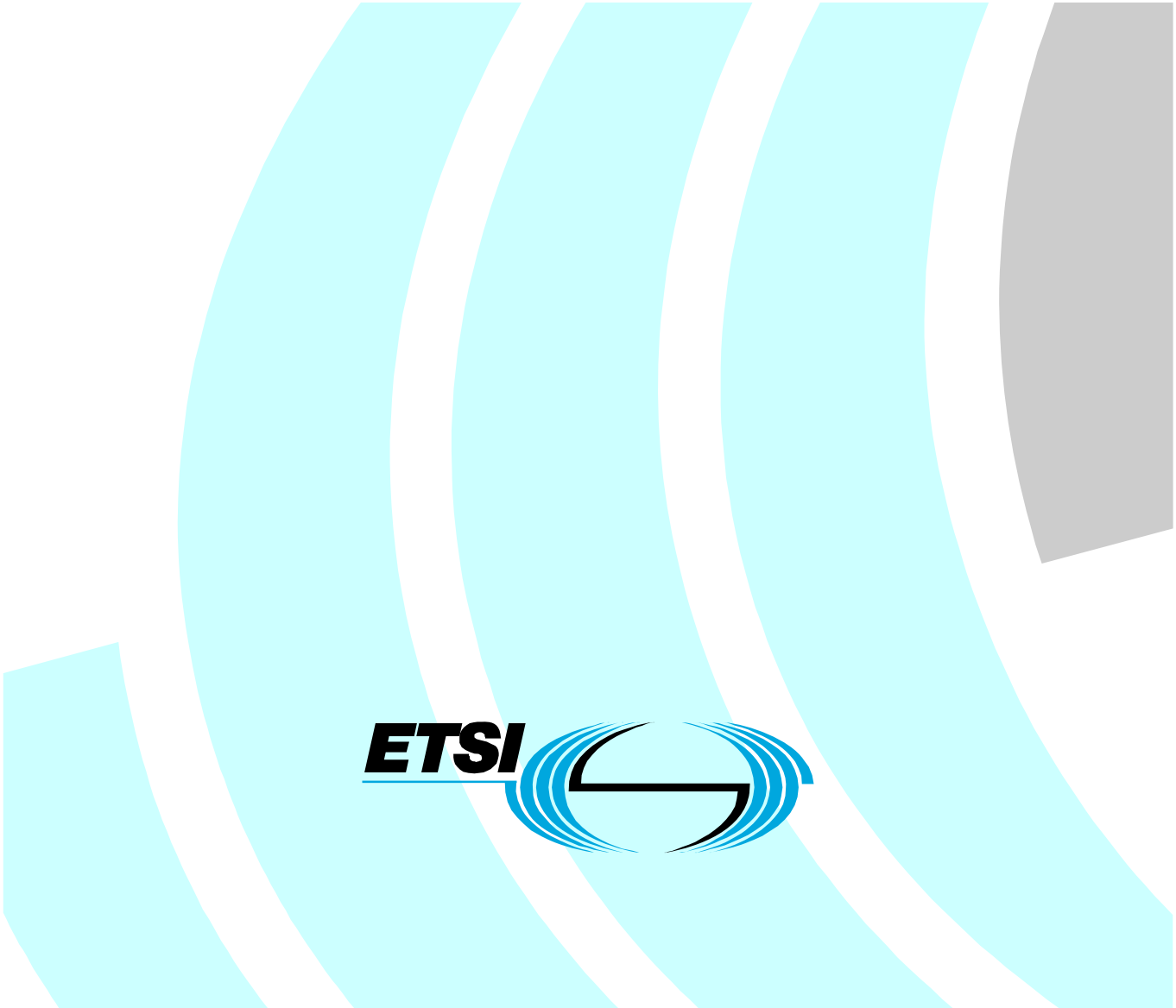
ETSI TS 182 025 V2.1.1 (2008-09)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business trunking; Architecture and functional description



Reference
DTS/TISPAN-02042-NGN-R2

Keywords
architecture, functional, trunking

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document provides architecture and functional requirements for business trunking for the Next Generation Network.

The present document also specifies the protocol requirements for the NGCN 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 Next Generation Corporate Networks (NGCN) using the NGN as a transit.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 181 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

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

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

[5] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 [Release 7], modified]".

[6] ETSI ES 282 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Charging [Endorsement of 3GPP TS 32.240 v6.3.0, 3GPP TS 32.260 v6.3.0, 3GPP TS 32.297 v6.1.0, 3GPP TS 32.298 v6.1.0 and 3GPP TS 32.299 v6.4.0 modified]".

[7] ETSI TS 182 023: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Core and Enterprise NGN Interaction Scenarios and Architectural Requirements".

[8] ETSI TS 183 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

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

[10] ETSI TS 183 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Common Basic Communication procedures; Protocol specification".

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

[12] ETSI TS 183 047: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN IMS Supplementary Services; Advice Of Charge (AOC)".

[13] ETSI TS 183 058: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); SIP Transfer of IP Multimedia Service Tariff Information; Protocol specification".

[14] ETSI TS 183 065: "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: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway Architecture and Reference Points".

[16] ETSI TS 187 003 (Release 2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[17] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[18] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[19] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[20] ECMA TR/NGCN-Identity: "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] IETF RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

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

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] draft-ietf-sip-location-conveyance-10 (February 2008): "Session Initiation Protocol Location Conveyance".

[i.2] draft-vanelburg-sipping-private-network-indication-01 (February 2008): "Requirements for explicit private network indication".

[i.3] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003)".

[i.4] ETSI TS 123 218: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia (IM) session handling; IM call model; Stage 2 (3GPP TS 23.218)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 181 019 [1], ES 282 004 [3], TS 123 228 [17], TS 123 003 [i.3] and TS 123 218 [i.4]apply:

3.2 Abbreviations

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

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
I-CSCF	Interrogating CSCF
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
LAN	Local Area Network
NASS	Network Attachment SubSystem
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
P-CSCF	Proxy CSCF
S-CSCF	Serving-CSCF
SIP	Session Initiation Protocol
SLA	Service Level Agreement

UE	User Equipment
UPSF	User Profile Server Function
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-CAN valid for TISPAN NGN using a Customer Network Gateway (CNG), as defined in 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 TS 185 003 [15], connected to a DSL-based access network (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 (figure 4.2).

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

NOTE 2: Within an NGCN site, the CNG functionality may 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 UPSF 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.

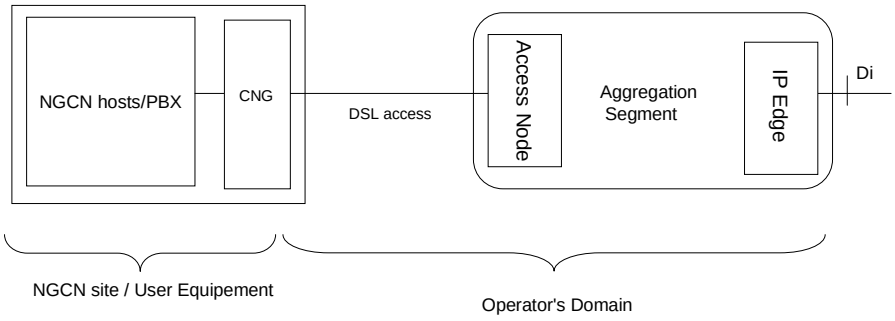


Figure 4.1: DSL access

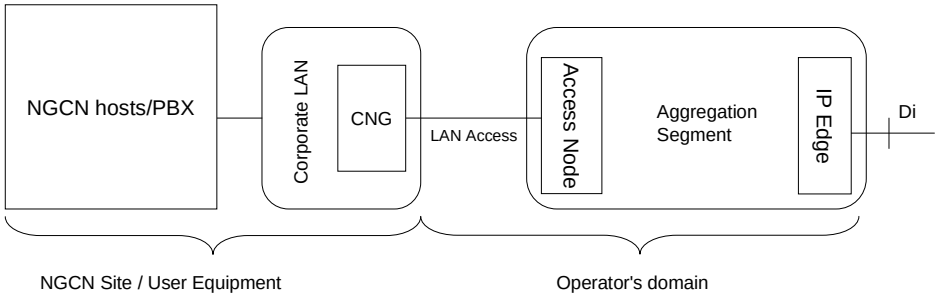


Figure 4.2: Corporate LAN access

Identifiers based on private numbers shall be handled in accordance with ECMA-TR/NGCN-Identity [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 clause 8.3 of ES 182 023 [7]. In this case each site of the NGCN has a service subscription to the IMS, with an appropriate entry in the UPSF. An AS is used to provide business trunking applications, e.g. those defined in TS 181 019 [1] clause 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 clause 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 clause 8.4 of ES 182 023 [7]. In this case there is no subscription to the IMS. However, the absence of a UPSF entry does not preclude the NGN to host enterprise specific data by other means. The service level capabilities of this scenario are described further in clause 6.2.

The second of these scenarios is called the peering-based approach due to the similarity of the scenario to the mechanism by which the IMS in two NGNs interconnection. For both cases, apart from the registration requirements of the subscription-based approach, the SIP entry point in the NGCN need provide no more functionality than a SIP proxy.

In neither case 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 clause 7.1 of ES 182 023 [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 clause 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 ES 282 001 [2].

5.2 Subscription based business trunking

5.2.1 General

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

Clause 8.3 of ES 182 023 [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 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);
- UPSF.

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 subscription-based business trunking can be found in clause 6.1.

5.2.3 Used reference points at the service layer

The main reference points from the IMS service layer as specified in 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;
- 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 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, e.g. I-CSCF, are not listed.

5.2.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in 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 Next Generation Corporate Network site (NGCN site) to the NGN using the IBCF as an entry point at the service layer.

Clause 8.4 of ES 182 023 [7] shows the arrangement of the involved functional entities.

5.3.2 Used functional entities at the service layer

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

- routeing function;
- IBCF.

The routeing function is defined in TS 123 228 [17] clause 5.19.

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 peering-based business trunking can be found in clause 6.2.

5.3.3 Used reference points at the service layer

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

- e2;
- Gq';
- Ic (this reference point forms the point of interconnection between the NGCN site and the NGN at the service layer);
- Mx.

NOTE: 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 ES 282 007 [4] that are used to realise session-level virtual 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, e.g. I-CSCF, are not listed.

5.3.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in 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.

5.4 Session-level virtual leased line

5.4.1 General

This describes the architectural requirements for the connection of an Next Generation Corporate Network site (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.

Clause 7.1 of ES 182 023 [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 ES 282 007 [4] that are used to realise session-level virtual leased line arrangements are as follows:

- routeing function;
- 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 clause 6.3.

5.4.3 Used reference points at the service layer

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

- Mx;
- Ic (this reference point forms the point of interconnection between the NGCN site and the NGN at the service layer);
- e2;

- Gq'.

5.4.4 Used functional entities at the transport layer

The main functional entities from the transport layer as specified in 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, e.g. I-CSCF, are not listed.

5.4.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in 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 Next Generation Corporate Network site (NGCN site) to the IMS using to allow NGCN users to roam into that IMS.

Clause 9.1 of ES 182 023 [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;
- 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 clause 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 ES 282 007 [4] used to realise roaming for NGCN users in NGN:

- Gm;
- Mx;
- e2;
- 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 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, e.g. I-CSCF, are not listed.

5.5.5 Used reference points at the transport layer

The main reference points from the transport layer as specified in 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 clause 6.1, the NGCN site shall comply with the requirements identified in TS 124 229 [18] clause 4.1 for a UE, taking into account the modifications specified in ES 283 003 [5].

In addition to the procedures specified in the clause 6.1, all functional IMS entities shall support the procedures appropriate for these entities specified in TS 124 229 [18] as modified by ES 283 003 [5] and in TS 183 028 [10].

NOTE: Some of the procedures in the referenced documents may not be applicable to an NGCN site. This area is for further study.

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 UPSF.

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!****!) or in the user portion of a SIP URI (e.g. sip:*@example.com). The wildcarded public user identity is configured in the UPSF 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: 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 clause 6.1.2, will be provided from the UPSF to the S-CSCF, the P-CSCF and the UA representing the NGCN site.

As part of the successful registration a security association as required by the access security requirements in TS 187 003 [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: 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 TS 187 003 [16].

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

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 UPSF to S-CSCF during registration as a result of performing the Cx Server Assignment procedure.

6.1.4 Requests originating from an NGCN user entering NGN

6.1.4.1 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 this clause has been split in a part that describes the procedure for:

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

Trust domain for asserted identity is defined in 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) that applies in the context of NGN is specified in ES 283 003 [5]. 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 a 18x message and a media flow being received, such a media flow would ideally not be authorized. 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.

6.1.4.2 NGCN not trusted by NGN

For a request originated in an untrusted NGCN and entering the NGN over the Gm reference point, normal IMS UNI procedures apply. When the request needs to be presented as originated from a particular NGCN user identified by a NGCN user identifier, the NGCN site can provide the NGCN user identifier in the P-Preferred-Identity header or in the P-Asserted-Identity header.

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

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

If the identity is provided either in a P-Preferred-Identity or a P-Asserted-Identity header field the P-CSCF checks whether this identity is part of the implicit registration set and if so the P-Preferred-Identity will be removed and the P-Asserted-Identity will be used within the NGN. When this identity is not part of the implicit registration set, a present P-Preferred-Identity and a present P-Asserted-Identity will be removed and the P-CSCF will provide a default identity in the P-Asserted-Identity. The default identity is the first identity on the list of URIs present in the P-Associated-URI header received as part of the registration procedure.

When the S-CSCF receives the request it finds a match between the P-Asserted-Identity and the wildcarded public user identity 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 with the contents of the From header, 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. This enables the NGCN user identifier to be sent to the destination in the form of an asserted identity.

6.1.4.3 NGCN trusted by NGN

If by policy the NGN and the NGCN form part of the same trust domain, the NGCN delivers the P-Asserted-Identity to the NGN. The NGN accepts the P-Asserted-Identity in this case.

NOTE: The P-Asserted-Identity is currently used by the S-CSCF to identify the served user, e.g. in relation to the appropriate set of initial filter criteria. In the trusted case, the P-Asserted-Identity may not relate to the numbers included in the business trunking agreement, e.g. due to forwarding in the NGCN before the call reached the NGN.

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

6.1.5 Requests terminating to an NGCN user leaving NGN

6.1.5.1 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 this clause has been split in a part that describes the procedure for:

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

Trust domain for asserted identity is defined in 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) that applies in the context of NGN is specified in ES 283 003 [5]. The Spec(T) to be used should be covered in the SLA.

6.1.5.2 NGCN not trusted by NGN

When an initial request for a new dialog or a request for a standalone transaction addressed to a NGCN site identifier or a NGCN user identifier in the Request-URI arrives at the I-CSCF, then I-CSCF performs a location request to UPSF to locate the S-CSCF where to forward the request to. The UPSF finds a match between the Request-URI and the registered NGCN site identifier or an implicitly registered wildcarded public user identity that belongs to the service profile of an NGCN site. The UPSF 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 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 in 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 UPSF during registration (see clause 6.9.1.3), it retains the received NGCN user identifier (including any URI parameters) in the Request-URI, then it adds to the Route header the contents of the Path header 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 UPSF. In such cases, the S-CSCF retains the received target identity in the Request-URI and adds the Contact address (stripping out the Display name field if any) to the Route header (as the last field value). 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 RFC 3261 [21].

For a response originated in an untrusted NGCN and entering the NGN over the Gm reference point, when the response needs to be presented as originated from a particular NGCN user identified by a NGCN user identifier, the NGCN site may provide the NGCN user identifier in the P-Asserted-Identity header field of a 18x or 2xx response.

If a P-Asserted-Identity header field is not present in the response from the NGCN, the P-CSCF shall provide the default identity for the NGCN site (see clause 6.1.4.1) in the P-Asserted-Identity header field.

If a P-Asserted-Identity header field is present in the response from the NGCN, the P-CSCF shall check whether this identity is part of the implicit registration set and if so the P-CSCF shall retain this identity when passing on the response. When this identity is not part of the implicit registration set, the NGN shall instead use the default identity for the NGCN site when passing on the response, replacing the value in the P-Asserted-Identity header field received from the NGCN.

NOTE: Sending a P-Asserted-Identity header by the UE over the Gm reference point is currently not supported according to IMS specifications.

In either case, if the Privacy header field with value "id" is received in a response, the P-CSCF shall retain it when passing on the response.

6.1.5.3 NGCN trusted by NGN

The procedures of clause 6.1.5.2 shall apply with the following exception.

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.

6.1.6 Business trunking applications

6.1.6.1 General

Business trunking applications are deployed on an AS. In case a 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.

TS 181 019 [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 Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2] 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 incoming 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 Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2], 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 TS 183 011 [8] clause 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 TS 183 011 [8], clause 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 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

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.

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

When a request or response received using an xDSL-based access the P-CSCF inserts a P-Access-Network-Info header into the forwarded request or response by setting the access-type field to one of the values specified in ES 283 003 [5] 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 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 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 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 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 ES 283 003 [5], 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 draft-ietf-sip-location-conveyance [i.1]. The P-CSCF can also provide location information in the P-Access-Network-Info header. 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 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 ES 282 010 [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 TS 183 047 [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 UPSF shall contain appropriate initial filter criteria ensuring that an Application Server supporting the procedures described in TS 183 047 [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 TS 183 058 [13] annex C.

6.1.13 NAT traversal

NOTE: TS 124 229 [18] annex F, annex G and annex K, as endorsed by ES 283 003 [5], specifies a number of 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.

6.1.14 Private network traffic

Private network traffic can be distinguished from public network traffic by the addition of a Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2].

NOTE: Procedures for use of the Private-Network-Indicator header field within the NGN require further study and are not covered in this release. Where an explicit indication of private network traffic is required within the NGN, then the Private-Network-Indicator header field is expected to be used.

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

The NGCN site can include Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2] in an initial request or standalone request, with a valid private network identification for its use.

The NGN can include Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2] 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 ECMA-TR/NGCN-Identity [20].

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 TS 124 229 [18], clause 4.1 for this functional entity, taking into account the modifications specified in ES 283 003 [5].

In addition to the procedures specified in the clause 6.2, all functional IMS entities shall support the procedures appropriate for these entities specified in TS 124 229 [18] as modified by ES 283 003 [5] and in TS 183 028 [10].

NOTE: Some of the procedures in the referenced documents may not be applicable to an NGCN site. This area is for further study.

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 this clause has been split in a part that describes the procedure for:

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

Trust domain for asserted identity is defined in 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) that applies in the context of NGN is specified in ES 283 003 [5]. 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 TS 187 003 [16].

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 or in the P-Asserted-Identity header is removed.

The IBCF will provide a default identity in the P-Asserted-Identity. 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, the IBCF shall not remove it when passing on the request.

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 to the NGN. The NGN does not remove the P-Asserted-Identity in this case.

If the Privacy header field with value "id" is received in a request, the IBCF shall not remove 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 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 this clause has been split in a part that describes the procedure for:

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

Trust domain for asserted identity is defined in 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) that applies in the context of NGN is specified in ES 283 003 [5]. The Spec(T) to be used should be covered in the SLA.

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 or in the P-Asserted-Identity header is removed.

The IBCF will provide a default identity in the P-Asserted-Identity. 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 response, the IBCF shall not remove it when passing on the 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 P-CSCF shall not remove this identity when passing on the response.

If the Privacy header field with value "id" is received in a response, the IBCF shall not remove it when passing on the response.

6.2.6 Business trunking application

Business trunking application are realised by the intelligent routeing function. In case a such services are offered to a specific enterprise the intelligent routeing function associated with a connected NGCN site needs to be configured so that it performs the business trunking application services.

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.

In order to provide these applications the intelligent routeing function then provides the procedures associated with an AS as specified in clause 6.1.6.

6.2.7 Signalling transparency

For private network traffic, an NGN shall be capable of transparent exchange of signalling elements that an 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

The P-Access-Network-Info header 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 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 handle 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 draft-ietf-sip-location-conveyance [i.1].

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 Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2].

NOTE: Procedures for use of the Private-Network-Indicator header field within the NGN require further study and are not covered in this release. Where an explicit indication of private network traffic is required within the NGN, then the Private-Network-Indicator header field is expected to be used.

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

The NGCN site can include Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2] in an initial request or standalone request, with a valid private network identification for its use.

The NGN can include Private-Network-Indicator header field as specified in draft-vanelburg-sipping-private-network-indication [i.2] 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 ECMA-TR/NGCN-Identity [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 clause 6.2.2 apply.

6.3.3 Registration

The procedures of clause 6.2.3 apply.

6.3.4 Session originating from a NGCN user entering NGN

6.3.4.1 General

The procedures of clause 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 clause 6.2.4.3 apply.

6.3.5 Session terminating to an NGCN user leaving NGN

6.3.5.1 General

The procedures of clause 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 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 clause 6.2.8 apply.

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

The procedures of clause 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

NOTE 1: Procedures for any use of the Private-Network-Indicator header field in this scenario require further study and are not covered in this release.

NOTE 2: 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 TS 124 229 [18] as modified by ES 283 003 [5], clause 5.1 for an IMS UE.

NOTE: As a roaming UE can not assume any security mechanisms, it therefore has to support IMS AKA. See also TS 133 203 [19].

A P-CSCF of a visited IMS shall support IMS registration procedures as specified in TS 124 229 [18] as modified by ES 283 003 [5], clause 5.2.

An IBCF acting as an exit point of the visited IMS shall support procedures as specified in TS 124 229 [15] as modified by ES 283 003 [5], clause 5.10.

An NGCN site that supports roaming of its users into NGN shall support registration procedures as if it where a home IMS, specified by concatenating the behaviour of the home IBCF acting as an entry point, home I-CSCF, home UPSF and home S-CSCF, clauses 5.10, 5.3 and 5.4 of TS 124 229 [18] as modified by ES 283 003 [5].

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 TS 124 229 [18] as modified by ES 283 003 [5], clause 5.1 for an IMS UE.

A P-CSCF of a visited IMS shall support IMS request origination procedures as specified in TS 124 229 [18] as modified by ES 283 003 [5], clause 5.2.

An IBCF acting as an exit point of the visited IMS shall support procedures as specified in TS 124 229 [18] as modified by ES 283 003 [5], clause 5.10.

An NGCN site that supports roaming of its users into NGN shall support request origination procedures as if it where a home IMS, specified by concatenating the behaviour of the home IBCF acting as an entry point, home I-CSCF, home UPSF and home S-CSCF, clauses 5.10, 5.3 and 5.4 of TS 124 229 [18] as modified by ES 283 003 [5].

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 TS 124 229 [18] as modified by ES 283 003 [5], clause 5.1 for an IMS UE.

A P-CSCF of a visited IMS shall support IMS request termination procedures as specified in TS 124 229 [18] as modified by ES 283 003 [5], clause 5.2.

An IBCF acting as an entry point of the visited IMS shall support procedures as specified in TS 124 229 [18] as modified by ES 283 003 [5], clause 5.10.

An NGCN site that supports roaming of its users into NGN shall support request termination procedures as if it where a home IMS, specified by concatenating the behaviour of the home IBCF acting as an exit point, home UPSF and home S-CSCF, clauses 5.10 and 5.4 of TS 124 229 [18] as modified by ES 283 003 [5].

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 Private-Network-Indicator header field to distinguish private network traffic, if any, in this scenario requires further study and 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 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 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 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 CNGCF if the procedures described in 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 may provide dedicated transport resources, others may provide sharing of transport resources across NGCNs, others may 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 TS 187 003 [16], clause 13 apply.

As specified by the requirements of TS 187 003 [16] the related security mechanisms as specified in TS 124 229 [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 ES 182 023 [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

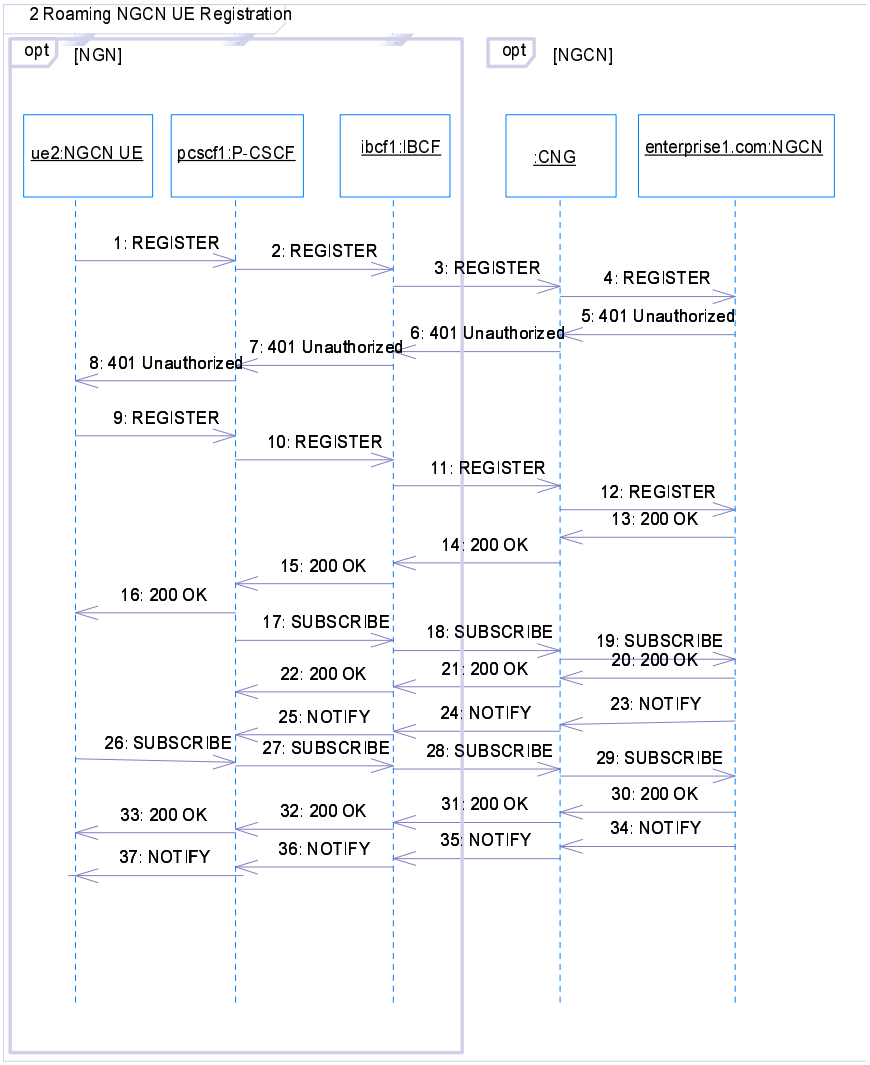


Figure A.1

(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 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
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"
```

(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 TS 124 229 [18] as modified by ES 283 003 [5], 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 the Spec(T) to be used for P-Asserted-Identity.

Annex C (informative): Bibliography

- ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 V7.2.0, modified)".
- ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

History

Document history		
V2.1.1	September 2008	Publication