registration set conforming to the requirements of subclause 6.1.2, will be provided from the HSS to the S-CSCF, the P-CSCF and the UE representing the NGCN site.

As part of the successful registration a security association as required by the access security requirements in 3GPP TS 33.203 [16] will be established between the NGCN site and the P-CSCF that the NGCN site used for registration. This security association is used to secure the signalling between the P-CSCF and the NGCN site. Also as the security association is formed based on mutual authentication of the NGCN site and the NGN, requests that the P-CSCF receives over such a security association are known to come from that NGCN site and no other entity.

NOTE 2: Although the term "security association" is often used in relation with IP-sec, in the above paragraph this term is also assumed to apply to equivalent procedures in other security mechanisms as specified in the access security requirements of 3GPP TS 33.203 [16].

The NGN will need to be configured to understand the presence of an attached NGCN instead of a normal UE.

The NGN shall support provisioning of a special "loose route" indication in the user profile if the NGCN site requires loose routing procedures to be applied by the NGN. When available this indication is sent from the HSS to S-CSCF during registration as a result of performing the Cx Server Assignment procedure.

An NGCN site shall initiate initial registration when one of following events occurs:

- The NGCN site attachment point is powercycled.
- The NGCN site attachment point is allocated a new IP address.
- The IP address of the P-CSCF as reported by the DNS has changed and the NGCN site is registered through that P-CSCF.

NOTE 3: The above criteria are applicable for registration through a single P-CSCF and registration through multiple P-CSCFs.

- No response is received to a keep-alive request and the NGCN site is registered through a single P-CSCF.
- An initial request fails due to a transport failure of some sort (generally, due to fatal ICMP errors in UDP or connection failures in TCP), the transaction layer times out without ever having received any response, provisional or final (i.e. timer B or timer F in IETF RFC 3261 [21] fires) and the NGCN site is registered through a single P-CSCF.

NOTE 4: The case where the NGCN site has registered an AOR through multiple P-CSCF instances is addressed in subclause 6.1.5.

6.1.4 Requests originating from an NGCN user entering NGN

6.1.4.1 General

The procedures for handling of requests from an NGCN especially applying to identities are very different depending on whether or not the NGCN is part of the same trust domain for asserted identities as the NGN, and if not, whether the NGCN is considered as privileged sender or not. To highlight those differences, three separate clauses below describe the procedure for:

- an NGCN not considered as privileged sender and not trusted by NGN;
- an NGCN considered as privileged sender and trusted by NGN; and
- an NGCN considered as privileged sender and not trusted by NGN.

Trust domain for asserted identity is defined in IETF RFC 3324 [22]. To be meaningful in a particular domain it requires the definition of a Spec(T) that specifies the requirements that all entities in the trust domain need to comply with. The Spec(T) to be used should be covered in the SLA.

INVITE requests sent by an NGCN site may include a P-Early-Media header with the "supported" parameter.

In the event of the P-Early-Media header not being present in an 18x message and a media flow being received, such a media flow is not forwarded in most cases. However, under these circumstances, an NGCN site may, as an NGCN option, forward the received media flow to the end-user and disable any locally generated call progress tones.

NOTE: This behaviour enables managing the case when the NGCN site and/or the remote entity generating early media do not support the P-Early-Media header.

The To header field may contain any URI format. The Request-URI shall be in a format supported by the NGN for the request to be accepted. 3GPP TS 24.229 [18], subclause 5.1.2A.1.2 gives information on the format of the Request-URI.

In an outgoing request initiating a dialog or in a target refresh request the Contact 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.

As an NGCN site may comprise multiple SIP entities, the Record-Route header field may be populated by entities within the NGCN site in a dialog initiating request sent to the NGN.

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

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

6.1.4.2 NGCN not considered as privileged sender and not trusted by NGN

For a request originated in an untrusted NGCN and entering the NGN over the Gm reference point, network policy or a setting in the IMS subscription for the NGCN site determines whether the procedures specified in 3GPP TS 24.229 [18] for a privileged sender apply or not.

When the request needs to be presented as originated from a particular NGCN user identified by an NGCN user identifier, the NGCN site can provide the NGCN user identifier in the P-Preferred-Identity header field.

NOTE 1: If the P-Preferred-Identity or P-Asserted-Identity header fields are not supplied by the NGCN site, the NGCN user identifier can be provided in the From header field.

As aliases are not managed by the NGN, it is up to the NGCN site to provide two P-Preferred-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 3GPP TS 22.519 [1]).

If no identity is presented by the NGCN in a P-Preferred-Identity header field, then the P-CSCF will provide a default identity in the P-Asserted-Identity header field. This identity is the first on the list of URIs present in the P-Associated-URI header field received as part of the registration procedure. It shall exist in the HSS by agreement between the NGCN and NGN operator, and shall identify an NGCN user who operates with the authority of the NGCN operator (e.g. an attendant).

If the identity is provided in a P-Preferred-Identity header field the P-CSCF checks whether this identity is part of the implicit registration set and if so the P-Preferred-Identity header field will be removed and its value copied into the P-Asserted-Identity header field that will be used within the NGN. When this identity is not part of the implicit registration set, a present P-Preferred-Identity header field will be removed and the P-CSCF will provide a default identity in the P-Asserted-Identity header field and if the NGCN site is considered a privileged sender in the P-Served-User header field. The default identity is the first identity on the list of URIs present in the P-Associated-URI header field received as part of the registration procedure.

A P-Asserted-Identity header field will be discarded if received, as specified in 3GPP TS 24.229 [18], subclause 5.2.6.3.3.

When the S-CSCF receives the request it finds a match between the P-Asserted-Identity header field and the distinct or wildcarded public user identities as in the implicit registration set of the NGCN site's profile. This allows the S-CSCF to perform its actions based on the service profile of the NGCN site; this includes the optional link in of an AS over ISC, for example to provide additional services to the enterprise.

NOTE 2: The above procedures do not preclude that the NGN may host a service on behalf of the NGCN that may perform further translations on the P-Asserted-Identity header field. For example in order to cope with NGCN sites that do not deliver the NGCN user identifier in a P-Preferred-Identity header field or a P-Asserted-Identity header field, an AS playing the role of a business trunking application on the originating side can decide to override the P-Asserted-Identity header field with the contents of the From header field, if consistent with the range of identities assigned to the NGCN or NGCN site and with the policy agreed between the NGN operator and the enterprise. If the From header field contained a SIP URI, the AS can also include a second P-Asserted-Identity header field with a TEL URI if possible. This enables the NGCN user identifier to be sent to the destination in the form of an asserted identity.

If the Privacy header field with value "id" is received in a request from the NGCN site, the P-CSCF retains the header field when passing on the request.

The NGCN site may receive a connected party identity that is not privacy-restricted in the P-Asserted-Identity header field in an 18x or 2xx final response depending on NGN policy.

6.1.4.3 NGCN considered as privileged sender and trusted by NGN

For a request originated in a trusted NGCN and entering the NGN over the Gm reference point, the procedures specified in 3GPP TS 24.229 [18] for a privileged sender apply.

When the request needs to be presented as originated from a particular NGCN user, the NGCN site can provide the NGCN user identifier in the P-Preferred-Identity header field or in the P-Asserted-Identity header field.

As aliases are not managed by the NGN, it is up to the NGCN site to provide two 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 3GPP TS 22.519 [1]).

When a P-Preferred-Identity header field is received and is part of the implicit registration set, the P-Served-User header field is set to the P-Preferred-Identity header field.

When no P-Preferred-Identity header field is received or when a received P-Preferred-Identity header field is not part of the implicit registration set, the P-CSCF includes a P-Served-User header field set to the default identity received in the P-Associated-URI header field during registration.

If one or two P-Asserted-Identity header field(s) are received from the NGCN site, the P-CSCF passes them on unchanged.

If no P-Asserted-Identity header field is received the P-CSCF includes a P-Asserted-Identity header field with a value copied from the P-Served-User header field.

If the Privacy header field with value "id" is received in a request from the NGCN site, the P-CSCF retains the header field when passing on the request.

NOTE: The above procedures do not preclude that the NGN may host a service on behalf of the NGCN that may perform further translations on the P-Asserted-Identity header field. For example in order to cope with NGCN sites that do not deliver the NGCN user identifier in a P-Preferred-Identity header field or P-Asserted-Identity header field, an AS playing the role of a business trunking application on the originating side can decide to override the P-Asserted-Identity header field with the contents of the From header field, if consistent with the range of identities assigned to the NGCN or NGCN site and with the policy agreed between the NGN operator and the enterprise. If the From header field contained a SIP URI, the AS can also include a second
P-Asserted-Identity header field with a TEL URI if possible. This enables the NGCN user identifier to be sent to the destination in the form of an asserted identity.

The NGCN site may receive a connected party identity in the P-Asserted-Identity header field in an 18x or 2xx final response. The identity will be accompanied by a Privacy header field set to "id" if its presentation is restricted.

6.1.4.4 NGCN considered as privileged sender and not trusted by NGN

If the NGCN site is considered as privileged sender the procedures of subclause 6.1.4.3 for the handling of requests shall apply. This means that the P-CSCF will pass on a P-Asserted-Identity header field unchanged if received in a request from the NGCN site. The NGCN site profile shall contain appropriate filter criteria to ensure that the identity in the
P-Asserted-Identity header field will be verified by an Application Server.

The NGCN site may receive a connected party identity that is not privacy-restricted in the P-Asserted-Identity header field in an 18x or 2xx final response depending on NGN policy.

6.1.5 Requests terminating to an NGCN user leaving NGN

6.1.5.1 General

The procedures for handling of requests to and responses from an NGCN especially applying to identities are very different depending on whether the NGCN is part of the same trust domain for asserted identities as the NGN or not. To highlight those differences three separate clauses below describe the procedure for:

- an NGCN not considered as privileged sender and not trusted by NGN;
- an NGCN considered as privileged sender and trusted by NGN; and

- an NGCN considered as privileged sender and not trusted by NGN.

Trust domain for asserted identity is defined in IETF RFC 3324 [22]. To be meaningful in a particular domain it requires the definition of a Spec(T) that specifies the requirements that all entities in the trust domain need to comply with. The Spec(T) to be used should be covered in the SLA.

When an initial request for a new dialog or a request for a standalone transaction addressed to an NGCN site identifier or an NGCN user identifier in the Request-URI arrives at the I-CSCF, the I-CSCF performs a location request to HSS to locate the S-CSCF where to forward the request to. The HSS finds a match between the Request-URI and the registered NGCN site identifier or an implicitly registered distinct or wildcarded public user identity that belongs to the service profile of an NGCN site. The HSS returns information about a particular S-CSCF allocated to that specific NGCN site service profile.

When the S-CSCF receives the request it finds a match between the Request-URI and the NGCN site identifier or the distinct or wildcarded public user identity as in the implicit registration set of the NGCN site service profile. This allows the S-CSCF to perform its actions based on the service profile for the NGCN site. This includes the optional link of AS over ISC, for example to provide additional services to an enterprise. When the S-CSCF is ready to forward the request to the NGCN via the P-CSCF and a "loose-route" indication has been received from the HSS during registration (see subclause 6.1.3), it retains the received NGCN user identifier (including any URI parameters) in the Request-URI, then it adds to the Route header field the contents of the Path header field as stored during registration as well as the registered Contact address. This will ensure that the request is first routed to the P-CSCF assigned during registration and that the P-CSCF can forward the request over the Gm reference point towards the NGCN site. The NGCN site can then use the Request-URI to forward the request further in the NGCN or it can use it to select an extension to forward the call to.

The above procedure assumes specific population rules applicable when a special indication stored in the user profile is received from the HSS. In such cases, the S-CSCF retains the received target identity in the Request-URI and, if the NGCN site has not registered using IETF RFC 5626 [29], adds the Contact address (stripping out the Display name field if any) to the Route header field (as the last field value). If the NGCN site has not registered using IETF RFC 5626 [29], after removing its own address, the P-CSCF uses the topmost Route header field (which happens to be the Contact address) to identify the security association (or equivalent in case no security association was established) and route the request according to IETF RFC 3261 [21]. If the NGCN site has registered using IETF RFC 5626 [29] the P-CSCF will use the procedures defined in IETF RFC 5626 [29] to forward the request over the Gm reference point towards the NGCN site.

NGCN sites that have implicitly registered a TEL URI are required to accept a Request-URI in the form of a TEL URI when the loose route indicator is set in their network profile.

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 1: The non-loose-route procedure may not be adequate for NGCN URIs that are not within the range of identities assigned to the NGCN site, e.g. private GRUUs. This issue requires further study.

In a 2xx final response to an incoming dialog initiating or target refresh request the Contact 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.

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

NOTE 2: The Max-Breadth header field may be passed on to the NGN, e.g. if the call is diverted back into the NGN. 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.

As an NGCN site may comprise multiple SIP entities, the Record-Route header field may have been populated by entities within the NGCN site in a response to a dialog initiating request received from the NGN.

When received by the NGCN attachment point in a request from the NGN, the Record-Route header field has to be passed on by the attachment point and the attachment point can also add its own Record-Route header field.

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

NOTE 3: 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.

6.1.5.2 NGCN not considered as privileged sender and not trusted by NGN

For a request terminated in an untrusted NGCN and leaving the NGN over the Gm reference point, network policy or a setting in the IMS Subscription for the NGCN site determines whether the procedures specified in 3GPP TS 24.229 [18] for a privileged sender apply or not.

The NGCN site may receive a calling party identity that is not privacy-restricted in the P-Asserted-Identity header field in a request from the NGN, depending on NGN policy.

If the Privacy header field with value "id" is received in a response, the P-CSCF retains it when passing on the response.

For a response originating in the NGCN the P-CSCF provides the saved public user identity from the P-Called-Party-ID header field that was received in the request, plus the display name if previously stored during registration for the NGCN site (see subclause 6.1.4.1) in the P-Asserted-Identity header field. The S-CSCF will add a second P-Asserted-Identity header field if possible.

6.1.5.3 NGCN considered as privileged sender and trusted by NGN

For a request terminated in a trusted NGCN and leaving the NGN over the Gm reference point, the procedures specified in 3GPP TS 24.229 [18] for a privileged sender apply.

The NGCN site may receive a calling party identity in the P-Asserted-Identity header field in a request from the NGN. The identity will be accompanied by a Privacy header field set to "id" if its presentation is restricted.

If a P-Asserted-Identity header field is present in the response from the NGCN, the P-CSCF shall retain this identity when passing on the response. As aliases are not managed by the NGN, it is up to the NGCN site to 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 3GPP TS 22.519 [1]).

NOTE: If there is no P-Asserted-Identity header field in the response, the P-CSCF will not add one.

If the Privacy header field with value "id" is received in a response, the P-CSCF retains it when passing on the response.

6.1.5.4 NGCN considered as privileged sender and not trusted by NGN

The NGCN site may receive a calling party identity that is not privacy-restricted in the P-Asserted-Identity header field in a request from the NGN, depending on NGN policy.

Subclause 6.1.5.3 for the handling of responses shall apply. This means that the P-CSCF will pass on a P-Asserted-Identity header field unchanged if received in a response from the NGCN site. The NGCN site profile shall contain appropriate filter criteria to ensure that an Application Server will be included in the path of a dialog initiating or stand-alone request in order to verify the identity in the P-Asserted-Identity header field in the response.

6.1.6 Business trunking applications

6.1.6.1 General

Business trunking applications are deployed on an AS. In case such services are offered to a specific enterprise the initial filter criteria of the service profile of a connected NGCN site needs to be configured so that the S-CSCF that serves the NGCN site invokes the AS that hosts the business trunking application.

The intent of this clause is not to specify the detail of the individual applications, but only to indicate some specific impacts on the protocol.

3GPP TS 22.519 [1] defines the business trunking application, this clause specifies protocol impact of the different applications.

6.1.6.2 Routeing capabilities

6.1.6.2.1 Overview

Not applicable.

6.1.6.2.2 Break-in

When break-in service is enabled for a specific NGCN site, a business trunking application converts incoming public network traffic to private network traffic if the conditions agreed between the enterprise and the NGN operator indicate this.

To convert public network traffic to private network traffic the break-in service shall insert a P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] with a private network identifier as expressed in the SLA between the enterprise and the NGN operator, in the initial request for a dialog or standalone request for a transaction.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions originating from and terminating to the served NGCN site.

6.1.6.2.3 Break-out

When break-out is enabled for a specific NGCN site, a business trunking application converts outgoing private network traffic to public network traffic if the conditions agreed between the enterprise and the NGN operator indicate this.

To convert private network traffic to public network traffic the break-out service shall remove P-Private-Network-Indication header field as specified in IETF RFC 7316 [31], from the initial request for a dialog or standalone request for a transaction.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions originating from and terminating to the served NGCN site.

6.1.6.2.4 Bulk rerouting

When bulk rerouting is enabled for a specific NGCN site, a terminating business trunking application forwards incoming public or private network traffic to a specified destination if the conditions agreed between the enterprise and the NGN operator indicate this.

The NGN operator defines the set of rules or policies under which this should occur, and the NGCN operator should be able to configure the capability within those rules and policies.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions terminating to the served NGCN site.

6.1.6.3 Communication admission control

When communication admission control is enabled a business trunking application serving an NGCN site executes the NGN operator defined set of rules or policies under which communication admission control applies, and the NGCN operator should be able to configure the capability within those rules and policies.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions originating from and terminating to the served NGCN site.

6.1.6.4 Anonymous communication rejection

When anonymous communication rejection is enabled a terminating business trunking application serving an NGCN site providing this service shall implement the procedure as specified in 3GPP TS 24.611 [8], subclause 4.5.2.6.2.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions terminating to the served NGCN site.

6.1.6.5 Communication barring

When communication barring is enabled, a terminating business trunking application shall reject incoming calls when the evaluation of the NGCN site specific incoming communication barring rules indicates so. The definition of the communication barring rules is out of scope of the present document.

When the communication barring application rejects a communication, it shall do so by implementing the protocol procedure for rejecting a communication as specified in 3GPP TS 24.611 [8], subclause 4.5.2.6.1, excluding the communication barring rule aspect of that procedure.

To allow this service to be provided it needs to be ensured that the business trunking application offering this service will be inserted in the signalling path of sessions terminating to the served NGCN site.

6.1.7 Signalling transparency

For private network traffic, an NGN shall be capable of transparent exchange of signalling elements that an IETF RFC 3261 [21] SIP proxy is not allowed to add, remove or modify, subject to the exception listed below, and shall be capable of being tolerant of and passing on without modification any signalling extension that is not supported. The exception is any information that needs to be changed to accomplish NAT traversal, i.e. IP addresses and ports in SDP. In particular, an NGN shall be capable of passing on a request, part of which is cryptographically signed (e.g. using the Identity header field), without removing or invalidating that signature. Whether such transparency is provided and to what degree is a matter for agreement between the NGN operator(s) and enterprise(s) concerned. This applies to any functional entity on the signalling path, including P-CSCF, S-CSCF, IBCF and AS.

NOTE: This is not intended to prevent intervention by an AS when needed to carry out specific services as agreed between operators or as negotiated by signalling.

6.1.8 Involvement of functions on the media path

6.1.8.1 General

For private network traffic, entities on the signalling path shall be capable of avoiding the insertion of functions into the media path that intervene above the transport layer, unless explicitly required by contractual arrangement between the NGN operator and the NGCN operator, explicitly requested through signalling, or in order to meet regulatory requirements. Examples of intervention that is prohibited (when exceptions do not apply) include transcoding, language translation, recording, re-encrypting and re-signing.

6.1.8.2 DTMF

As specified in 3GPP TS 24.229 [18], 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 IETF RFC 4733 [26].

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.

6.1.8.3 Codecs

ETSI TS 181 005 [27] specifies principles for the use of codecs in the NGN. Specifically ETSI TS 181 005 [27] 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 ETSI TS 181 005 [27], 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 [28] coded speech with a packetization size of 20 ms.

6.1.9 Handling of the P-Access-Network-Info header field

When a request or response received using an xDSL-based access the P-CSCF inserts a P-Access-Network-Info header field into the forwarded request or response by setting the access-type field to one of the values specified in 3GPP TS 24.229 [18] for this type of access. The P-CSCF adds the "network-provided" parameter and the "dsl-location" parameter with the value received in the Location-Information header in the User-Data Answer command as specified in ETSI ES 283 035 [11] or with a provisioned value if a static IP address is used and no interface to the NASS exist.

When a request or response received using an LAN-based access the P-CSCF inserts a P-Access-Network-Info header field into the forwarded request or response by setting the access-type field to "ETH", adding the "network-provided" parameter and the "eth-location" parameter with the value received in the Location-Information header in the User-Data Answer command as specified in ETSI ES 283 035 [11] or with a provisioned value if a static IP address is used and no interface to the NASS exist.

6.1.10 Emergency calls

The NGCN site will normally identify an emergency call as an emergency call and ensure that it is received in the NGN with a Request-URI set to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in IETF RFC 5031 [24]. An additional sub-service type can be added if information on the type of emergency service is known.

The P-CSCF will handle requests identified as emergency calls and which are public network traffic in the same fashion as calls from UEs not using business communication procedures.

For requests identified as private network traffic, the P-CSCF can handle such requests according to normal routeing procedures for requests, and not follow the procedures of clause 5.2.10 of 3GPP TS 24.229 [18], or handle the request as if it was public network traffic.

NOTE 1: Such emergency calls are handled within some other NGCN site, which can either provide the emergency service routeing proxy, or the emergency answer point. Further study is required for what policy applies in selecting the one of the above options, and whether this choice is applicable to all or some identification of emergency calls.

An NGCN site will normally provide a geolocation in conjunction with such calls, using the procedures of IETF RFC 6442 [30]. The P-CSCF can also provide location information in the P-Access-Network-Info header field. Which of these two information is used by the E-CSCF to select a PSAP depends on the policy of the NGN operator and the regulatory constraints in force.

NOTE 2: The location information available in the P-Access-Network-Info header field when provided by the NGN usually represents the location of the access point where the NGCN site is connected to the NGN, and not the terminal attached to the NGCN.

The presence of the private network indication can modify the emergency call handling at the P-CSCF. This is necessary if emergency calls relating to private network traffic are to be routed to a separate PSAP (a "private PSAP"), to the PSAP used for emergency calls relating to public network traffic.

6.1.11 Charging

The applicable charging procedures are defined in 3GPP TS 32.260 [6].

6.1.12 Advice of Charge

An NGCN site supporting advice of charge services shall support the INFO method and shall accept MIME bodies of type "application/vnd.etsi.aoc+xml" defined in 3GPP TS 24.647 [12].

If the agreement between the NGN and the NGCN specifies that an NGCN site shall received advice of charge information, the NGCN site profile in the HSS shall contain appropriate initial filter criteria ensuring that an Application Server supporting the procedures described in 3GPP TS 24.647 [12] is inserted in the signalling path of outgoing sessions.

When processing originating sessions, this application server shall be able to act as a Charging Generation Point (CGP) with regards to the NGCN site and may take into account charging information received from upstream in the format defined in 3GPP TS 29.658 [13], annex C.

6.1.13 NAT traversal

NOTE 1: 3GPP TS 24.229 [18], annexes F and K specify mechanisms for NAT traversal. The application of these mechanisms is not precluded, but detailed implications of their use in a business communication environment have not been studied.

Two solutions to keep a connection alive, depending on the NAT traversal mechanism (Latching-based as defined in 3GPP TS 24.229 [18], annex F or SIP Outbound-based as defined in 3GPP TS 24.229 [18]) used, are provided in 3GPP TS 24.229 [18].

When using the latching-based NAT traversal mechanism, as defined in 3GPP TS 24.229 [18], subclause F.4.2 provides two solutions for keeping the signalling connection alive:

- short registration timers (see note 1 in 3GPP TS 24.229 [18], subclause F.4.2); and

- SIP outbound keep-alive as a stand-alone mechanism (see note 2 in 3GPP TS 24.229 [18], subclause F.4.2).

When using SIP outbound, as specified in 3GPP TS 24.229 [18], the SIP-outbound keep-alive mechanism applies.

NOTE 2: Use of alternative mechanisms (e.g. OPTIONS method) is outside the scope of the present document.

6.1.14 Private network traffic

Private network traffic can be distinguished from public network traffic by the addition of a P-Private-Network-Indication header field as specified in IETF RFC 7316 [31].

NOTE: Procedures for use of the P-Private-Network-Indication header field within the NGN are specified in 3GPP TS 24.229 [18]. Where an explicit indication of private network traffic is required within the NGN, then the P-Private-Network-Indication header field is expected to be used.

The NGN will handle the P-Private-Network-Indication header field in accordance with its trust domain specification.

The NGCN site can include a P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] in an initial request or standalone request, with a valid private network identification for its use.

The NGN can include a P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] in an initial request or standalone request to the NGCN site, with a valid private network identification for its use.

For transactions relating to private network traffic, the NGCN site may include and receive tel URIs (and their SIP equivalents) specifying Private Numbering Plan (PNP) numbers in accordance with ETSI TR 102 634 [20].

6.1.15 P-CSCF and IP-CAN redundancy

3GPP TS 24.229 [18], clause 9 describes several methods enabling a UE to obtain a list of IP addresses or the SIP server domain name of the P-CSCF. The addressing material acquired through these methods should be used to build a SIP URI corresponding to the P-CSCF. Once the SIP URI of the P-CSCF is obtained, IETF RFC 3263 [25] procedures as specified in 3GPP TS 24.229 [18], subclause E.2.2.1 should 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.

An NGCN site may decide to perform multiple registrations for the same Address of Records through different P-CSCFs or from different local network interfaces attached to different IP-CANs. In this case, as specified in 3GPP TS 24.229 [18], subclause 5.1.1.2.1, the following settings apply to the REGISTER request header fields:

1) the Contact header field shall include a "+sip.instance" header field parameter containing the instance ID associated to the NGCN site and a "reg-id" header field parameter as described in IETF RFC 5626 [29]; and

2) the "outbound" option-tag shall be included in the Supported header field.

As specified in 3GPP TS 24.229 [18], subclause 5.1.2A.1.1, the NGCN site shall then include an "ob" SIP URI parameter in the Contact header field of the initial request, except REGISTER.

A load distribution or a load balancing strategy can be applied when sending an initial request to the NGN. The load distribution strategy can use a round-robin algorithm. A load balancing strategy can make use of the actual load of the P-CSCFs if this information is made available by the DNS.

If for an AOR multiple registrations through different P-CSCF instances according to IETF RFC 5626 [29] are performed and an initial request except REGISTER, fails as specified in IETF RFC 3263 [25], subclause 4.3 or if the P-CSCF does not respond to keep alive messages, the NGCN site can attempt to send that request to another P-CSCF where it is registered.

NOTE: Load balancing or load distribution for terminating request across multiple P-CSCFs as specified in 3GPP TS 24.229 [18], subclause 6.1 can be achieved by applying appropriate policies at the S-CSCF when multiple registrations exist. These policies are implementation specific.

6.2 Peering-based business trunking

6.2.1 Introduction

The NGCN site shall appear to the NGN as if it were an IBCF complying with the requirements identified in 3GPP TS 24.229 [18], subclause 4.1 for this functional entity.

In addition to the procedures specified in the subclause 6.2, all functional IMS entities shall support the procedures appropriate for these entities specified in 3GPP TS 24.229 [18] and in 3GPP TS 24.628 [10].

6.2.2 Identification

Each NGCN site is responsible for a set of public user identities.

6.2.3 Registration

There is no registration of NGCN sites in the IMS.

NOTE: Terminating requests are routed over the final NGN entity to the NGCN site by using standard DNS techniques, which apply to the remainder of the routeing.

6.2.4 Requests originating from an NGCN user entering NGN

6.2.4.1 General

The procedures for handling of requests to or from an NGCN especially applying to identities are very different depending on whether the NGCN is part of the same trust domain for asserted identities as the NGN or not. To highlight those differences two separate clauses describe the procedure for:

- an NGCN not trusted by NGN; and
- an NGCN trusted by NGN.

Trust domain for asserted identity is defined in IETF RFC 3324 [22]. To be meaningful in a particular domain it requires the definition of a Spec(T) that specifies the requirements that all entities in the trust domain need to comply with. The Spec(T) to be used should be covered in the SLA.

A request will be identified in the IBCF as coming from an NGCN site relating to a particular enterprise by means of appropriate security associations required by the network domain security requirements specified in 3GPP TS 33.203 [16].

In case no business trunking applications are provided, the "intelligent routeing function" as defined in subclause 5.3.1 just offers originating transit functionality in the NGCN originating case (figure 5.1).

Depending on the agreements between NGN an NGCN, originating business trunking applications are to be provided to the NGCN (e.g. those specified in 3GPP TS 22.519 [1]). In this case an AS needs to be invoked by the intelligent routeing function to perform the originating business trunking application, which may be realised by the IBCF forcing the CSCF routeing capabilities to treat the NGCN originated request as an originating request, reacting on enterprise specific data of the originating NGCN in the HSS.

NOTE: 3GPP TS 23.228 [17] defines in subclause 14.4 the capability of an IBCF to indicate whether an incoming SIP request is to be handled as an originating request by subsequent nodes in the IMS (e.g. by inserting the "orig" parameter, defined in 3GPP TS 24.229 [18], subclause 7.2A.6 and intended to tell the S-CSCF that it has to perform the originating services instead of terminating services and to tell the I-CSCF that it has to perform originating procedures).

6.2.4.2 NGCN not trusted by NGN

For a request originated in an untrusted NGCN, when the request needs to be presented as originated from a particular NGCN user identified by an NGCN user identifier, any identity provided by the NGCN site in the P-Preferred-Identity header field or in the P-Asserted-Identity header field is removed.

The IBCF will provide a default identity in the P-Asserted-Identity header field. This identity is configured in the IBCF, and shall identify a NGCN user who operates with the authority of the NGCN operator (e.g. an attendant).

Depending on NGN policy, the IBCF may send to the NGCN site a connected party identity that is not privacy-restricted, included in the P-Asserted-Identity header field of a 18x or 2xx final response.

If the Privacy header field with value "id" is received in a request from or a response to the NGCN site, the IBCF retains it when passing on the request or response.

6.2.4.3 NGCN trusted by NGN

If according to SLA the NGN and the NGCN form part of the same trust domain, the NGCN delivers the P-Asserted-Identity header field to the NGN. The NGN does not remove the P-Asserted-Identity header field in this case.

The IBCF may send to the NGCN site a connected party identity included in the P-Asserted-Identity header field of an 18x or 2xx final response.

If the Privacy header field with value "id" is received in a request from or a response to the NGCN site, the IBCF retains it when passing on the request.

6.2.5 Requests terminating to an NGCN user leaving NGN

6.2.5.1 General

The procedures for handling of requests to and responses from an NGCN especially applying to identities are very different depending on whether the NGCN is part of the same trust domain for asserted identities as the NGN or not. To highlight those differences two clauses describe the procedure for:

- an NGCN not trusted by NGN; and
- an NGCN trusted by NGN.

Trust domain for asserted identity is defined in IETF RFC 3324 [22]. To be meaningful in a particular domain it requires the definition of a Spec(T) that specifies the requirements that all entities in the trust domain need to comply with. The Spec(T) to be used should be covered in the SLA.

In case no business trunking applications are provided, the "intelligent routeing function" as defined in subclause 5.3.1 just offers basic and transparent routeing functionality in the NGCN terminating case (figure 5.2).

Depending on the agreements between NGN an NGCN, terminating business trunking applications are to be provided to the NGCN (e.g. those specified in 3GPP TS 22.519 [1]). In this case an AS needs to be invoked by the intelligent routeing function to perform the terminating business trunking application, which may be realised by the I-CSCF on basis of NGCN-specific data retrieved from the HSS.

6.2.5.2 NGCN not trusted by NGN

For a response originated in an untrusted NGCN, when the response needs to be presented as coming from a particular NGCN user identified by a NGCN user identifier, any identity provided by the NGCN site in the P-Preferred-Identity header field or in the P-Asserted-Identity header field is removed. The IBCF will provide a default identity in the P-Asserted-Identity header field. This identity is configured in the IBCF, and shall identify a NGCN user who operates with the authority of the NGCN operator (e.g. an attendant).

If the Privacy header field with value "id" is received in a request to or a response from the NGCN site, the IBCF retains it when passing on the request or response.

6.2.5.3 NGCN trusted by NGN

For a response originating in a trusted NGCN, if a P-Asserted-Identity header field is present in a response from the NGCN, the IBCF shall not remove this identity when passing on the response.

If the Privacy header field with value "id" is received in a request to or response from the NGCN site, the IBCF retains it when passing on the request or response.

6.2.6 Business trunking application

6.2.6.1 General

The provision of the business trunking applications (e.g. those defined in 3GPP TS 22.519 [1], clause 4.4) is realized by an intelligent routeing function, which may involve an AS depending on the actual enterprise specific data.

In the case no business trunking applications are provided, the "intelligent routeing function" as defined in subclause 5.3.1 just offers originating transit functionality in the NGCN originating case (figure 5.1). This originating case then corresponds to the second scenario of 3GPP TS 23.228 [17], subclause 5.19. In the terminating case the "intelligent routing function" just forwards requests to the appropriate IBCF.

The intent of this clause is not to specify the detail of the individual services, but only to indicate some specific impacts on the protocol.

6.2.6.2 Routeing related business trunking applications

6.2.6.2.0 General

For Break-in, Break-out and bulk rerouteing see subclause 6.1.6.2.

6.2.6.2.1 Originating requests

If the business trunking application receives an originating request from a NGCN, the business trunking application shall, based on the P-Served-User header field, identify the NGCN.

If the request contains a P-Asserted-Identity header field and does not contain a P-Private-Network-Indication header field, the business trunking application shall verify the P-Asserted-Identity header field against the profile of the NGCN. If the verification fails or if the request does not contain a P-Asserted-Identity header field, the business trunking application shall insert a P-Asserted-Identity header field identifying the main enterprise user. If the request contains a P-Private-Network-Indication header field, the business trunking application shall, if present, forward the received P-Asserted-Identity header field unchanged.

NOTE 1: The profile of the NGCN is provisioned in the business trunking application or in the subscription profile in HSS if this application uses the HSS for subscription storage.

NOTE 2 The profile of the NGCN can also be provisioned in the P-CSCF. In this case, the above procedures are already executed by the P-CSCF and need thus not be executed by the business trunking application anymore.

6.2.6.2.2 Terminating responses to an originating request

When the business trunking application receives a terminating response to the above request, if this response contains a P-Asserted-Identity header field and does not contain a P-Private-Network-Indication header field, the business trunking application shall verify the P-Asserted-Identity header field against the profile of the NGCN. If the verification fails or if the response does not contain a P-Asserted-Identity header field, the business trunking application shall insert a P-Asserted-Identity header field identifying the main enterprise user. If this response contains a P-Private-Network-Indication header field, the business trunking application shall, if present, forward the received P-Asserted-Identity header field unchanged.

NOTE 1: The profile of the NGCN is provisioned in the business trunking application or in the subscription profile in HSS if this application uses the HSS for subscription storage.

NOTE 2 The profile of the NGCN can also be provisioned in the P-CSCF. In this case, the above procedures will be executed by the P-CSCF and need thus not be executed by the business trunking application.

6.2.6.2.3 Terminating requests

If the business trunking application receives a terminating request to an NGCN, the business trunking application shall identify the particular NGCN the enterprise user belongs to, and also the P-CSCF(s) or IBCF(s), respectively serving the NGCN, and shall forward the request towards the NGCN. Therefore, the business trunking application shall create a route to the NGCN by adding a SIP URI of the P-CSCF or IBCF, respectively serving the NGCN and the NGCN in a Route header field as bottommost entries.

NOTE 1: The profile of the NGCN is provisioned in the business trunking application or in the subscription profile in the HSS if this application uses the HSS for subscription storage.

NOTE 2: Inserting the SIP URI of the NGCN in a Route header field will suppress triggering any other AS after the business trunking application. Hence this AS has to be last in the chain of iFCs.

Editor's note: [BusTI-CT, CR 0001] It is FFS whether in certain scenarios another AS needs to be the last AS to be triggered (e.g. the SCC AS) in order to allow all desired services.

6.2.6.3 Communication admission control

See subclause 6.1.6.3.

6.2.6.4 Anonymous communication rejection

See subclause 6.1.6.4.

6.2.6.5 Communication barring

See subclause 6.1.6.5.

6.2.7 Signalling transparency

For private network traffic, an NGN shall be capable of transparent exchange of signalling elements that an IETF RFC 3261 [21] SIP proxy is not allowed to add, remove or modify, subject to the exception listed below, and shall be capable of being tolerant of and passing on without modification any signalling extension that is not supported. The exception is any information that needs to be changed to accomplish NAT traversal, i.e. IP addresses and ports in SDP. In particular, an NGN shall be capable of passing on a request, part of which is cryptographically signed (e.g. using the Identity header field), without removing or invalidating that signature. Whether such transparency is provided and to what degree is a matter for agreement between the NGN operator(s) and enterprise(s) concerned. This applies to any functional entity on the signalling path, including IBCF and routeing function.

6.2.8 Involvement of functions on the media path

For private network traffic, entities on the signalling path shall be capable of avoiding the insertion of functions into the media path that intervene above the transport layer, unless explicitly required by contractual arrangement between the NGN operator and the NGCN operator, explicitly requested through signalling, or in order to meet regulatory requirements. Examples of intervention that is prohibited (when exceptions do not apply) include transcoding, language translation, recording, re-encrypting and re-signing.

6.2.9 Handling of the P-Access-Network-Info header field

The P-Access-Network-Info header field is not provided by an NGCN site in the peering-based approach to business trunking.

6.2.10 Emergency calls

The NGCN site will normally identify an emergency call as an emergency call and ensure that it is received in the NGN with a Request-URI set to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in IETF RFC 5031 [24]. An additional sub-service type can be added if information on the type of emergency service is known. Requests identified with this indication will be routed to an E-CSCF.

The IBCF will handle requests identified as emergency calls and which are public network traffic by routeing them to an E-CSCF.

NOTE 1: The above constitutes an extension to the IMS architecture which still needs to be studied as to its inclusion in the main IMS architecture documents.

For requests identified as private network traffic, the IBCF handles such requests according to normal routeing procedures for requests, or handle the request as if it was public network traffic.

NOTE 2: Such emergency calls are handled within some other NGCN site, which can either provide the emergency service routeing proxy, or the emergency answer point. Further study is required for what policy applies in selecting the one of the above options, and whether this choice is applicable to all or some identification of emergency calls, or handle the request as if it was public network traffic.

An NGCN site will normally provide a geolocation in conjunction with such calls, using the procedures of IETF RFC 6442 [30].

The presence of the private network indication can modify the emergency call handling at the IBCF. This is necessary if emergency calls relating to private network traffic are to be routed to a separate PSAP (a "private PSAP"), to the PSAP used for emergency calls relating to public network traffic.

6.2.11 Charging

NOTE: Not covered in this release of the present document.

6.2.12 Advice of Charge

NOTE: Not covered in this release of the present document.

6.2.13 NAT traversal

NOTE: The application of NAT traversal mechanisms is not precluded, but detailed implications of their use in a business communication environment have not been studied.

6.2.14 Private network traffic

Private network traffic can be distinguished from public network traffic by the addition of a P-Private-Network-Indication header field as specified in IETF RFC 7316 [31].

NOTE: Procedures for use of the P-Private-Network-Indication header field within the NGN are specified in 3GPP TS 24.229 [18]. Where an explicit indication of private network traffic is required within the NGN, then the P-Private-Network-Indication header field is expected to be used.

The NGN will handle the P-Private-Network-Indication header field in accordance with its trust domain specification.

The NGCN site can include P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] in an initial request or standalone request, with a valid private network identification for its use.

The NGN can include P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] in an initial request or standalone request to the NGCN site, with a valid private network identification for its use.

For transactions relating to private network traffic, the NGCN site may include and receive tel URIs (and their SIP equivalents) specifying PNP numbers in accordance with ETSI TR 102 634 [20].

6.3 Session-level virtual leased line between NGCN sites

6.3.1 Introduction

Session level virtual leased line provides a mechanism for transfer of requests from one entry point to one exit point with the provision of no application. The requests are private network traffic only.

6.3.2 Identification

The procedures of subclause 6.2.2 apply.

6.3.3 Registration

The procedures of subclause 6.2.3 apply.

6.3.4 Session originating from a NGCN user entering NGN

6.3.4.1 General

The procedures of subclause 6.2.4.1 apply with the exception that:

a) None of the entities within the NGN supporting the session level leased line provide a trust domain boundary. While the NGCN site either side of the leased line can themselves be a trust domain boundary, the NGN provides only the procedures associated with an NGCN trusted by the NGN.

6.3.4.2 NGCN not trusted by NGN

Not applicable.

6.3.4.3 NGCN trusted by NGN

The procedures of subclause 6.2.4.3 apply.

6.3.5 Session terminating to an NGCN user leaving NGN

6.3.5.1 General

The procedures of subclause 6.2.5.1 apply with the following exceptions:

a) None of the entities within the NGN supporting the session level leased line provide a trust domain boundary. While the NGCN site either side of the leased line can themselves be a trust domain boundary, the NGN provides only the procedures associated with an NGCN trusted by the NGN.

6.3.5.2 NGCN not trusted by NGN

Not applicable.

6.3.5.3 NGCN trusted by NGN

The procedures of clause 6.2.5.3 apply.

6.3.6 Business trunking applications

Not applicable.

6.3.7 Signalling transparency

The NGN shall be capable of transparent exchange of signalling elements that an IETF RFC 3261 [21] SIP proxy is not allowed to add, remove or modify, subject to the exception listed below, and shall be capable of being tolerant of and passing on without modification any signalling extension that is not supported. The exception is any information that needs to be changed to accomplish NAT traversal, i.e. IP addresses and ports in SDP. In particular, an NGN shall be capable of passing on a request, part of which is cryptographically signed (e.g. using the Identity header field), without removing or invalidating that signature. Whether such transparency is provided and to what degree is a matter for agreement between the NGN operator(s) and enterprise(s) concerned. This applies to any functional entity on the signalling path, including IBCF and routeing function.

6.3.8 Involvement of functions on the media path

The procedures of subclause 6.2.8 apply.

6.3.9 Handing of the P-Access-Network-Info header

The procedures of subclause 6.2.9 apply.

6.3.10 Emergency calls

No emergency call functionality is provided in this scenario.

NOTE: Any emergency call will be routed from entry point to exit point in the same manner as any other SIP request.

6.3.11 Charging

NOTE: Not covered in this release of the present document.

6.3.12 Advice of Charge

NOTE: Not covered in this release of the present document.

6.3.13 NAT traversal

NOTE: The application of NAT traversal mechanisms is not precluded, but detailed implications of their use in a business communication environment have not been studied.

6.3.14 Private network traffic

The NGCN site can include P-Private-Network-Indication header field as specified in IETF RFC 7316 [31] in an initial request or standalone request, with a valid private network identification for its use.

NOTE: In a virtual leased line scenario all traffic is private network traffic.

6.4 NGCN user roaming into NGN public network

6.4.1 Introduction

Void.

6.4.2 Identification

Not applicable.

6.4.3 Registration

An NGCN UE that supports roaming into NGN shall support IMS registration procedures as specified in 3GPP TS 24.229 [18], subclause 5.1 for an IMS UE.

NOTE: As a roaming UE cannot assume any security mechanisms, it therefore has to support IMS AKA. See also TS 133 203 [16].

A P-CSCF of a visited IMS shall support IMS registration procedures as specified in 3GPP TS 24.229 [18].

An IBCF acting as an exit point of the visited IMS shall support procedures as specified in 3GPP TS 24.229 [18], subclause 5.10.

An NGCN site that supports roaming of its users into NGN shall support registration procedures as if it were a home IMS, specified by concatenating the behaviour of the home IBCF acting as an entry point, home I-CSCF, home HSS and home S-CSCF, subclauses 5.10, 5.3 and 5.4 of 3GPP TS 24.229 [18].

6.4.4 Requests originating from an NGCN user roaming in NGN

An NGCN UE that supports roaming into NGN shall support IMS request origination procedures as specified in 3GPP TS 24.229 [18], subclause 5.1 for an IMS UE.

A P-CSCF of a visited IMS shall support IMS request origination procedures as specified in 3GPP TS 24.229 [18], subclause 5.2.

An IBCF acting as an exit point of the visited IMS shall support procedures as specified in 3GPP TS 24.229 [18], subclause 5.10.

An NGCN site that supports roaming of its users into NGN shall support request origination procedures as if it were a home IMS, specified by concatenating the behaviour of the home IBCF acting as an entry point, home I-CSCF, home HSS and home S-CSCF, subclauses 5.10, 5.3 and 5.4 of 3GPP TS 24.229 [18].

6.4.5 Requests terminating on an NGCN user roaming in NGN

An NGCN UE that supports roaming into NGN shall support IMS request termination procedures as specified in 3GPP TS 24.229 [18], subclause 5.1 for an IMS UE.

A P-CSCF of a visited IMS shall support IMS request termination procedures as specified in 3GPP TS 24.229 [18], subclause 5.2.

An IBCF acting as an entry point of the visited IMS shall support procedures as specified in 3GPP TS 24.229 [18], subclause 5.10.

An NGCN site that supports roaming of its users into NGN shall support request termination procedures as if it were a home IMS, specified by concatenating the behaviour of the home IBCF acting as an exit point, home HSS and home S-CSCF, subclauses 5.10 and 5.4 of 3GPP TS 24.229 [18].

6.4.6 Business trunking applications

Not applicable.

6.4.7 Signalling transparency

No additional requirements on the visited NGN are identified.

6.4.8 Involvement of functions on the media path

No additional requirements on the visited NGN are identified.

6.4.9 Handing of the P-Access-Network-Info header

No additional requirements on the visited NGN are identified.

6.4.10 Emergency calls

No additional requirements on the visited NGN are identified.

6.4.11 Charging

NOTE: Not covered in this release of the present document.

6.4.12 Advice of Charge

NOTE: Not covered in this release of the present document.

6.4.13 NAT traversal

NOTE: The application of NAT traversal mechanisms is not precluded, but detailed implications of their use in this scenario have not been studied.

6.4.14 Private network traffic

NOTE: The use of the P-Private-Network-Indication header field to distinguish private network traffic, if any, in this scenario is not covered in this release of the present document.

7 Use of transport functions

7.1 Use of transport control sublayer

7.1.1 Use of NASS

An NGCN site can obtain an IP address from the public/carrier access network to which it is attached as per the procedures developed in ETSI ES 282 004 [3]. Other parameters such as the P-CSCF identity may also be received from the NASS.

When requesting an IP address from the NGN, the NGCN site shall conform to ETSI TS 183 019 [9].

Within an NGCN site, the entity responsible for requesting an IP address from the NASS is either the CNG or, in case the CNG operates as a bridge (as specified in ETSI TS 185 003 [15]), a front-end device connected to the CNG playing the role of a NASS user. Other devices in the NGCN site are assigned IP addresses routable only within the corporate network.

As an alternative to the dynamic IP address allocation procedures described in NASS the NGN may offer an option to assign static IP addresses to the NGCN. In this case there may be no direct interaction between the NGCN and the NASS.

When the subscription based approach is used and no P-CSCF identity has been received from the NASS, the NGCN site will use a provisioned identity or an identity received from a Customer Network Gateway Control Function (CNGCF) if the procedures described in ETSI TS 183 065 [14] are supported by the NGCN site.

7.1.2 Use of RACS

In the present document it is assumed that there is no interaction between any policy driven resource control mechanisms deployed in the NGCN with those deployed in the NGN. The NGN may provide resource and admission control based on operator policy and the nature of the business trunking service provided to the NGCN (e.g. certain business trunking services can provide dedicated transport resources, others can provide sharing of transport resources across NGCNs, others can only provide best efforts). The control of Network Address Translation at the edge of the NGN is also part of the necessary resource and admission control supported by the NGN when providing business trunking services.

7.1.3 Use of PCC

In the present document it is assumed that there is no interaction between any policy driven resource control mechanisms deployed in the NGCN with those deployed in the NGN. The NGN may provide resource control based on operator policy and the nature of the business trunking service provided to the NGCN (e.g. certain business trunking services can provide dedicated transport resources, others can provide sharing of transport resources across NGCNs, others can only provide best efforts).

The control of Network Address Translation at the edge of the NGN is also part of the necessary resource and admission control supported by the NGN when providing business trunking services.

7.2 Use of transport processing functions

NOTE: Not covered in this release of the present document.

8 Security

The requirements of 3GPP TS 33.203 [16], clause 13 apply.

As specified by the requirements of 3GPP TS 33.203 [16] the related security mechanisms as specified in 3GPP TS 24.229 [18] apply.

9 Management

NOTE: Not covered in the present document.

Annex A (informative): Example signalling flows of business trunking and roaming arrangements

A.1 Scope of signalling flows

Void.

A.2 Introduction

Void.

A.3 Signalling flows for registration

A.3.1 Introduction

Void.

A.3.2 Registration of a roaming NGCN UE visiting an NGN/IMS with which the NGCN has a direct roaming agreement

A.3.2.1 General

The signalling flow shown here corresponds with scenario 7 figure 9.1.1 from 3GPP TS 24.523 [7].

A.3.2.2 Signalling flow for registration of a roaming NGCN UE visiting an NGN/IMS with which the NGCN has a direct roaming agreement

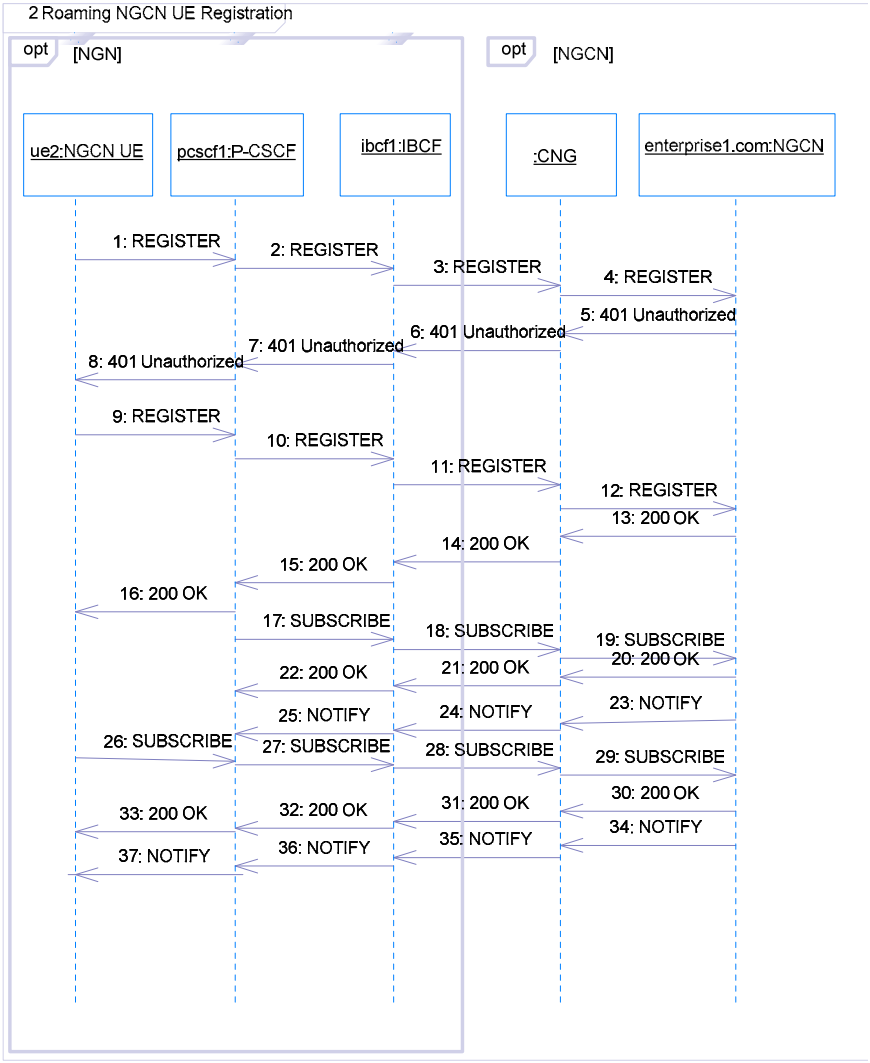

Figure A.1

(0) Preconditions:

The NGCN ue1 attached to the network by some means (acquired IP address, discovered P-CSCF, and established an IP-CAN bearer for signalling).

The following IMS parameters are assumed to be available to the UE:

a private user identity;

a public user identity; and

a home network domain name to address the SIP REGISTER request to.

Assumed authentication method: IMS AKA.

Assumed network domain security applies between IBCF and CNG on the Ic reference point.

(1) Unprotected REGISTER (No security association exists yet)

NGCN ue1 constructs a REGISTER request towards its home domain hosted by his NGCN, by Routing it via the obtained P-CSCF.

```
REGISTER sip:enterprise1.com
```

```
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
Route: sip:pcscf1.ngn1.com;lr
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
Contact: sip:ue1-ip;expires=600000
Authorization: Digest username="userA_private@operator1.com", realm="enterprise1.com",
uri="sip:enterprise1.com", nonce="", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha1-1-96; spi-c=3929102; spi-s=0293020; port-c=3333; port-
s=5059
Supported: path
Require: sec-agree
Proxy-Require: sec-agree
```

(2) NGN pcscf1 receives the request

removes itself from the Route header;

then routes the request based on the Request URI, this means that the NGN I-DNS needs to somehow resolve the enterprise1.com name to an entry point of the corporate network or an IBCF that handles traffic towards the enterprise1.com entrypoint.

```
REGISTER sip:enterprise1.com
Via: SIP/2.0/UDP sip:pcscf1.ngn1.com;lr;branch=p1xx
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
Path: sip:term@pcscf1.ngn1.com;lr
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
Contact: sip:ue1-ip;expires=600000
Authorization: Digest username="userA_private@operator1.com", realm="enterprise1.com", nonce="",
uri="sip:enterprise1.com", nonce="", response="", integrity-protected="no"
Require: path
Supported: path
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
P-Visited-Network-ID: "Visited NGN1"
```

(3) IBCF exit point receives the REGISTER

The functionalities of the IBCF include: network configuration hiding, application level gateway, transport plane control, i.e. QoS control, screening of SIP signalling; and inclusion of an Interworking Function (IWF) if appropriate. Assuming all these functions are active, then:

encrypt the existing Path header value and all headers which reveal topology information, such as Via, Route, Record-Route, Service-Route, and Path;

adds itself to the top of the Path header;

then routes the request based on the Request URI, this means that the NGN I-DNS needs to somehow resolve the enterprise1.com name to an entry point of the corporate network when it is the IBCF that resolves, or it is configured in the IBCF that handles traffic towards the enterprise1.com entrypoint.

```
REGISTER sip:enterprise1.com
Via: SIP/2.0/UDP sip:ibcf1.ngn1.com;branch=b1xx,
SIP/2.0/UDP <Token>; tokenized-by=ngn1.com,
SIP/2.0/UDP ue1-ip;branch=b1xx
Path: sip:term@ibcf1.ngn1.com;lr ,
<Token>;tokenized-by=ngn1.com
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
Call-ID: 111111
Contact: sip:ue1-ip;expires=600000
Authorization: Digest username="userA_private@operator1.com", realm="enterprise1.com", nonce="",
uri="sip:enterprise1.com", nonce="", response="", integrity-protected="no"
Require: path
Supported: path
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
P-Visited-Network-ID: "Visited NGN1"
```

(4,5) in corporate domain

(6) IBCF receives 401 Unauthorized

```
SIP/2.0 401 Unauthorized
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=n1xx
Call-ID: 111111
Via: SIP/2.0/UDP sip:ibcf1.ngn1.com;branch=b1xx,
SIP/2.0/UDP <Token>; tokenized-by=ngn1.com,
SIP/2.0/UDP ue1-ip;branch=b1xx
WWW-Authenticate: Digest realm="enterprise1.com",
nonce="asf86585sffajsdf",
algorithm=AKAv1-MD5,
ik="0123456789abcdeedcba9876543210",
ck="9876543210abcdeedcba0123456789"
```

(7) P-CSCF receives

```
SIP/2.0 401 Unauthorized
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=ib1xx
Via: SIP/2.0/UDP sip:pcscf1.ngn1.com;lr;branch=p1xx,
SIP/2.0/UDP ue1-ip;branch=b1xx
WWW-Authenticate: Digest realm="enterprise1.com",
nonce="asf86585sffajsdf",
algorithm=AKAv1-MD5,
ik="0123456789abcdeedcba9876543210",
ck="9876543210abcdeedcba0123456789"
```

(8) UE receives the challenge in the 401 from the P-CSCF

```
SIP/2.0 401 Unauthorized
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=ib1xx
Call-ID: 111111
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
WWW-Authenticate: Digest realm="enterprise1.com",
    nonce="asf86585sffajsdf",
    algorithm=AKAv1-MD5
Security-Server: ipsec-3gpp; alg=hmac-sha1-1-96; spi-c=9102392; spi-s=3020029; port-c=5555; port-
s=6666
```

(9) UE Sends a REGISTER with a challenge-response to the protected port of the P-CSCF (via security association just established)

```
REGISTER sip:enterprise1.com
Via: SIP/2.0/UDP ue1-ip: 5059;branch=b1xx
Route: sip:pcscf1.ngn1.com:6666;lr
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
Call-ID: 111111
Contact: sip:ue1-ip: 5059;expires=600000
Authorization: Digest username="userA_private@operator1.com", realm="enterprise1.com",
uri="sip:enterprise1.com", nonce="asf86585sffajsdf", response="jafl89908asdf", algorithm=AKAv1-MD5
Security-Client: ipsec-3gpp; alg=hmac-sha1-1-96; spi-c=3929102; spi-s=0293020; port-c=3333; port-
s=5059
Security-Server: ipsec-3gpp; alg=hmac-sha1-1-96; spi-c=9102392; spi-s=3020029; port-c=5555; port-
s=6666
Supported: path
Require: sec-agree
Proxy-Require: sec-agree
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234256ABCDEF
```

(10) P-CSCF sends

```
REGISTER sip:enterprise1.com
Via: SIP/2.0/UDP sip:pcscf1.ngn1.com;lr;branch=p1xx
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
Path: sip:term@pcscf1.ngn1.com;lr
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
```

```
Contact: sip:ue1-ip:5059;expires=600000
Authorization: Digest username="userA_private@operator1.com", realm="enterprise1.com", nonce="",
uri="sip:enterprise1.com", nonce="", response="", integrity-protected="yes"
Require: path
Supported: path
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234256ABCDEF
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
P-Visited-Network-ID: "Visited NGN1"
```

(11) IBCF sends

```
REGISTER sip:enterprise1.com
Via: SIP/2.0/UDP sip:ibcf1.ngn1.com;branch=b1xx,
SIP/2.0/UDP <Token>; tokenized-by=ngn1.com,
SIP/2.0/UDP ue1-ip;branch=b1xx
Path: sip:term@ibcf1.ngn1.com;lr ,
    <Token>;tokenized-by=ngn1.com
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com
Call-ID: 111111
Contact: sip:ue1-ip;expires=600000
uthorization: Digest username="userA_private@operator1.com", realm="enterprise1.com", nonce="",
    uri="sip:enterprise1.com", nonce="", response="", integrity-protected="yes"
Require: path
Supported: path
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234256ABCDEF
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
P-Visited-Network-ID: "Visited NGN1"
```

(12, 13) corporate network

(14) IBCF receives 200 OK

```
SIP/2.0 200 OK
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=n1xx
Call-ID: 111111
Via: SIP/2.0/UDP sip:ibcf1.ngn1.com;branch=b1xx,
SIP/2.0/UDP <Token>; tokenized-by=ngn1.com,
SIP/2.0/UDP ue1-ip;branch=b1xx
Contact: sip:ngcn-ip; expires=600000
P-Associated-URI: userA@enterprise1.com, userA@home.net
Service-Route: sip:orig@ngcn-site2.enterprise1.com;lr
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com; term-ioi=ngcn1.com
```

(15) P-CSCF receives 200 OK

```
SIP/2.0 200 OK
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=ib1xx
Via: SIP/2.0/UDP sip:pcscf1.ngn1.com;lr;branch=p1xx,
SIP/2.0/UDP ue1-ip;branch=b1xx
Contact: sip:ngcn-ip; expires=600000
P-Associated-URI: userA@enterprise1.com, userA@home.net
Service-Route: sip:orig@ngcn-site2.enterprise1.com;lr
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com; term-ioi=ngcn1.com
```

(16) UE receives 200 OK

```
SIP/2.0 200 OK
From: userA@enterprise1.com;tag=d1xx
To: userA@enterprise1.com;tag=ib1xx
Call-ID: 111111
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
Contact: sip:ngcn-ip; expires=600000
P-Associated-URI: userA@enterprise1.com, userA@home.net
Service-Route: sip:orig@ngcn-site2.enterprise1.com;lr
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com; term-ioi=ngcn1.com
```

(17) P-CSCF subscribes to regevent package

Following 3GPP TS 24.229 [18], for the SUBSCRIBE the same routing is used as for the REGISTER, i.e. the Service-Route is not used for this case. So the SUBSCRIBE will be routed by resolving the Request-URI, etc.

```
SUBSCRIBE sip: userA@enterprise1.com
Via: SIP/2.0/UDP sip:pcscf1.ngn1.com;lr;branch=p1xx
Path: sip:term@pcscf1.ngn1.com;lr
From: sip:pcscf1.ngn1.com;tag=ds1x
To: userA@enterprise1.com
Event: reg
Expires: 600001
P-Asserted-Identity: sip:pcscf1.ngn1.com
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
Contact: sip:pcscf1.ngn1.com
```

(18) IBCF

Determine the next hop by DNS or preconfigured list.

(26) UE subscribes to regevent package

```
SUBSCRIBE sip:userA@enterprise1.com
Route: sip:orig@pcscf1.ngn1.com:6666;lr,
    sip:orig@ngcn-site2.enterprise1.com;lr
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
From: userA@enterprise1.com;tag=ds1x
To: userA@enterprise1.com
Event: reg
Expires: 600000
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
Contact: ue1-ip:5059
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234256ABCDEF
```

(27) P-CSCF receives on its protected port on the SA with the UE the SUBSCRIBE

When routing via IBCF it is the P-CSCF that inserts the IBCF on the Route header. The IBCF does not record itself in the Service-Route for some reason, so the P-CSCF will add it to the route when needed.

It adds/modifies:

```
P-Asserted-Identity: sip:userA@enterprise1.com
Route: sip:ibcf1.ngn1.com;lr,
    sip:orig@ngcn-site2.enterprise1.com;lr
Record-Route: sip:orig@pcscf1.ngn1.com:6666;lr
Via: sip:pcscf1.ngn1.com;branch=p2xx
Via: SIP/2.0/UDP ue1-ip;branch=b1xx
P-Charging-Vector: icid-value="i1xxx"; orig-ioi=ngn1.com
```

(28) IBCF performs

record routes;

topology hiding, etc.

(34-37) The NOTIFY from the NGCN site being a subsequent request should follow reversely the recorded route for the SUBSCRIBE dialog

A.3.2.3 Overview of routing decisions

Table A.1 gives an overview of the points in the signalling flow where routing decisions have to be taken.

Table A.1

	Request-URI	**ngcn-ue1**	**p-cscf 1**	**ibcf 1**
Unprotected REGISTER	sip:enterprise1.com	(1) R-URI: sip:enterprise1.com Route: p-cscf1 - insert obtained outbound proxy "p-cscf1" in route header and route based on that.	(2) R-URI: sip:enterprise1.com - Remove self from Route - Route on Request-URI *- If based on DNS then DNS should resolve* "sip:enterprise1.com" *to the exit point of the NGN i.e. the IBCF* (See note)	(3) R-URI: sip:enterprise1.com - Route on Request-URI *- If based on DNS then DNS should resolve "*sip:enterprise1.com*" to the entry point of the NGCN* (See note)
Protected REGISTER	sip:enterprise1.com	(9) idem	(10) idem	(11) idem
SUBSCRIBE regevent subscribe from P-CSCF	sip:userA@enterprise1.com		(17) R-URI: sip:userA@enterprise1.com - Route to *the preconfigured exit point of the NGN i.e. the IBCF* (See note)	(18) Route on Request-URI sip:userA@enterprise1.com *- If based on DNS then DNS should resolve "*sip:enterprise1.com*" to the entry point of the NGCN* (See note)
SUBSCRIBE regevent from UE (protected)	sip:userA@enterprise1.com	(26) Route: pcscf1, ngcn-site2 (from service-route)	(27) Route: ibcf1, ngcn-site2	(28) Route: ngcn-site2
INVITE from UE (protected)	sip:userB@anywhere.com	Route: pcscf1, ngcn-site2 (from service-route)	Route: ibcf1, ngcn-site2	Route: ngcn-site2
NOTE: If combining a roaming arrangement with a subscription based business trunking arrangement in the same NGN, P-CSCF needs a different view on DNS for this. Also on the IBCF view the DNS should be carefully constructed.				

A.4 Signalling flows for call origination

Void.

A.5 Signalling flows for call termination

Void.

Annex B (informative): Service Level Agreement (SLA) considerations

This annex provides guidance on technical considerations that should form part of an SLA between an NGN operator and an NGCN operator:

1) define the NGCN sites that need to be interconnected, along with any business trunking application provided in the NGN;

2) define the mechanism used for business trunking for each NGCN site (peering based or subscription based);

3) define the host names within addresses of record used for each NGCN site;

4) define the use of public telecommunication numbers and PNP numbers by each NGCN site;

5) define the NGCN site identifier for each site, e.g. used for registration in the subscription based approach;

6) authentication and integrity protection mechanisms, including any credentials used;

7) the method of discovery of the outbound proxy (P-CSCF or IBCF) and any required preconfigured address if not discoverable;

8) the domain name of the NGN for subscription based approach;

9) the static IP address(s) assigned to each NGCN site of the enterprise for the purpose of communicating with the NGN;

10) take into account media types and formats to be supported and with what Quality of Service (QoS). In particular, it should indicate NGN handling of media types or formats that are not recognized or supported by the NGN, e.g. whether such media types or formats are accepted subject to "best effort" QoS or rejected;

11) define whether the NGN trust domain for P-Asserted-Identity header field extends to the NGCN, and if so, the Spec(T) to be used; in this case the NGCN sites are regarded as privileged senders; and

12) if the NGCN is not trusted with regard to P-Asserted-Identity header field, define whether the NGCN sites are regarded as privileged sender or not; in the former case an application server will perform identity validation.

Annex C (informative):
Void

Annex D (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2014-03					Version 0.0.0 Editor's internal draft	-	0.0.0	
2014-05					Incorporation of PCRs C1-141812 C1-141813 C1-141814 Correction of minor editorial errors.	0.0.0	0.1.0	
2014-06	CT-64	CP-140280			Version 1.0.0 presented for information at CT-64	0.1.0	1.0.0	
2014-07					Incorporation of PCRs C1-142702 C1-142703 C1-142868 C1-143206 C1-143230 Correction of minor editorial errors.	1.0.0	1.1.0	
2014-09	CT-65	CP-140632			Version 2.0.0 presented for approval at CT-65	1.1.0	2.0.0	
2014-09	CT-65	CP-140719			Plenary tdoc revised to include missing cover sheet	1.1.0	2.0.0	
2014-09	Post CT-65				Version 12.0.0 created after approval at CT-65	2.0.0	12.0.0	
2014-12	CT-66	CP-140839	0001	5	Addition of Business Trunking Applications	12.0.0	12.1.0	C1-145046
2014-12	CT-66	CP-140848	0002	1	Use of transport functions	12.0.0	12.1.0	C1-144880
2014-12	CT-66	CP-140848	0003	1	Intelligent routeing tables in peering-based business trunking	12.0.0	12.1.0	C1-144881
2014-12	CT-66	CP-140848	0004		Support of subscription based business trunking using ISC gateway function	12.0.0	12.1.0	C1-144547
2014-12	CT-66	CP-140848	0005		Reference update from draft-vanelburg-dispatch-private-network-ind to RFC 7316	12.0.0	12.1.0	C1-144548
2014-12	CT-66	CP-140848	0006		Closure of open issues relating to base IMS specification usage	12.0.0	12.1.0	C1-144549
2015-03	CT-67	CP-150082	0007		Removal of Hanging Paragraph	12.1.0	13.0.0	C1-150050
2016-06	CT-72	CP-160304	0009	1	Wrong EN on reference	13.0.0	13.1.0	C1-162868

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	CT-75					Upgrade to Rel-14	14.0.0
2018-06	SA-80	-	-	-		Update to Rel-15 version (MCC)	15.0.0

History

Document history		
V15.0.0	June 2018	Publication