VoLTE Service Description and Implementation Guidelines

Version 1.1

26 March 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

Voice over LTE, or VoLTE is a GSMA profile of the standards definition for the delivery of services currently provided via Circuit Switch networks - mainly voice and SMS - over the Packet Switched only network of LTE, leveraging the core network IP Multimedia Sub-System (IMS). When mobile networks deploy LTE radio access technology, conformity to the VoLTE profile provides operators with assurance of interworking between their LTE network and the devices that connect to it, as well as providing for the expected user experience of voice Multi-Media Telephony service and SMS. In combination with Policy Control, IMS provides for the required QoS appropriate for voice service using LTE radio access technology, thereby providing the user experience of voice calls that subscribers expect. Moreover, VoLTE is designed to fully integrate with the existing user experience that is currently implemented with circuit switched voice devices, and therefore whether the call is a circuit switched call or a VoLTE call is transparent to the end user (including when moving in and out of LTE coverage) and is dependent only on which radio access technology to which the user is attached. At the same time, using new, wideband codecs can provide higher voice quality and enhance the user experience.

VoLTE is in accordance with 3GPP specifications and additional profiling is defined within GSMA Permanent Reference Documents.

GSMA PRD IR.92 [54] defines the UNI for IMS voice and SMS. It defines a profile that identifies a minimum mandatory set of features which are defined in 3GPP specifications that a wireless device (UE) and network are required to implement in order to guarantee an interoperable, high quality IMS-based telephony service over LTE.

The NNI for VoLTE is defined in the IMS Roaming & Interworking Guidelines GSMA PRD IR.65 [51].

VoLTE Roaming is defined in the LTE Roaming Guidelines GSMA PRD IR.88 [53].

This document defines the VoLTE service description and implementation guidelines in order to provide an end-to-end VoLTE deployment.

Note that in this version of the document, CSFB and SRVCC are not in scope.

1.2 Relationship to Standards

VoLTE is based on publically available and published 3GPP specifications as listed in Section 1.5. 3GPP Release 8, the first release supporting LTE, is taken as a basis for the VoLTE profile. It should be noted, however that not all the features mandatory in 3GPP Release 8 are required for compliance with VoLTE.

Conversely, some features required for compliance with VoLTE are based on functionality defined in 3GPP Release 9 or higher releases.

Unless otherwise stated, the latest version of the referenced specifications for the relevant 3GPP release applies.

Detailed information related to the support of specific 3GPP functionality per release is defined within GSMA PRD IR.92 [54].

1.3 Scope

This document is separated into 5 main sections.

- Section 2 VoLTE Architecture:- defines the logical architecture, functional node description, and interfaces required for VoLTE deployment.
- Section 3 VoLTE Implementation – Single PMN:- defines what is required to deploy VoLTE within a single MNO's domain; detailing call flows, supplementary services required, Diameter configuration aspects, traffic management and QoS aspects, security, etc.
- Section 4 VoLTE Implementation – Interconnect:- defines what is required in addition to an Intra-PMN deployment, for interconnecting two MNO's VoLTE deployments; detailing call flows, bi-lateral interconnect, IPX interconnect, ENUM/DNS, usage of Session Border Controllers, etc.
- Section 5 VoLTE Implementation – Roaming:- defines what is required in addition to an Intra-PMN deployment, for allowing subscribers to roam between two MNO's VoLTE deployments; detailing call flows, Local-BreakOut (LBO), Impacts to Diameter routing, policy and QoS aspects, etc.
- Section 6 Implementation Guidelines:- highlights the issues discovered during VoLTE Interoperability testing (IOT) and in commercial operator deployments.

1.4 Definition of Terms

Term	Description
3GPP	3rd Generation Partnership Project
A-SBC	Access Session Border Controller
ACR	Anonymous Call Rejection
AMBR	Aggregate Maximum Bit Rate
AMR	Adaptive Multi-Rate
AMR-WB	Adaptive Multi-Rate Wideband
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation and Retention Priority
AS	Application Server
AUTN	Authentication Token
AVP	Attribute Value Pair
BGCF	Border Gateway Control Function
BICC	Bearer Independent Call Control
CAMEL	Customised Application for Mobile network Enhanced Logic
CDIV	Communication Diversion
CDR	Charging Data Record
CN	Core Network
CONF	Conferencing

CS	Circuit Switched
CSCF	Call Server Control Function
CSFB	Circuit Switched Fall Back
CW	Call Waiting
DEA	Diameter Edge Agent
DiffServ	Differentiated Services
DL	DownLink
DNS	Domain Name System
DPI	Deep Packet Inspection
DRA	Diameter Relay Agent
DRX	Discontinuous Reception
DSCP	DiffServ Code Point
ECGI	E-UTRAN Cell Global Identifier
e2ae	end to access edge
e2e	end to end
eKSI	E-UTRAN Key Set Identifier
ENUM	E.164 Number Mapping
EPC	Evolved Packet Core
EPS	Evolved Packet System
ERAB	E-UTRAN Radio Access Bearer
ESM	EPS Session Management
eSRVCC	Enhanced Single Radio Voice Call Continuity
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Access Network
FDD	Frequency Division Duplex
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBR	Guaranteed Bit Rate
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HPMN	Home Public Mobile Network
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
I-CSCF	Interrogating Call Session Control Function

I-SBC	Interconnect Session Border Controller
IBCF	Interconnection Border Control Function
icid	IM CN subsystem charging identifier
ICS	IMS Centralised Services
ICSI	IMS Communication Service Identifier
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IM	IP Multimedia
IM-GW	IP Media Gateway
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMS-AKA	IMS Authentication and Key Agreement
IMS-AGW	IMS Access Gateway
IMS-ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identity
IOT	Interoperability Testing
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	IP Security
IPX	IP Packet Exchange
ISIM	IM Services Identity Module
ISUP	ISDN User Part
LBO	Local Breakout
LTE	Long Term Evolution
MAC	Medium Access Control
MBR	Maximum Bit Rate
MCC	Mobile Country Code
ME	Mobile Equipment
MGCF	Media Gateway Control Function
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMTel	Multimedia Telephony
MNC	Mobile Network Code
MNO	Mobile Network Operator
MRF	Media Resource Function
MSISDN	Mobile Subscriber ISDN Number
MSRP	Message Session Relay Protocol
MTU	Maximum Transmission Unit

MWI	Message Waiting Indicator
NAPTR	Name Authority Pointer
NAS	Non-Access Stratum
NAT	Network Address Translation
NNI	Network to Network Interface
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
P-CSCF	Proxy Call Session Control Function
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCO	Protocol Configuration Options
PCRF	Policy Charging and Rules Function
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PHB	Per Hob Behaviour
PLMN	Public Land Mobile Network
PMN	Public Mobile Network
PS	Packet Switched
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAND	RANDom number (used for authentication)
RAT	Radio Access Technology
RES	user RESponse (used in IMS-AKA)
RLC	Radio Link Control
RRC	Radio Resource Control
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving Call Session Control Function
SAE	System Architecture Evolution
SBC	Session Border Controller
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SEG	Security Gateway
SGW	Serving Gateway
SGSN	Serving GPRS Support Node
SIGCOMP	Signalling Compression

SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SMS	Short Message Service
SON	Self-Organising Networks
SRTP	Secure RTP
SRVCC	Single Radio Voice Call Continuity
TAS	Telephony Application Server
TAI	Tracking Area Identity
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TEID	Tunnel End Point Identifier
TFT	Traffic Flow Template
THP	Traffic Handling Priority
TLS	Transport Layer Security
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TrGW	Transition Gateway
TTM	Time To Market
UDC	User Data Convergence
UDP	User Datagram Protocol
UDR	User Data Repository
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
ULI	User Location Information
UMTS	Universal Mobile Telecommunications System
UNI	User to Network Interface
URN	Uniform Resource Name
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
VoHSPA	Voice over HSPA
VoLTE	Voice over LTE
VPMN	Visited Public Mobile Network
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language
XRES	eXpected user RESponse (used in IMS-AKA)

1.5 Document Cross-References

Ref	Document Number	Title
[1]	3GPP TS 23.002	Network Architecture
[2]	3GPP TS 23.003	Numbering, addressing and identification
[3]	3GPP TS 23.060	General Packet Radio Service (GPRS); Service description; Stage 2
[4]	3GPP TS 23.203	Policy and charging control architecture
[5]	3GPP TS 23.228	IP Multimedia Subsystem (IMS); Stage 2
[6]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[7]	3GPP TS 24.147	Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3
[8]	3GPP TS 24.173	IMS Multimedia telephony communication service and supplementary services; Stage 3
[9]	3GPP TS 24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[10]	3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
[11]	3GPP TS 24.247	Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3
[12]	3GPP TS 24.341	Support of SMS over IP networks; Stage 3
[13]	3GPP TS 24.604	Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[14]	3GPP TS 24.605	Conference (CONF) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[15]	3GPP TS 24.606	Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[16]	3GPP TS 24.607	Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[17]	3GPP TS 24.608	Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[18]	3GPP TS 24.610	Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[19]	3GPP TS 24.611	Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
[20]	3GPP TS 24.615	Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol Specification

[21]	3GPP TS 24.623	Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services
[22]	3GPP TS 29.061	Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
[23]	3GPP TS 29.163	Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks
[24]	3GPP TS 29.165	Inter-IMS Network to Network Interface (NNI)
[25]	3GPP TS 29.212	Policy and Charging Control (PCC); Reference points
[26]	3GPP TS 29.214	Policy and charging control over Rx reference point
[27]	3GPP TS 29.215	Policy and Charging Control (PCC) over S9 reference point; Stage 3
[28]	3GPP TS 29.228	IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents
[29]	3GPP TS 29.229	Cx and Dx interfaces based on the Diameter protocol; Protocol details
[30]	3GPP TS 29.272	Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
[31]	3GPP TS 29.274	3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
[32]	3GPP TS 29.281	General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
[33]	3GPP TS 29.328	IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents
[34]	3GPP TS 29.329	Sh interface based on the Diameter protocol; Protocol details
[35]	3GPP TS 29.332	Media Gateway Control Function (MGCF) - IM Media Gateway; Mn interface
[36]	3GPP TR 29.809	Study on Diameter overload control mechanisms
[37]	3GPP TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application
[38]	3GPP TS 32.240	Telecommunication management; Charging management; Charging architecture and principles
[39]	3GPP TS 32.260	Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging
[40]	3GPP TS 32.298	Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
[41]	3GPP TS 33.107	3G security; Lawful interception architecture and functions
[42]	3GPP TS 33.328	IP Multimedia Subsystem (IMS) media plane security
[43]	3GPP TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture
[44]	3GPP TS 36.300	Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);

		Overall description; Stage 2
[45]	3GPP TS 36.413	Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)
[46]	3GPP TS 36.423	Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP)
[47]	ETSI TS 183 038	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Simulation Services; Extensible Markup Language (XML) Document Management; Protocol Specification
[48]	GSMA PRD IR.34	Inter-Service Provider IP Backbone Guidelines
[49]	GSMA PRD IR.58	IMS Profile for Voice over HSPA
[50]	GSMA PRD IR.64	IMS Service Centralization and Continuity Guidelines
[51]	GSMA PRD IR.65	IMS Roaming and Interworking Guidelines
[52]	GSMA PRD IR.67	DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers
[53]	GSMA PRD IR.88	LTE Roaming Guidelines
[54]	GSMA PRD IR.92	IMS Profile for Voice and SMS
[55]	IETF RFC 768	User Datagram Protocol
[56]	IETF RFC 2246	The TLS Protocol Version 1.0
[57]	IETF RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
[58]	IETF RFC 3550	RTP: A Transport Protocol for Real-Time Applications
[59]	IETF RFC 3588	Diameter Base Protocol
[60]	IETF RFC 3711	The Secure Real-time Transport Protocol (SRTP)
[61]	IETF RFC 4867	RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
[62]	IETF RFC 4961	Symmetric RTP / RTP Control Protocol (RTCP)
[63]	IETF RFC 5009	Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media
[64]	IETF RFC 6357	Design Considerations for Session Initiation Protocol (SIP) Overload Control
[65]	3GPP TS 29.235	Interworking between SIP-I based circuit-switched core network and other networks
[66]	3GPP TS 23.205	Bearer-independent circuit-switched core network; Stage 2
[67]	3GPP TS 23.231	SIP-I based circuit-switched core network; Stage 2
[68]	IETF RFC 3966	The tel URI for Telephone Numbers
[69]	IETF RFC 3261	SIP: Session Initiation Protocol
[70]	IETF RFC 3312	Integration of Resource Management and Session Initiation Protocol (SIP)
[71]	IETF RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

[72]	3GPP TS 29.238	Interconnection Border Control Function (IBCF) – Transition Gateway (TrGW) interface, Ix interface; Stage 3.
[73]	3GPP TS 29.334	IMS Application Level Gateway (ALG) – IMS Access Gateway (IMS-AGW); Iq interface; Stage 3.
[74]	GSMA PRD AA.80	IP Packet eXchange Service Agreement
[75]	3GPP TS 23.335	User Data Convergence (UDC); Technical Realization and Information Flows; Stage 2
[76]	3GPP TS 29.079	Optimal Media Routing within the IP Multimedia System (IMS); Stage 3
[77]	IETF RFC 5031	A Uniform Resource Name (URN) for Emergency and other Well-Known Services
[78]	3GPP TS 23.167	IP Multimedia Subsystem (IMS) Emergency Sessions
[79]	3GPP TS 29.213	Policy and Charging Control signalling flows and Quality of Service (QoS) Parameter Mapping.
[80]	IETF RFC 4028	Session Timers in the Session Initiation Protocol (SIP)

2 VoLTE Architecture

The VoLTE logical architecture is based on the 3GPP defined architecture and principles for VoLTE UE, Long Term Evolution (LTE), Evolved Packet Core network (EPC), and the IMS Core Network. It consists of the following:-

- **VoLTE UE:** The VoLTE UE contains functionality to access the LTE RAN and the EPC to allow mobile broadband connectivity. An embedded IMS stack and VoLTE IMS application are required to access VoLTE services.
- **Radio Access Network**. The Evolved Universal Terrestrial Radio Access Network (E-UTRAN); this is often referred to as Long Term Evolution (LTE). LTE radio capabilities for FDD LTE only, TDD LTE only, or both FDD and TDD LTE are applicable for VoLTE.
- **Core Network**. The Evolved Packet Core (EPC).
- **IMS Core Network.** The IMS Core Network within the VoLTE architecture provides the service layer for providing Multimedia Telephony.

The VoLTE logical architecture, including roaming and interconnect, is shown in Figure 1.

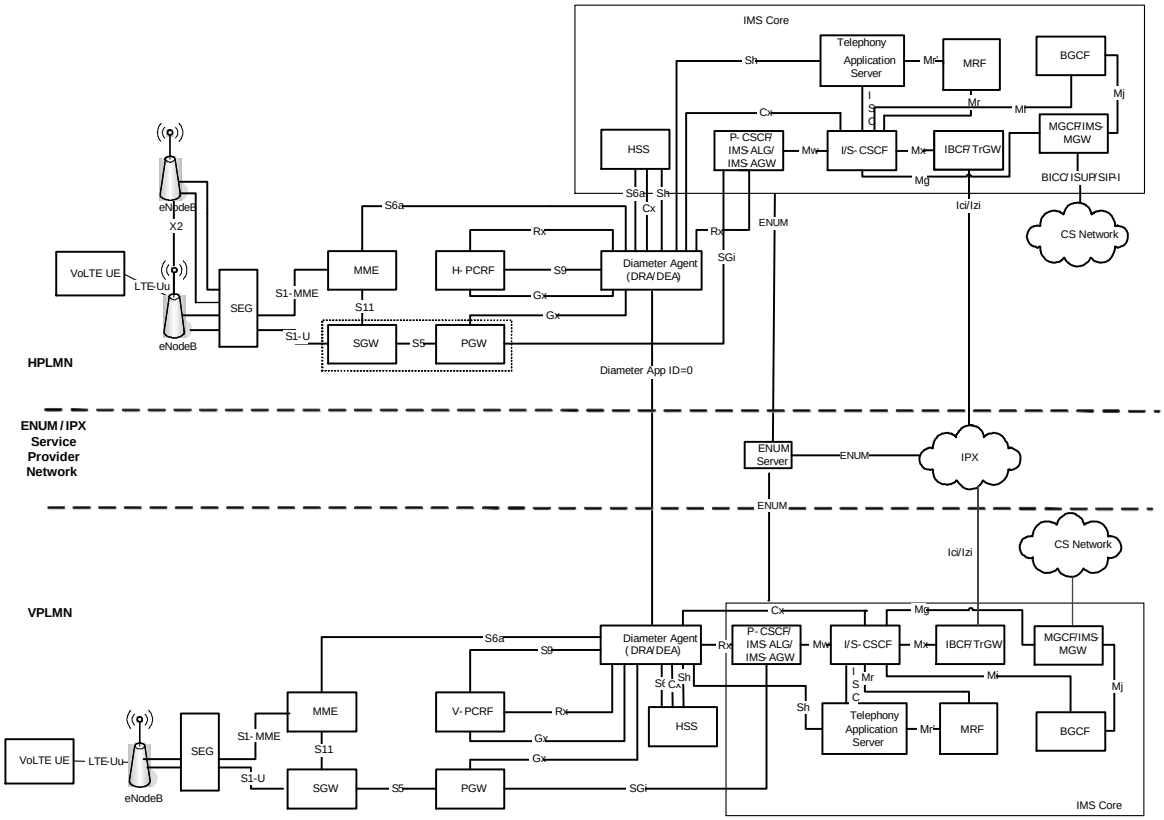

Figure 1: VoLTE Logical Architecture

NOTE: The Gm interface (UE to P-CSCF) is included in the VoLTE architecture although not shown in the above figure.

NOTE: The Ut interface (UE to TAS) is included in the VoLTE architecture although not shown in the above figure.

NOTE: The figure details the logical nodes within the VoLTE architecture; however it is possible to combine functional nodes into a single physical node implementation (e.g. SGW and PGW). When this is performed, the relevant interfaces between the logical nodes (e.g. S5) become internal interfaces and therefore are not exposed in the network.

2.1 VoLTE Functional Node Description

The main functional nodes of the VoLTE architecture are defined by 3GPP and are described below. Further information can viewed in 3GPP TS 23.002 [1].

2.1.1 VoLTE UE (User Equipment)

The User Equipment that is used to connect to the EPC, in the figure above this is an LTE capable UE accessing EPC via the LTE-Uu radio interface. Other access technologies may also be supported by the UE.

2.1.2 Evolved Universal Terrestrial Access Network (E-UTRAN)

2.1.2.1 eNodeB

The EUTRAN consists of a single node, the eNodeB that interfaces with the UE. The eNodeB hosts the Physical (PHY), Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Convergence Protocol (PDCP) layers that include the functionality of user-plane header-compression and encryption. It also offers Radio Resource Control (RRC) functionality corresponding to the control plane. It performs many functions including radio resource management, admission control, scheduling, enforcement of negotiated UL QoS, cell information broadcast, ciphering/deciphering of user and control plane data, and compression/decompression of DL/UL user plane packet headers.

2.1.3 Evolved Packet Core

2.1.3.1 MME (Mobility Management Entity)

The Mobility Management Entity (MME) is the key control-node for the LTE access network. It is responsible for idle mode UE tracking and paging procedures including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the SGW for the UE at the initial attach and at the time of intra-LTE handover involving Core Network node relocation. It is responsible for authenticating the user (in conjunction with the HSS). The NAS (Non-Access Stratum) signalling terminates at the MME which is also responsible for the generation and allocation of temporary identities to the UEs. The MME validates the permission of the UE to camp on the service provider's PMN and enforces UE roaming restrictions. The MME is the termination point in the network for ciphering/integrity protection for NAS signalling and handles security key management. Lawful interception of signalling is also a function provided by the MME. The MME provides the control plane function for mobility between LTE and 2G/3G access networks and interfaces with the home HSS for roaming UEs.

2.1.3.2 SGW (Serving Gateway)

The SGW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating the S4 interface and relaying the traffic between 2G/3G systems and PGW). For idle state UEs, the SGW terminates the DL data path and triggers paging when the DL data arrives for the UE. It manages and stores UE contexts and performs replication of the user traffic in case of lawful interception. The SGW and PGW functions could be realized as a single network element.

2.1.3.3 PGW (Packet Data Network Gateway)

The PGW provides connectivity between the UE and external packet data networks. It provides the entry and exit point of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple Packet Data Networks. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening. The SGW and PGW functions could be realized as a single network element.

2.1.3.4 HSS (Home Subscriber Server)

The HSS is a network database that holds both static and dynamic data elements related to subscribers. The HSS provides user profile information to the MME and IMS core during UE attach and IMS registration.

2.1.3.5 PCRF (Policy Charging and Rules Function)

The PCRF provides policy control decisions and flow based charging controls. The PCRF determines how a service data flow shall be treated in the enforcement function (PGW in this case) and ensure that the user plane traffic mapping and treatment is in accordance with the user's profile.

2.1.4 IMS

IMS is the control infrastructure for supporting next generation IP Multimedia Services and consists of many separate elements which are listed below.

2.1.4.1 P-CSCF (Proxy Call Session Control Function)

The P-CSCF is the initial point of contact for session signalling for the IMS-enabled VoLTE UE. The P-CSCF behaves as a SIP proxy by forwarding SIP messages between the UE and the IMS Core Network, maintains the security associations between itself and the VoLTE UE, and incorporates the Application Function aspect of PCC to enable binding of the IMS session with the bearer for applying dynamic policy and receiving notifications of bearer level events. The P-CSCF may be implemented in an Access Session Border Controller which may also incorporate the IMS-ALG/IMS-AGW.

2.1.4.2 I-CSCF (Interrogating Call Session Control Function)

The I-CSCF is the contact point within an operator's network for all connections destined to a user of that network. On IMS registration, it interrogates the HSS to determine which suitable S-CSCF to route the request for registration. For mobile terminating calls, it interrogates the HSS to determine which S-CSCF the user is registered on.

2.1.4.3 S-CSCF (Serving Call Session Control Function)

The S-CSCF provides session set-up, session tear-down, session control and routing functions. It generates records for billing purposes for all sessions under its control, and invokes Application Servers based on IFCs received from the HSS. The S-CSCF acts as SIP registrar for VoLTE UEs that the HSS and I-CSCF assign to it. It queries the HSS for the applicable subscriber profiles and handles calls involving these end points once they have been registered.

2.1.4.4 Telephony Application Server (TAS)

The TAS is an IMS Application Server providing support for a minimum set of mandatory MultiMedia Telephony (MMTel) services as defined by 3GPP e.g. supplementary service functionality, and profiled within GSMA PRD IR.92 [54].

2.1.4.5 MRF (Media Resource Function)

The MRF is a common media resource function, for use by IMS Application Servers and I/S-CSCFs, to provide media plane processing independent of application types, e.g.

transcoding, multiparty conferencing, network announcements/tones, etc. under the control of IMS Application Servers (VoLTE AS) as well as basic media processing functions to CSCFs. The control plane interfaces to MRFs are defined by the 3GPP references Mr, Mr', and Cr interfaces (SIP/SDP and XML encoded media service requests) while the media plane interfaces to MRFs are defined by 3GPP reference Mb for RTP/RTCP transport.

2.1.4.6 IBCF/TrGW (Interconnection Border Control Function/Transition Gateway)

The IBCF/TrGW is responsible for the control/media plane at the network interconnect point to other PMNs. The IBCF/TrGW may be implemented in an Interconnect Session Border Controller.

2.1.4.7 IMS-ALG/IMS-AGW (IMS Application Level Gateway/IMS Access Gateway)

The IMS-ALG/IMS-AGW is not a stand-alone function, but is located with the P-CSCF. The IMS-ALG/IMS-AGW is responsible for the control/media plane at the access point to the IMS network. It provides functions for Gate Control & Local NAT, IP realm indication and availability, Remote NAT traversal support, Traffic Policing, QoS Packet Marking, IMS Media Plane Security, etc.

2.1.4.8 MGCF/IMS-MGW (Media Gateway Control Function / IMS Media Gateway)

The MGCF/IMS-MGW is responsible for the control/media plane interworking at the network interconnect point to circuit-switched networks. This includes interworking to CS Networks based on BICC/ISUP/SIP-I and may include transcoding of the media plane.

2.1.4.9 BGCF (Breakout Gateway Control Function)

The BGCF is responsible for determining the next hop for routing of SIP messages. This determination is based on information received within the SIP/SDP and routing configuration data (which can be internal configuration data or ENUM/DNS lookup). For CS Domain terminations, the BGCF determines the network in which CS domain breakout is to occur and selects the appropriate MGCF. For terminations in peer IMS networks, the BGCF selects the appropriate IBCF to handle the interconnect to the peer IMS domain. The BGCF may also provide directives to the MGCF/IBCF on which Interconnect or next network to select . Such directives may be given by inclusion of a route header pointing to the next network ingress node.

2.1.5 Additional Network Functionality

2.1.5.1 ENUM

This functionality enables translation of E.164 numbers to SIP URIs using DNS to enable message routing of IMS sessions. In the above figure, a single ENUM Server is shown that is accessible from either PMN as well as IPX. Please refer to GSMA PRD IR.67 [52] for further information.

2.1.5.2 IPX

This is the IP Packet Exchange transit network providing an interconnect capability between PMNs. Please refer to GSMA PRD IR.34 [48] for further information.

2.1.5.3 Diameter Agent

The Diameter Agent defined by IETF RFC 3588 [59] and utilised by GSMA PRD IR.88 [53], is a network element that controls Diameter signalling, enabling the seamless

communication and control of information between network elements within LTE or IMS networks and across network borders. A Diameter Agent reduces the mesh of Diameter connections that negatively impacts network performance, capacity and management.

2.1.5.4 SEG (Security Gateway)

The SEG may be used to originate and terminate secure associations between the eNodeB and the Evolved Packet Core network. IPsec tunnels are established with pre-shared security keys, which can take a number of different formats. IPsec tunnels enforce traffic encryption, for added protection, according to the parameters exchanged between the two parties during tunnel setup. This enables secure communications between the eNodeB and EPC across the S1-MME, S1-U and X2 interfaces.

2.2 VoLTE Interface Description

The main interfaces of the VoLTE architecture are defined by 3GPP and are described below. Further information can be viewed in 3GPP TS 23.002 [1].

2.2.1 LTE-Uu Interface (UE – eNodeB)

LTE-Uu is the radio interface between the eNodeB and the User Equipment. It is defined in 3GPP TS 36.300 [44] series of documents.

2.2.2 S1-MME Interface (UE – MME)

S1-MME is the control plane interface between EUTRAN and MME. The protocols used over this interface are the Non-access stratum protocols (NAS) defined in 3GPP TS 24.301 [10].

2.2.3 S1AP Interface (eNodeB – MME)

S1AP is the S1 application protocol between the EUTRAN and MME and is defined in 3GPP TS 36.413 [45].

2.2.4 S1-U Interface (eNodeB – SGW)

S1-U is the interface between EUTRAN and the S-GW for per-bearer user plane tunnelling and inter-eNodeB path switching during handover. The transport protocol over this interface is GPRS Tunnelling Protocol-User plane (GTPv1-U) defined in 3GPP TS 29.281 [32].

2.2.5 X2 Interface (eNodeB – eNodeB)

X2 is the interface between eNodeB's and is used for X2-based Handover and some Self-Organising Network (SON) capabilities. The signalling protocol (X2 Application Protocol) is defined in 3GPP TS 36.423 [46] and the user plane (GTPv1-U) is defined in 3GPP TS 29.281 [32].

2.2.6 S5 Interface (SGW – PGW)

The S5 interface provides user plane tunnelling and tunnel management between SGW and PGW. The SGW and PGW may be realized as a single network element in which case the S5 interface is not exposed. The control plane protocol (GTPv2-C) is defined in 3GPP TS 29.274 [31] and the user plane protocol (GTPv1-U) is defined in 3GPP TS 29.281 [32].

2.2.7 S6a Interface (HSS – MME)

The interface enables the transfer of subscription and authentication data for authenticating/authorizing user access. The protocol used on the S6a interface is Diameter and is defined in 3GPP TS 29.272 [30].

2.2.8 S9 Interface (H-PCRF – V-PCRF)

The S9 interface provides policy and charging rules and QoS information between the Home PMN and the Visited PMN in order to support PCC roaming related functions. The

protocol used on the S9 interface is Diameter and is defined in 3GPP TS 29.215 [27]. The S9 interface is optional and deployed by bilateral agreement between the Home and Visited Operators. The policy and charging rules for roaming subscribers may be realised by local configuration data in the Visited PCRF. However, for completeness, S9 interaction is shown for all appropriate flows in this document.

2.2.9 S10 Interface (MME – MME)

The S10 interface provides for MME – MME information transfer and is used to enable MME relocation. The protocol used on the S10 interface is GPRS Tunnelling Protocol-Control plane (GTPv2-C) and is defined in 3GPP TS 29.274 [31].

2.2.10 S11 Interface (MME – SGW)

The S11 interface is between the MME and S-GW to support mobility and bearer management. The protocol used on the S11 interface is GPRS Tunnelling Protocol-Control plane (GTPv2-C) and is defined in 3GPP TS 29.274 [31].

2.2.11 Gx Interface (PCRF – PGW)

The Gx interface is between the PCRF and the PGW, allowing the PCRF direct control over the policy enforcement functions of the PGW. The protocol used on the Gx interface is Diameter and is defined in 3GPP TS 29.212 [25].

2.2.12 Rx Interface (PCRF – P-CSCF)

The Rx interface is between the appropriate Application Function (the P-CSCF in the case of VoLTE) and the PCRF allowing the Application Function to request the application of an appropriate policy for a session. The protocol used on the Rx interface is Diameter and is defined in 3GPP TS 29.214 [26].

2.2.13 SGi Interface (PGW – P-CSCF)

The SGi interface is between the PGW and the P-CSCF within the IMS Network. The Gm reference point from the UE to P-CSCF is tunnelled within SGi for VoLTE services. SGi is IP-based and is defined within 3GPP TS 29.061 [22].

2.2.14 Cx Interface (I/S-CSCF – HSS)

The Cx interface is between the I/S CSCF and HSS to enable IMS registration and passing of subscriber data to the S-CSCF. The protocol used on the Cx interface is Diameter and is defined in 3GPP TS 29.228 [28] and 3GPP TS 29.229 [29].

2.2.15 Sh Interface (VoLTE AS – HSS)

The Sh interface is between the VoLTE Application Server and HSS to enable service and subscriber related information to be passed to the Application Server or stored in the HSS. The protocol used on the Sh interface is Diameter and is defined in 3GPP TS 29.328 [33] and 3GPP TS 29.329 [34].

2.2.16 Gm Interface (UE – P-CSCF)

The Gm interface is between the UE and the P-CSCF and enables connectivity between the UE and the IMS network for registration, authentication, encryption, and session control. The protocol used on the Gm interface is SIP/SDP and is defined within 3GPP TS 24.229 [9] and profiled within GSMA PRD IR.92 [54].

2.2.17 Ut Interface (UE – VoLTE AS)

The Ut interface is between the UE and the VoLTE Application Server and allows user configuration of the supplementary services specified for VoLTE service. The protocol used on the Ut interface is XCAP and is defined in 3GPP TS 24.623 [21].

2.2.18 Mx Interface (x-CSCF – IBCF)

The Mx interface is between CSCF and IBCF used for the interworking with another IMS network. The protocols used on the Mx interface are SIP and SDP and are defined in 3GPP TS 24.229 [9].

2.2.19 Mw Interface (x-CSCF – x-CSCF)

The Mx interface is between a x-CSCF and another x-CSCF within the IMS core network (e.g. P-CSCF to I/S-CSCF). The protocols used on the Mw interface are SIP and SDP and are defined in 3GPP TS 24.229 [9].

2.2.20 Mg Interface (xCSCF – MGCF)

The Mg reference point allows the MGCF to forward incoming SIP/SDP messages that the MGCF has interworked from the CS Network to the CSCF. The protocols used on the Mg interface are SIP and SDP and are defined in 3GPP TS 24.229 [9].

2.2.21 Mi Interface (xCSCF – BGCF)

The Mi reference point allows the Serving CSCF to forward the SIP/SDP messages to the Breakout Gateway Control Function for the purpose of MGCF selection for interworking with CS networks. The protocols used on the Mi interface are SIP and SDP and are defined in 3GPP TS 24.229 [9].

2.2.22 Mj Interface (BGCF – MGCF)

The Mj reference point allows the Breakout Gateway Control Function to exchange SIP/SDP messages with the BGCF for the purpose of interworking with CS networks. The protocols used on the Mj interface are SIP and SDP and are defined in 3GPP TS 24.229 [9].

2.2.23 ISC Interface (S-CSCF –TAS)

The ISC interface is between S-CSCF and Telephony Application Server and is used to interact with the MMTel supplementary services implemented on the TAS. The protocol used on the ISC interface is SIP and is defined in 3GPP TS 24.229 [9].

2.2.24 Mr Interface (S-CSCF – MRF)

The Mr interface is between the S-CSCF and the MRF to allow interaction with the media resource for specific supplementary services (e.g. conference call). The protocol used on the Mr interface is SIP/SDP and is defined in 3GPP TS 24.229 [9].

2.2.25 Mr' Interface (TAS – MRF)

The Mr' interface is between the Telephony Application Server and the MRF to allow interaction with the media resource for specific supplementary services (e.g. conference call). The protocol used on the Mr' interface is SIP/SDP and is defined in 3GPP TS 24.229 [9].

2.2.26 Cr Interface (TAS – MRF)

The Cr interface is between the Telephony Application Servers and the MRF. And is used for sending/receiving XML encoded media service requires (Cr) which are served by the MRF. The protocol is defined in 3GPP TS 24.229 [9], 3GPP TS 24.147 [7], and 3GPP TS 24.247 [11].

2.2.27 Mb Interface (media bearer)

Mb interface is the media bearer plane between UEs and network elements that interact with the bearer (e.g. MRF). The protocol is based on symmetric RTP/RTCP over UDP as defined in IETF RFC 3550 [58], IETF RFC 768 [55], and IETF RFC 4961 [62].

2.2.28 Ici Interface (IBCF – IBCF)

Ici interface is between an IBCF and another IBCF or I-CSCF belonging to a different IMS network. The protocols used on the Ici interface are SIP and SDP and are defined in 3GPP TS 29.165 [24].

2.2.29 Izi Interface (TrGW – TrGW)

The Izi interface is between a TrGW and another TrGW or media handling node belonging to a different IMS network. The protocols used on the Izi interface are RTP and MSRP and are defined in 3GPP TS 29.165 [24].

2.3 Related GSMA Permanent Reference Documents

The following GSMA PRD's shown in Table 1 are utilised within the VoLTE architecture.

PRD	Title	Description
IR.34 [48]	Inter-Service Provider IP Backbone Guidelines	The document provides a brief introduction to the requirement for IP interworking and the IPX. It covers the background to the forerunner of the IPX, the GRX.
IR.58 [49]	IMS Profile for Voice over HSPA	This document defines a voice over HSPA IMS profile by profiling a number of HSPA, (Evolved) Packet Core, IMS core, and UE features which are considered essential to launch interoperable IMS based voice on HSPA. This document is based on the IMS Voice and SMS profile described in GSMA PRD IR.92 [54].
IR.64 [50]	IMS Service Centralization and Continuity Guidelines	This document provides guidelines for the centralization of IMS based services and IMS based service continuity for radio devices by listing a number of Evolved Packet Core, IMS core, and User Equipment (UE) features on top of the features defined in IR.92.
IR.65 [51]	IMS Roaming and Interworking Guidelines	This document gives common guidelines for IMS (IP Multimedia Subsystem as specified by 3GPP) inter-operator connections in order to prevent non-interoperable and/or inefficient IMS services & networks. Areas covered in the document are IMS specific issues in roaming and interworking, addressing of users and network elements, routing of traffic, inter-operator related security issues, IP version usage and requirements for inter-PLMN backbone caused by IMS. Document concentrates on the network level issues.
IR.67 [52]	DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers	This document consists of an overview of DNS/ENUM in relation to the successful interworking of MNO services, guidelines for general and MNO service specific configuration of DNS/ENUM servers, and describes GSMA defined processes and procedures relating to configuration and usage of domain names, updates to the GRX Root DNS Server and so on.
IR.88 [53]	LTE Roaming Guidelines	This document presents material about LTE Roaming. The document addresses aspects which are new and incremental to LTE. It recognises that much of the data-roaming infrastructure is reused from GPRS and High-Speed Packet Access (HSPA) Roaming, and for which information and specification is found in other PRDs.

IR.92 [54]	IMS Profile for Voice and SMS	This document defines a voice over IMS profile by listing a number of Evolved Universal Terrestrial Radio Access Network, evolved packet core, IMS core, and UE features that are considered essential to launch interoperable IMS based voice.
AA.80 [74]	IP Packet eXchange Service Agreement	This document defines the terms and conditions for IPX which underpin the Service Level Agreement between the IPX Provider and IPX Client.

Table 1: VoLTE GSMA Permanent Reference Documents

3 VoLTE Implementation - Single PMN

The initial deployments of LTE and indeed VoLTE will likely be self-contained within a single MNO's domain, serving its own subscribers only (no inter-operator VoLTE interconnect or roaming capability).

Interworking between a single operators VoLTE network and its CS network is also within scope.

This section describes the implementation for these scenarios.

3.1 General

The VoLTE architecture for a single PMN deployment is shown in Figure 2.

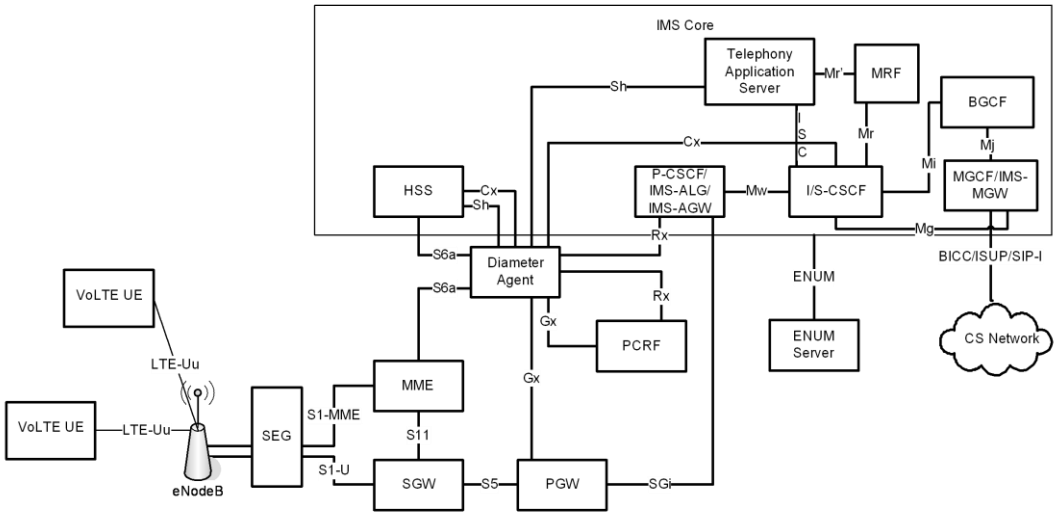

Figure 2: Intra-PMN VoLTE deployment

NOTE: The Gm interface (UE to P-CSCF) is included in the Intra-PMN VoLTE deployment although not shown in the above figure.

NOTE: The Ut interface (UE to VoLTE AS) is included in the VoLTE architecture although not shown in the above figure.

3.2 VoLTE Basic Call Flows

The VoLTE basic call flows are in accordance with 3GPP specifications for E-UTRAN/EPC, IMS, and PCC. Please refer to 3GPP TS 23.401 [6], 3GPP TS 23.228 [5], and 3GPP TS 23.203 [4] respectively for further detailed information.

The following sub-sections define the additional requirements for the VoLTE service. References to specific functionality within GSMA PRDs (e.g. IR.92) and 3GPP specifications will be made within each sub-section.

NOTE: The messages within the call flows within this section are not necessarily performed in sequential order (e.g. there may be no sequential dependency on some SIP <-> Diameter interactions). Reference to the 3GPP specifications for further detailed information is recommended.

3.2.1 VoLTE UE Attachment and IMS Registration

3.2.1.1 General

A VoLTE UE, under LTE coverage, shall automatically perform an LTE Attach followed by an IMS registration for VoLTE, if the network supports VoLTE (for further details on the conditions for IMS registration see section 2.2.1 of GSMA IR.92 [54]). This ensures that the VoLTE UE shall be available for VoLTE services (i.e. incoming calls, outgoing calls and supplementary services), similar to the voice experience in today's CS network deployments.

3.2.1.2 Message Sequence

Figure 3 shows the message sequence for the VoLTE UE Attachment and IMS Registration for the case that the IMS APN is the default APN.

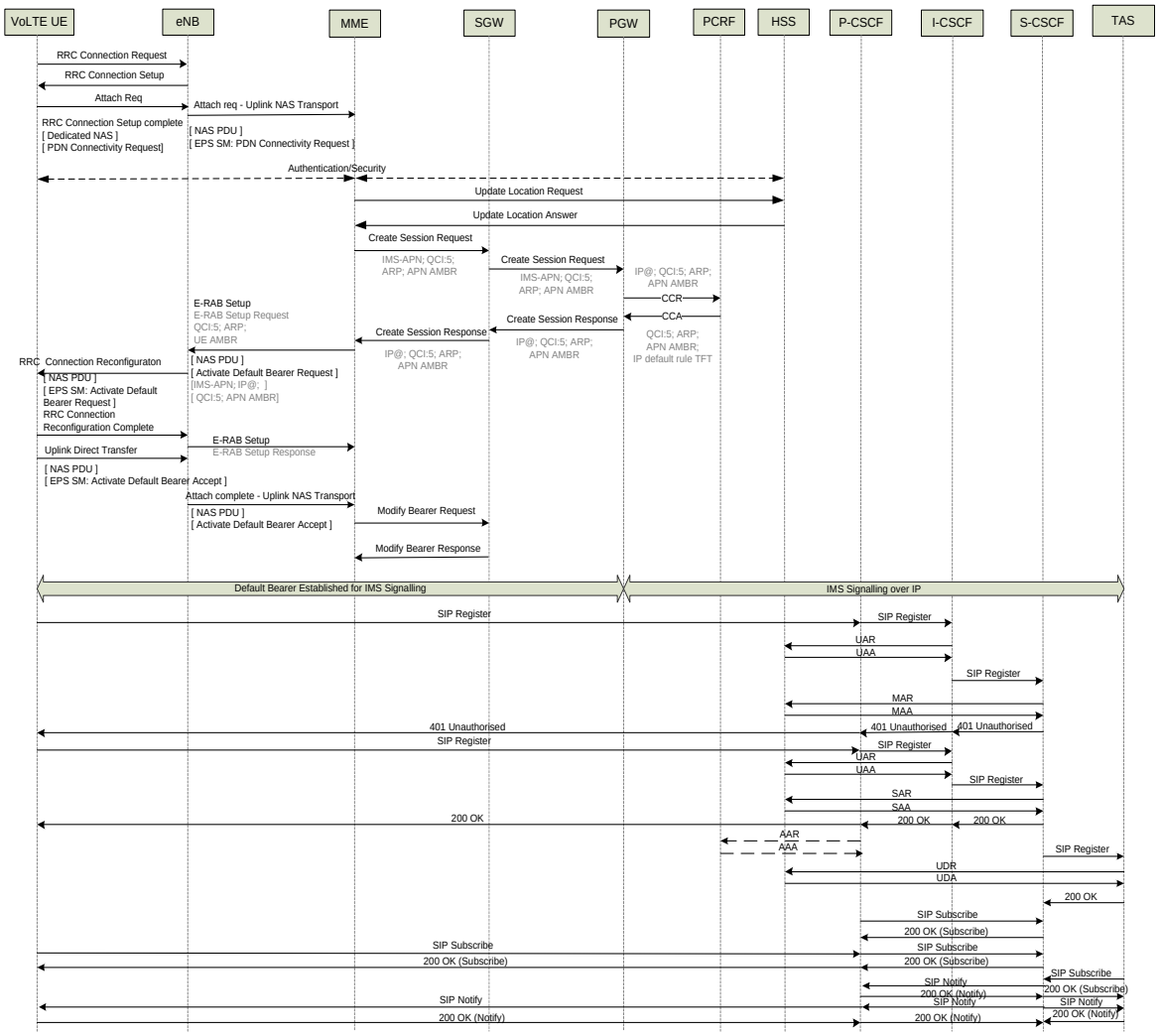

Figure 3: VoLTE UE Attachment and IMS Registration message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

3.2.1.3 Detailed Description

3.2.1.3.1 VoLTE UE Attach

When a VoLTE UE attaches to LTE, it executes the normal attach procedure as defined in 3GPP TS 23.401 [6] section 5.3.2.

LTE Radio capabilities are described in GSMA PRD IR.92 [54]; radio bearer capabilities – section 4.2.1, DRX mode of operation – section 4.2.2, and RLC configuration section 4.3.2.

The VoLTE UE initiates the Attach Request to the eNodeB, with mandatory information including the EPS Attach Type, NAS key set identifier, IMSI, UE network capability, DRX parameters, PDN Type (set to IPv4v6), PCO (P-CSCF IPv4 Address Request, P-CSCF IPv6 Address Request, IPv4 Link MTU Request), Voice Domain Preference and UE's Usage Setting (indicating support of IMS voice), ESM message container, etc.

The eNodeB selects the MME from the RRC parameters and forwards the Attach Request to the MME with the Selected Network and the TAI+ECGI location information of the cell where it received the message.

Authentication and security mechanisms are performed to activate integrity protection and NAS ciphering. The MME shall initiate the Security Mode Command to the UE containing the Selected NAS algorithms, eKSI, ME Identity request, and UE Security Capability. The UE responds with the Security Mode Complete with the NAS-MAC and ME Identity. After the completion, all NAS messages are protected by the NAS security functions (integrity and ciphering).

The MME performs an Update Location to the HSS to retrieve the subscriber profile. Additional information includes the IMSI, MME Identity, ME Identity and MME capabilities and homogenous support for IMS Voice over PS session when being able to determine such support prior performing Update Location. The HSS confirms the Update Location to the MME with the related IMSI and subscriber data containing a PDN subscription context with a subscribed QoS profile and subscribed APN-AMBR (Aggregate Maximum Bit Rate).

The UE shall not provide the IMS APN in the initial attach (see clause 4.3.1 of IR.92). The default APN configured in the HSS can be set as the IMS-APN, and the HSS returns the IMS-APN name for establishment of the default bearer. The APN-OI information is inserted by the MME.

If the IMS APN is not configured as default APN, and the UE has determined the need to establish a PDN connection to the IMS APN, then the UE must establish a PDN Connection to the IMS APN in a subsequent PDN connection request as specified in clause 4.3.1 in IR.92.

The MME initiates a Create Session Bearer request to the SGW to create a default bearer for VoLTE IMS signalling. This message contains the IMSI, MSISDN, IMS-APN, QCI=5, ARP value, the APN-AMBR, user location information (e.g. TAI+ECGI), UE Time Zone, RAT-type (EUTRAN), PCO, etc. The SGW creates a new entry in the EPS Bearer table, allocating a relevant TEID for the control plane and the user plane, which enables it to route GTP control plane traffic between the MME and the PGW, and forwards the request to the PGW.

The PGW allocates an IP Address (which can be IPv4 or IPv6) for the UE and utilises dynamic PCC to initiate a Credit Control Request to the PCRF to obtain the default PCC rules for the default bearer to be used for IMS signalling. Included in the message are the IMSI, UE IP Address, default bearer QoS parameters (i.e. QCI=5, ARP, APN-AMBR), user

location information, time zone information, RAT type (EUTRAN), etc. The PCRF binds the related policy rules to the IP Address of the default bearer, and responds to the PGW with the default TFT (traffic flow template) and potentially modified QoS parameters. In the message to the PGW, the PCRF shall also subscribe to modifications related to the default bearer in the PGW (e.g. RELEASE_OF_BEARER, DEFAULT_EPS_BEARER_QOS_CHANGE, etc.).

The PGW creates a new entry in the EPS Bearer table, allocating relevant TEID for the control plane and the user plane, which enables it to route user plane data between the SGW and the IMS network with the related policy rules obtained from the PCRF applied. The PGW sends a Create Session Response to the SGW with the IP Address for the UE, QoS parameters, PCO, relevant TEID's for the GTP control plane and GTP user plane, etc. The PGW maps the IMS-APN received in the request to a pre-configured IMS P-CSCF IP address and inserts this into the PCO as described in GSMA PRD IR.92 [54] section 4.4. The SGW returns the Create Session Response to the MME.

The MME sends an Attach Accept to the eNodeB with the IMS-APN, IP Address for the UE, QoS parameters, PCO, IMS Voice over PS supported indication, TAI list, ESM message container, etc. The eNodeB communicates with the UE to update the RRC configuration and includes the information received from the core network as part of the create session request.

The UE sends the Attach Complete message to the eNodeB, which forwards to the MME. At this time, the UE is capable of sending uplink packets. The MME initiates a Modify Bearer Request to the SGW including the EPS Bearer Identity, eNodeB address, and eNodeB TEID. The SGW acknowledges the request to the MME and is capable of sending downlink packets.

At this stage, the VoLTE UE is attached to the network via a default bearer that is established for IMS Signalling.

3.2.1.3.2 VoLTE UE Initial IMS Registration

When a VoLTE UE performs the IMS registration, it executes the procedures as defined in 3GPP TS 23.228 [5] section 5.2.

GSMA PRD IR.92 [54] provides additional profiling of IMS Registration procedures – section 2.2.1, IMS authentication - section 2.2.2, IMS Addressing – section 2.2.3.

The VoLTE UE shall not use SIGCOMP as defined in GSMA PRD IR.92 [54] section 2.2.7.

Where an ISIM is present on the UICC, ISIM based authentication and IMS-AKA as described in GSMA PRD IR.92 [54] section 2.2.2, shall be used. The ISIM application shall be preconfigured with the related IMS Identities as defined in 3GPP TS 31.103 [37].

Where no ISIM is present on the UICC, USIM based authentication and IMS-AKA as described in GSMA PRD IR.92 [54] section 2.2.2 shall be used. The UE shall generate the Private User Identity and the Public User Identity from the IMSI as defined in 3GPP TS 23.003 [2].

The VoLTE UE initiates a SIP REGISTER to the P-CSCF, using the P-CSCF IP Address that was made available during the LTE Attach. The registration request contains:-

- Within the Contact header, the IMS Communication Service Identifier's (ICSI) for IMS Multimedia Telephony:-
  - urn:urn-7:3gpp-service.ims.icsi.mmtel
  - “+sip.instance” containing an IMEI URN
- The feature tag for SMS over IP:- +g.3gpp.smsip

- The IMS Public User Identity (as derived above) in one of the forms below:-
  - Alphanumeric SIP-URI: e.g. user@example.com
  - MSISDN as a SIP-URI: e.g. sip:+447700900123@example.com;user=phone
  - MSISDN as Tel-URI: e.g. tel:+447700900123
- The IMS Private User Identity as an NAI: e.g. username@realm
- P-Access-Network-Info with:-
  - access-type= 3GPP-E-UTRAN-FDD or 3GPP-E-UTRAN-TDD
  - UTRAN-cell-id-3gpp parameter
- Request-URI set to the SIP-URI of the domain name of the home network
- Related headers for IMS AKA parameters
- etc.

The P-CSCF receives the SIP REGISTER request from the UE and inserts a Path header with a SIP-URI identifying the P-CSCF for routing, a P-Charging-Vector header with the icid-value, a P-Visited-Network-ID to identify the P-CSCF's network domain and forwards the request to the I-CSCF. The I-CSCF name is determined via a DNS query or may be pre-configured within the P-CSCF.

The I-CSCF queries the HSS using the User Authorization Request for authorization and obtaining the S-CSCF name for the Public User Identity. The HSS validates that the Public User Identity and Private User Identity are valid and not barred. If there is not an S-CSCF associated to the Public User Identity, the HSS may return information related to the S-CSCF capabilities allowing the I-CSCF to select an appropriate S-CSCF. Once the S-CSCF is identified, the I-CSCF forwards the SIP REGISTER request to the S-CSCF.

The S-CSCF identifies that the SIP REGISTER is part of an initial IMS registration with IMS-AKA related security. The S-CSCF initiates a Multimedia Authentication Request to the HSS to retrieve the authentication vectors to perform IMS-AKA security. The HSS stores the related S-CSCF name for the Public User Identity being registered and returns the authentication vectors to the S-CSCF.

Upon receipt of the IMS AKA authentication vectors, the S-CSCF stores the XRES and replies to the SIP REGISTER request with a 401 Unauthorised response indicating that AKAv1-MD5 is the security mechanism to be used. The RAND and AUTN parameters, Integrity Key and Cipher Key are also included.

The P-CSCF removes the Cipher Key and Integrity Key from the 401 Unauthorised response and binds these to the Private User Identity with a set of temporary security associations for the result of the challenge. The P-CSCF then forwards the response to the UE.

The UE extracts the RAND and AUTN parameters, calculates the RES, and derives the Cipher Key and Integrity Key from the RAND. The UE creates a temporary set of security associations based on parameters received from the P-CSCF (IPSec), and sends a new REGISTER request to the P-CSCF with a populated Authorization header containing the RES indicating that the message is integrity protected.

The P-CSCF checks the temporary security associations, and verifies the security related information received from the UE. This P-CSCF forwards the SIP REGISTER request to the I-CSCF with the RES included.

The I-CSCF uses the User Authorization Request message to retrieve the S-CSCF name stored within the HSS, and forwards the request to the relevant S-CSCF.

The S-CSCF checks whether the RES received in the SIP REGISTER and the XRES previously stored match. The S-CSCF then performs the Server Assignment Request procedure to the HSS to download the relevant user profile and register the VoLTE UE. The S-CSCF stores the route header of the P-CSCF and binds this to the contact address of the VoLTE UE, this is used for routing to the VoLTE UE in future messages. Parameters of the P-Charging-Vector header are stored, and the S-CSCF sends a 200 OK response to the I-CSCF, including the user's display name (retrieved from the user profile in the HSS) within the P-Associated-URI, which forwards the message to the P-CSCF.

On receipt of the 200 OK from the I-CSCF, the P-CSCF changes the temporary set of security associations to a newly established set of security associations. It protects the 200 OK with these associations and sends the 200 OK to the VoLTE UE. All future messages sent to the UE will be protected using the security associations.

Optionally, the P-CSCF sends an AAR message to the PCRF to perform application binding to the default bearer (i.e. the P-CSCF is requesting to be informed in the event of the default bearer being lost/disconnected in order to trigger an IMS de-registration). The PCRF performs the binding and responds with a AAA message to the P-CSCF. Note that if this message is not sent, then IMS relies on other mechanisms to detect loss of the underlying default bearer, i.e., loss of connectivity (e.g. timeouts on trying to signal to the UE for an incoming call or the UE registers in the IMS with a new IP address).

On receipt of the 200 OK, the UE changes the temporary security association to a newly established set of security associations that will be used for further messages to the P-CSCF.

The VoLTE UE is now registered with the IMS network for VoLTE services, with SIP signalling being transported over the default EPC bearer.

The S-CSCF sends a third party SIP REGISTER to the VoLTE AS, as configured in the initial filter criteria (iFC) within the subscriber profile. The TAS may use the User Data Request procedure to read VoLTE data stored in the HSS.

The VoLTE UE, P-CSCF and TAS shall subscriber to the registration event package using the SIP SUBSCRIBE message, in order to be notified on any change of registration state for the public user identity. In turn, the S-CSCF shall send a SIP NOTIFY to the subscribing entities informing them of the active registration status.

3.2.2 VoLTE UE Initiated Detach and IMS Deregistration

3.2.2.1 General

A VoLTE UE shall automatically deregister from IMS before performing an LTE Detach, if the UE is not moving to another access technology that supports Voice over IMS. This ensures that the VoLTE subscriber can have any terminating services routed accordingly (e.g. terminating call being routed directly to voicemail) rather than a failed attempt to route the call to the VoLTE UE. This behaviour is similar to the voice experience in today's CS network deployments.

3.2.2.2 Message Sequence

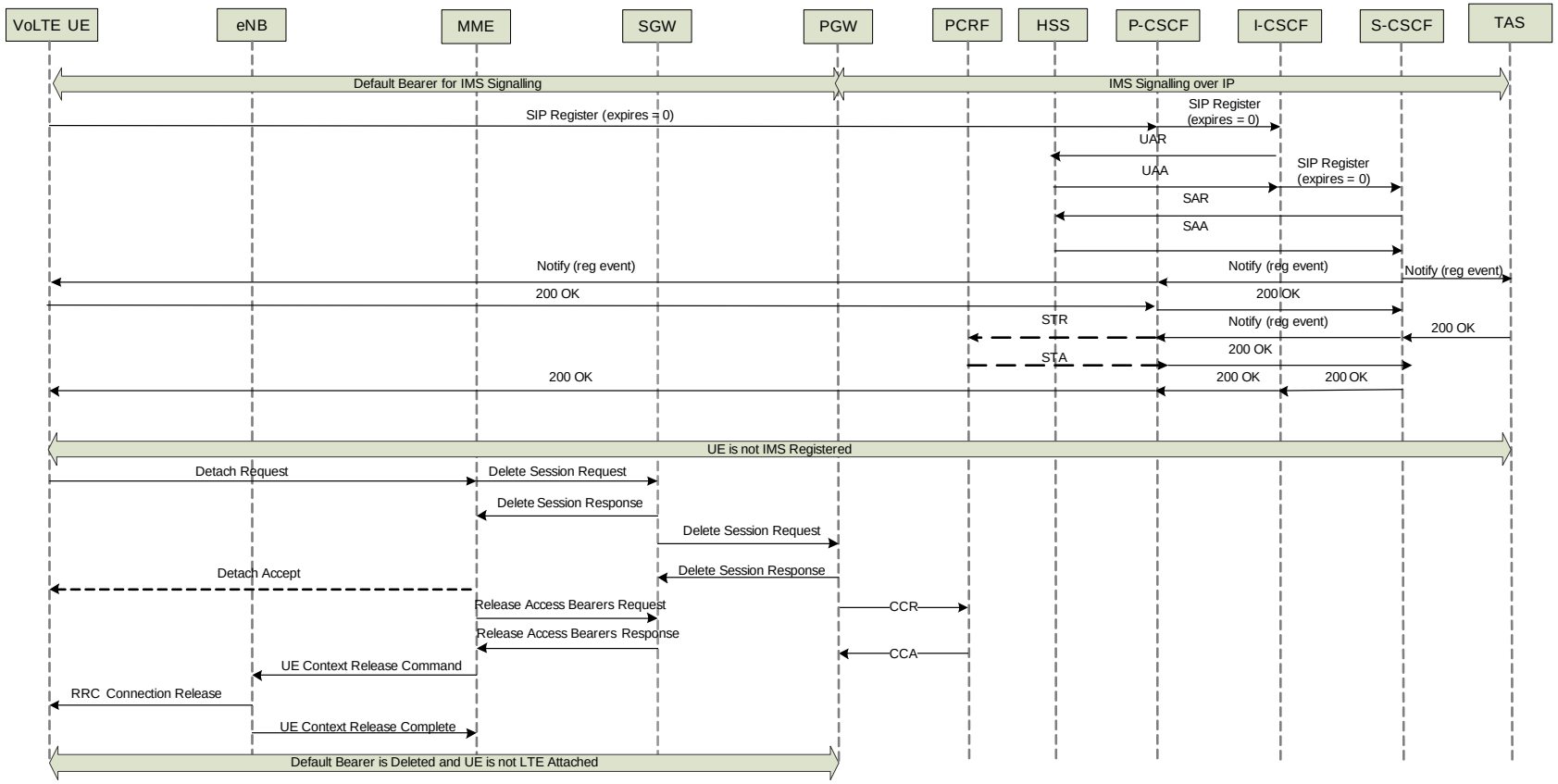

Figure 4: VoLTE UE Initiated Detach and IMS Deregistration message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

NOTE: The I-CSCF is shown in the signalling path in figure 4. This is optional and the I-CSCF may also be omitted.

3.2.2.3 Detailed Description

3.2.2.3.1 IMS Deregistration

When a VoLTE UE performs the IMS deregistration, it executes the procedures as defined in 3GPP TS 23.228 [5] section 5.3.

The VoLTE initiates a SIP REGISTER message towards the P-CSCF including the Public User Identity, Private User Identity, the Request-URI with the SIP-URI of the domain name of the home network, the P-Access-Network-Info, etc. The registration expiration interval timer shall be set to zero.

The P-CSCF forwards the SIP-REGISTER to the I-CSCF.

The I-CSCF uses the User Authorization Request message to retrieve the S-CSCF name stored within the HSS, and forwards the request to the relevant S-CSCF.

Upon receiving the SIP REGISTER (expiration time of zero), the S-CSCF shall initiate the Server Assignment Request procedure to the HSS, indicating User Deregistration Store Server Name. The HSS shall keep the S-CSCF name associated to the public user identity for future use and to enable unregistered services to be applied (e.g. routing of a terminating voice call to voicemail). Note that if the HSS does not keep the S-CSCF name, then the HSS would need to assign a S-CSCF to handle a new terminating INVITE message.

The S-CSCF shall send a SIP NOTIFY to the VoLTE UE, TAS and P-CSCF to notify them of the change of the registration state (the UE, TAS and P-CSCF having previously subscribed to the reg-event package). The VoLTE UE / TAS / P-CSCF respond with a 200 OK (NOTIFY). If application session binding had been performed at registration, the P-CSCF (on being notified of the change of registration state) sends a STR message to the PCRF to remove the session binding to underlying default bearer. The P-CSCF shall remove the security associations that were established between the P-CSCF and the UE.

The S-CSCF shall send a 200 OK (REGISTER) to acknowledge the de-registration.

The P-CSCF shall forward the 200 OK (REGISTER) to the UE.

On receiving the 200 OK responses, the UE shall remove all the registration details for the Public User Identity and delete the stored security associations. The UE shall consider the subscription to the registration event package as cancelled.

The VoLTE UE is now de-registered from the IMS network for VoLTE services, no further SIP signalling is being transported over the default EPC bearer.

3.2.2.3.2 VoLTE UE Detach

When a VoLTE UE detaches from LTE, it executes the normal detach procedure as defined in 3GPP TS 23.401 [6] section 5.3.8.

The VoLTE UE initiates a Detach Request to the MME, via the eNodeB which includes the location information (TAI+ECGI) of the cell the VoLTE UE is using.

The MME initiates a Delete Session Request to the SGW, including the ECGI and timestamp, to deactivate the default bearer. The SGW releases the default bearer context information and sends the Delete Session Response to the MME.

The SGW initiates a Delete Session Request to the PGW including the ECGI , Time Zone and Timestamp. The PGW acknowledges with the Delete Session Response to the SGW.

The PGW initiates a Credit Control Request to the PCRF to indicate that the default bearer is released. The user location information (i.e. ECGI) and the Time Zone information are included.

The MME utilises the Release Access Bearer Request to release the connection between the SGW and the eNodeB.

The Detach Accept is sent by the MME, and the radio resources between the UE and the eNodeB are removed.

At this stage, the VoLTE UE is not attached to the network and the default bearer that was established for IMS Signalling is removed.

3.2.3 Basic VoLTE UE to VoLTE UE Call Establishment – Originating Side

3.2.3.1 General

A VoLTE UE, shall perform call establishment by using the IMS network. The IMS Signalling shall be sent over the default bearer, and a new dedicated bearer shall be dynamically established for the voice traffic.

3.2.3.2 Message Sequence

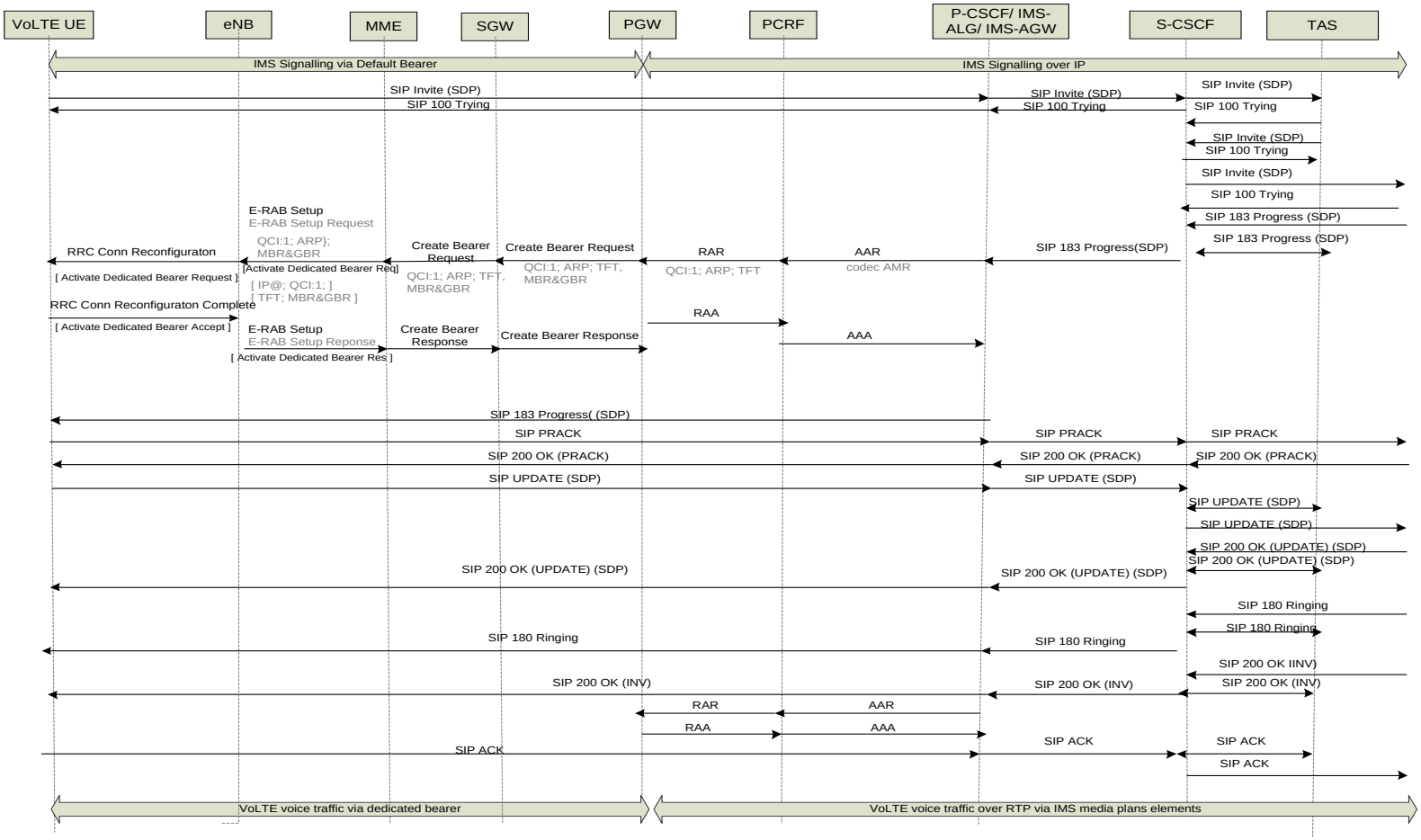

Figure 5: Basic VoLTE UE to VoLTE UE Call Establishment - Originating Side message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

NOTE: The figure shows the PCRF being invoked only once on receipt of the of the SDP answer (uplink & downlink configuration); this is sufficient if the UE is using preconditions as mandated in GSMA IR.92 [54]. It is also possible to invoke the PCRF twice, i.e. on receipt of both the SDP Offer (downlink configuration) and SDP Answer (uplink configuration). Both options are valid - – see 3GPP TS 29.213 ([79]) annex B.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [70] and described in 3GPP TS 24.229 ([9]) clauses 5.1.3 and 6.1.2.

NOTE: The PRACK and 200 OK (PRACK) messages also traverse through the AS but this is not shown.

3.2.3.3 Detailed Description

When a VoLTE UE originates a voice call from LTE, it executes the normal mobile origination procedure as defined in 3GPP TS 23.228 [5] section 5.6.2.

The VoLTE UE initiates a SIP INVITE request, containing the SDP offer with IMS media capabilities as specified in GSMA PRD IR.92 [54] section 3. The SDP offer shall contain the AMR Narrowband codec, and it is recommended that the AMR Wideband codec is included to provide support for HD Voice and shall indicate that local preconditions for QoS are desired but not yet met, using the segmented status type (as defined in RFC 3312 [70]) and that the media stream is set to inactive as described in 3GPP TS 24.229 ([9]) clause 6.1.2 The desired QOS for the remote end are set to “none” as the originating UE is unaware of the QOS requirements at the terminating side. The request is sent to the P-CSCF that was discovered during the registration procedure. The INVITE request contains:-

- Within the Contact header and the P-Preferred-Service header, the IMS Communication Service Identifier's (ICSI) for IMS Multimedia Telephony:-
  - urn:urn-7:3gpp-service.ims.icsi.mmtel
- The IMS Public User Identity of the calling-party in one of the forms below:-
  - Alphanumeric SIP-URI: e.g. user@example.com
  - MSISDN as a SIP-URI: e.g. sip:+447700900123@example.com;user=phone
  - MSISDN as Tel-URI: e.g. tel:+447700900123
- P-Access-Network-Info with:-
  - access-type= 3GPP-E-UTRAN-FDD or 3GPP-E-UTRAN-TDD
  - UTRAN-cell-id-3gpp parameter
- Request-URI set to the SIP-URI or tel-URI of the called-party.
- Within the Supported header, the P-Early-Media, 100rel& precondition option tags are present (see IETF RFC 5009 [69], IETF RFC 3312 [70] and IETF RFC 3262 [71]). The timer option tag may also be present (RFC 4028 [80]) when SIP keep-alives are supported.
- etc.

The P-CSCF adds the P-Charging-Vector header and forwards the SIP INVITE to the S-CSCF that was identified during the registration process.

If an IMS-ALG/AGW is deployed, then the P-CSCF will also invoke the IMS-AGW over the Iq reference point (see 3GPP TS 23.334 [73]) to provide appropriate resources in the media plane. The IMS-AGW is an IP-IP GW and serves as a border element in the media plane in an IMS network at the access side. .

The P-CSCF forwards the SIP INVITE to the S-CSCF The offered SDP address shall reflect the media pin-hole created in the IMS-AGW if applicable.

The S-CSCF receives the SIP INVITE from the P-CSCF, and invokes any VoLTE services as triggered by the initial filter criteria within the subscriber profile that was received during the IMS Registration. The S-CSCF checks the P-Preferred-Service header in the SIP INVITE (e.g. MMTel ICSI) and verifies that the user is authorised for the service by validating against the subscribed services that were retrieved in the service profile during IMS Registration (Core Network Service Authorisation – Service ID). If the MMTel ICSI is not in the subscribed services, the INVITE request shall be rejected (403 Forbidden). If validated, the S-CSCF then adds the ICSI into the P-Asserted-Service header, and removes the P-Preferred-Service header. Due to service logic within the user profile, and the identification of the call as a VoLTE call (i.e. MMTel ICSI), the S-CSCF shall route the SIP INVITE to the TAS at this point to invoke VoLTE supplementary services. The TAS invokes any supplementary service logic and routes the SIP INVITE to the S-CSCF. The S-CSCF determines that the Called-Party is within the home network (i.e. ENUM/DNS lookup/internal configuration) and routes the SIP INVITE to the I-CSCF to determine the terminating S-CSCF of the Called-Party (see section 3.2.4).

The called party's VoLTE UE will return an SDP answer in a SIP 183 Progress message. The SDP answer should contain only one codec and indicates that preconditions are also desired but not yet met at the terminating end and that a confirmation should be sent when QOS preconditions have been met at the originating side and that the media stream is inactive. This message is received by the S-CSCF and forwarded to the P-CSCF. The P-CSCF uses the SDP answer to configure the IMS-AGW if deployed.

In addition, the P-CSCF analyses the SDP in the SDP Answer and sends the Authorize/Authenticate-Request message to the PCRF with the related service information (IP address, port numbers, information on media-type). The PCRF authorises the request and associates the service information with the stored subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information. The PCRF identifies the affected IP-CAN session (e.g. default bearer) that has been established during the LTE Attach procedure, and initiates a Re-Auth-Request to the PGW to initiate the creation of a dedicated bearer for voice with the related QoS parameters (QCI=1, ARP) and the related traffic flow template. The PCRF shall also subscribe to modifications related to the dedicated bearer in the PGW (e.g. INDICATION_OF_RELEASE_OF_BEARER, etc.).

The PGW acknowledges the Re-Auth-Request to the PCRF, which then acknowledges the Authorize/Authenticate-Request message sent from the P-CSCF. At this point the IMS SIP session and the dedicated bearer used for voice are bound together via PCC.

The PGW sends the Create Bearer Request to the SGW to create the dedicated bearer for VoLTE media. This message contains the dedicated bearer identity, Linked Bearer Identity to identify the associated default bearer, the traffic flow template, and the associated QoS parameters (QCI=1, ARP, GBR and MBR), etc. The SGW sends the request to the MME.

The MME sends a Bearer Setup Request message to the eNodeB with the dedicated bearer identity, Linked Bearer Identity, the traffic flow template, and the associated QoS parameters in order to activate the dedicated bearer for voice traffic.

The eNodeB maps the QoS parameters to those required for the radio bearer, and then signals a RRC Connection Reconfiguration to the UE. The UE stores the dedicated bearer

identity and links the dedicated bearer to the default bearer indicated by the Linked EPS Bearer Identity. The UE binds the TFT and associated QoS parameters to the dedicated bearer, and acknowledges the request to the eNodeB, which then acknowledges the Bearer Request Setup to the MME.

The MME sends the Create Bearer Response message to the SGW to acknowledge the bearer activation. The message includes the dedicated bearer identity and User Location Information (ECGI). This is then forwarded to the PGW.

The P-CSCF forwards the SIP 183 Progress response to the VoLTE UE. This message shall also utilize 100rel and the originating UE shall generate a PRACK which is transited to the terminating side of the call with an associated 200 OK (PRACK) being received.

The VoLTE UE shall reserve internal resources to reflect the SDP answer and shall confirm resource reservation by sending a SIP UPDATE message with a new SDP Offer confirming the selected codec, that local preconditions have been met at the originating end (due to the establishment of the dedicated bearer) and that the media stream is now set to active. The UPDATE message is forwarded via the P-CSCF and S-CSCF to the terminating leg of the call. Note that if the SDP Answer in the 183 Progress message contained more than one voice codec, then the UE would ensure only a single codec from that multiple list was included in the new Offer in the UPDATE message (as described in clause 6.1.2. of 3GPP TS 24.229 ([9]).

The 200 OK (UPDATE) response is received from the terminating leg of the call containing the SDP answer containing a single voice codec and confirming that preconditions are also met at the terminating side and that the media stream is active. This message is passed onto the originating UE via the S-CSCF and P-CSCF.

As preconditions have been met, the terminating UE is now alerted and shall send a SIP 180 (Ringing) response that is received by the S-CSCF and onto the P-CSCF and originating UE.

The P-Early-Media header is not present in the SIP 180 Ringing message and so the UE will generate local ring tone to the subscriber. This message shall not utilize 100rel as there is no SDP within the message.

When the called party's VoLTE UE has answered the call, it sends a 200 OK to the calling party VoLTE UE. This is received by the S-CSCF and forwarded to the P-CSCF. The P-CSCF invokes the PCRF with an AAA message to enable both the uplink and downlink of the dedicated bearer. In turn the PCRF invokes the P-GW with a RAR message to enable the media flows at the P-GW. The P-CSCF (IMS-ALG) invokes the IMS-AGW (if deployed) to ensure that duplex media can be conveyed via IMS-AGW at this point.

The P-CSCF forwards the SIP 200 OK (INVITE) to the VoLTE UE.

The VoLTE UE receives the 200 OK, and sends a SIP ACK message to acknowledge that the call has been established.

At this stage, the VoLTE UE has a call established with voice traffic sent over the dedicated bearer and via the IMS-AGW. The IMS Signalling is sent over the default bearer. Support of Robust Header Compression is mandated and described in GSMA PRD IR.92 [54] section 4.1.

3.2.4 Basic VoLTE UE to VoLTE UE Call Establishment – Terminating Side

3.2.4.1 General

A VoLTE UE, shall receive a call via IMS network. The IMS Signalling shall be sent over the default bearer, and a new dedicated bearer is established by the network for the voice traffic.

3.2.4.2 Message Sequence

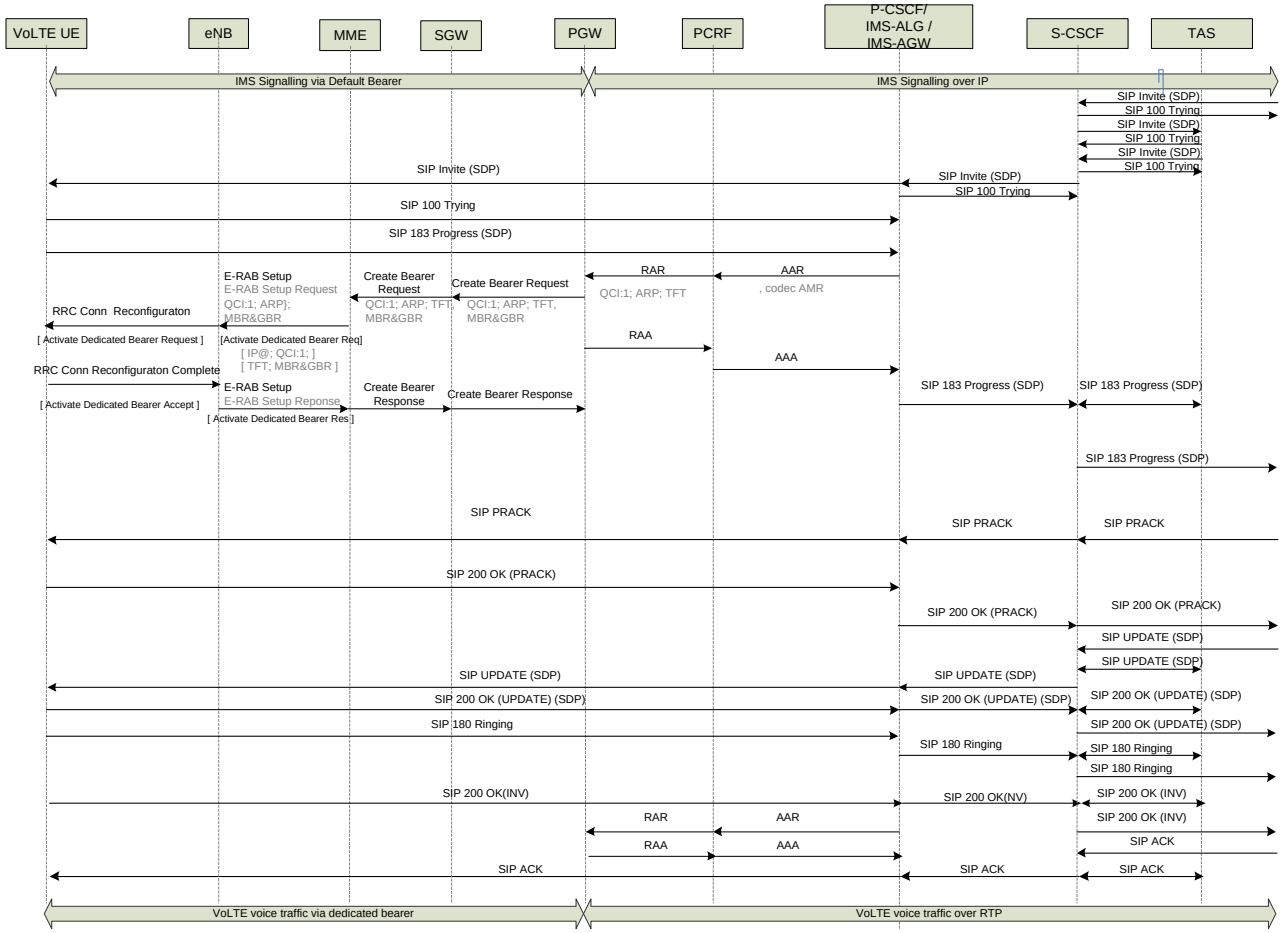

Figure 6: Basic VoLTE UE to VoLTE UE Call Establishment – Terminating Side message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

NOTE: The figure shows the PCRF being invoked only once on receipt of the of the SDP answer (uplink & downlink configuration); this is sufficient if the UE is using preconditions as mandated in GSMA IR.92 [54]. It is also possible to invoke the PCRF twice, i.e. on receipt of both the SDP Offer (downlink configuration) and SDP Answer (uplink configuration). Both options are valid - see 3GPP TS 29.213 ([79]) annex B.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [70] and described in 3GPP TS 24.229 ([9]) clauses 5.1.4 and 6.1.2.

NOTE: The PRACK and 200 OK (PRACK) messages also traverse through the AS but this is not shown.

3.2.4.3 Detailed Description

When a VoLTE UE receives an incoming voice call request, it executes the normal mobile termination procedure as defined in 3GPP TS 23.228 [5] section 5.7.2.

The S-CSCF receives a SIP INVITE containing an SDP Offer with IMS media capabilities as specified in GSMA PRD IR.92 [54] section 3. The SDP offer shall contain the AMR Narrowband codec, and optionally the AMR Wideband codec. The SDP indicates that preconditions are applicable and that QOS preconditions are desired but not yet reserved at the originating side. The media stream is set to inactive.

The S-CSCF invokes any VoLTE services as triggered by the initial filter criteria within the subscriber profile that was received during the IMS Registration. The S-CSCF shall route the SIP INVITE to the TAS at this point to invoke VoLTE supplementary services. The TAS invokes any supplementary service logic and routes the SIP INVITE to the S-CSCF. The S-CSCF routes the SIP INVITE to the terminating P-CSCF that was associated to the subscriber during IMS registration.

If an IMS-ALG/AGW is deployed, then the P-CSCF (IMS-ALG) invokes the IMS-AGW to reserve resources for the media connection. In this event, the SDP address in the INVITE is over-written to reflect the media pin-hole created on the IMS-AGW.

The P-CSCF forwards the SIP INVITE to the VoLTE UE. When the VoLTE UE receives the SIP INVITE it shall allocate resources for the call and select one voice codec from the SDP Offer (as described in section 6.1.3 of 3GPP TS 24.229 ([9]). The UE shall send a SIP 183 Progress response containing the SDP Answer. The message shall indicate that 100rel is required. The SDP Answer indicates that QOS preconditions are desired but not yet met at the terminating side of the call. In addition, the SDP shall indicate that the originating side should confirm when its local QOS preconditions have been met.

On receipt of the SIP 183 Progress message, the P-CSCF updates the IMS-AGW if applicable with the SDP answer from the UE and sends the Authorize/Authenticate-Request message to the PCRF with the related updated service information (IP address, port numbers, information on media-type). The PCRF authorises the request and associates the service information to the stored subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information. The PCRF identifies the affected IP-CAN session (e.g. default bearer) that has been established during the LTE Attach procedure, and initiates a Re-Auth-Request to the PGW to initiate the creation of a dedicated bearer for voice with the related QoS parameters (QCI=1, ARP) and the related traffic flow template. The PCRF shall also subscribe to modifications related to

the dedicated bearer in the PGW (e.g. LOSS_OF_BEARER, INDICATION_OF_RELEASE_OF_BEARER, etc.).

The PGW acknowledges the Re-Auth-Request to the PCRF, which then acknowledges the Authorize/Authenticate-Request message sent from the P-CSCF. At this point the IMS SIP session and the dedicated bearer used for voice are bound together via PCC.

The PGW sends the Create Bearer Request to the SGW to create the dedicated bearer for VoLTE media. This message contains the dedicated bearer identity, Linked Bearer Identity to identify the associated default bearer, the traffic flow template, and the associated QoS parameters (QCI=1, ARP, GBR and MBR), etc. The SGW sends the request to the MME.

The MME sends a Bearer Setup Request message to the eNodeB with the dedicated bearer identity, Linked Bearer Identity, the traffic flow template, and the associated QoS parameters in order to activate the dedicated bearer for voice traffic.

The eNodeB maps the QoS parameters to those required for the radio bearer, and then signals a RRC Connection Reconfiguration to the UE. The UE stores the dedicated bearer identity and links the dedicated bearer to the default bearer indicated by the Linked EPS Bearer Identity. The UE binds the TFT and associated QoS parameters to the dedicated bearer, and acknowledges the request to the eNodeB, which then acknowledges the Bearer Request Setup to the MME.

The MME sends the Create Bearer Response message to the SGW to acknowledge the bearer activation. The message includes the dedicated bearer identity and User Location Information (ECGI). This is then forwarded to the PGW.

On receipt of the AAA response from the PCRF, the P-CSCF will convey the SIP 183 Progress (SDP) message to the S-CSCF. The contained SDP reflects the address of the media pin hole in the IMS-AGW if applicable.

The PRACK message is transited from the originating side of the call.

The terminating side sends a 200 OK (PRACK) in response to the PRACK.

A second SDP Offer is now received from the originating leg of the call in a SIP UPDATE message indicating that preconditions have been met at the originating side and that the media stream is active.

The UPDATE is passed to the UE via the S-CSCF and P-CSCF. The UE sends a 200 OK (UPDATE) response containing a SDP Answer confirming that QOS preconditions are also satisfied at the terminating side (due to the establishment of the dedicated bearer) and that the media stream is active. The 200 OK (UPDATE) message is sent to the originating leg of the call via the P-CSCF and S-CSCF.

As preconditions are now met at both ends, the UE will alert the user and send a SIP 180 Ringing response. This message does not contain SDP and so will not utilize 100rel. The P-Early-Media header is not present in this message.

The SIP 180 Ringing response is sent to the originating leg via the P-CSCF and S-CSCF.

When the call is answered, the VoLTE UE shall send a SIP 200 OK (INVITE) message to the P-CSCF.

The P-CSCF invokes the PCRF with an AAA message to enable both the uplink and downlink of the dedicated bearer to reflect the SDP exchange. In turn the PCRF invokes the P-GW with a RAR message to enable the media flows at the P-GW.

The P-CSCF (IMS-ALG) shall also invoke the IMS-AGW to if applicable ensure that duplex media can traverse the IMS-AGW.

The 200 OK is forwarded to the S-CSCF and then to the originating side of the call.

At this stage, the VoLTE UE has a call established with voice traffic sent over the dedicated bearer via the IMS-AGW. The IMS Signalling is sent over the default bearer. Support of Robust Header Compression is mandated and described in GSMA PRD IR.92 [54] section 4.1.

3.2.5 Basic VoLTE UE to VoLTE UE Call Clearing - Initiated

3.2.5.1 General

A VoLTE UE, shall perform call clearing by using the IMS network. The IMS Signalling shall be sent over the default bearer, and the dedicated bearer that was dynamically established for the voice traffic shall be removed.

3.2.5.2 Message Sequence

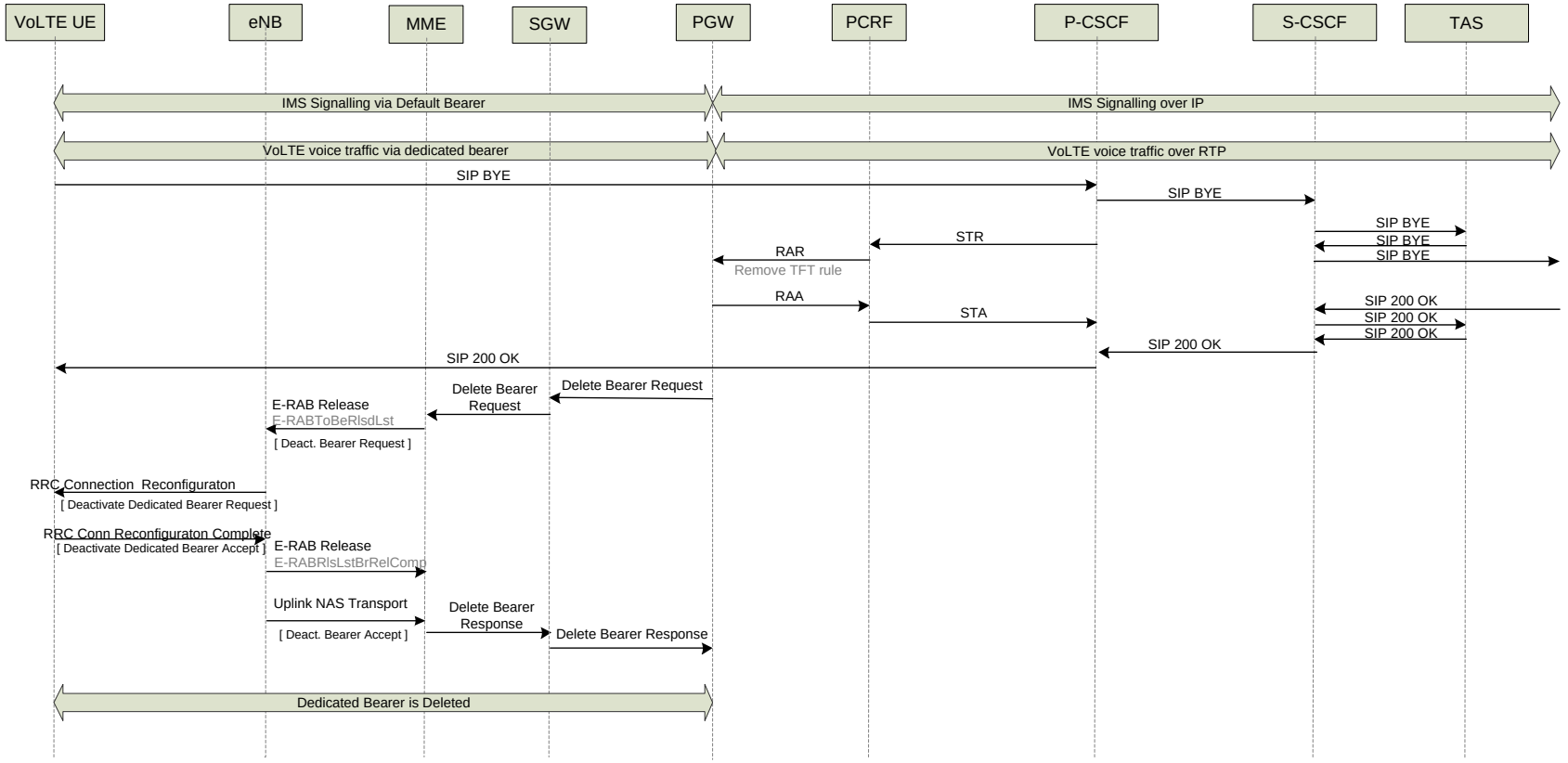

Figure 7: Basic VoLTE UE to VoLTE UE Call Clearing – Initiated message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

3.2.5.3 Detailed Description

When a VoLTE UE terminates a voice call from LTE, it executes the normal mobile termination procedure as defined in 3GPP TS 23.228 [5] section 5.10.

The VoLTE UE sends a SIP BYE message to the P-CSCF. If applicable, the P-CSCF (IMS-ALG) releases the resources in the IMS-AGW.

The P-CSCF also initiates a Session Termination Request to the PCRF to initiate the process of removing the dedicated bearer that was established for the voice traffic. The PCRF removes the binding between the stored subscription information and the IMS service information, and initiates a Re-Auth-Request to the PGW to remove the dedicated bearer for voice with the related QoS parameters (QCI=1, ARP) and the related traffic flow template.

The Delete Bearer Request, Bearer Release Request, and RRC Reconfiguration Request are utilised to remove the dedicated bearer utilised for voice traffic.

The P-CSCF forwards the SIP BYE message to the S-CSCF which may invoke any VoLTE service logic as triggered by the initial filter criteria within the subscriber profile that was received during the IMS Registration. The S-CSCF shall forward the SIP BYE to the TAS at this point where VoLTE supplementary services may have been invoked . The S-CSCF routes the SIP BYE to the S-CSCF of the other party. The other party acknowledges the SIP BYE with a 200 OK.

At this stage, the VoLTE UE has cleared the call and the dedicated bearer for voice traffic has been removed.

3.2.6 Basic VoLTE UE to VoLTE UE Call Clearing - Received

3.2.6.1 General

A VoLTE UE shall perform call clearing by using the IMS network. The IMS Signalling shall be sent over the default bearer, and the dedicated bearer that was dynamically established for the voice traffic shall be removed.

3.2.6.2 Message Sequence

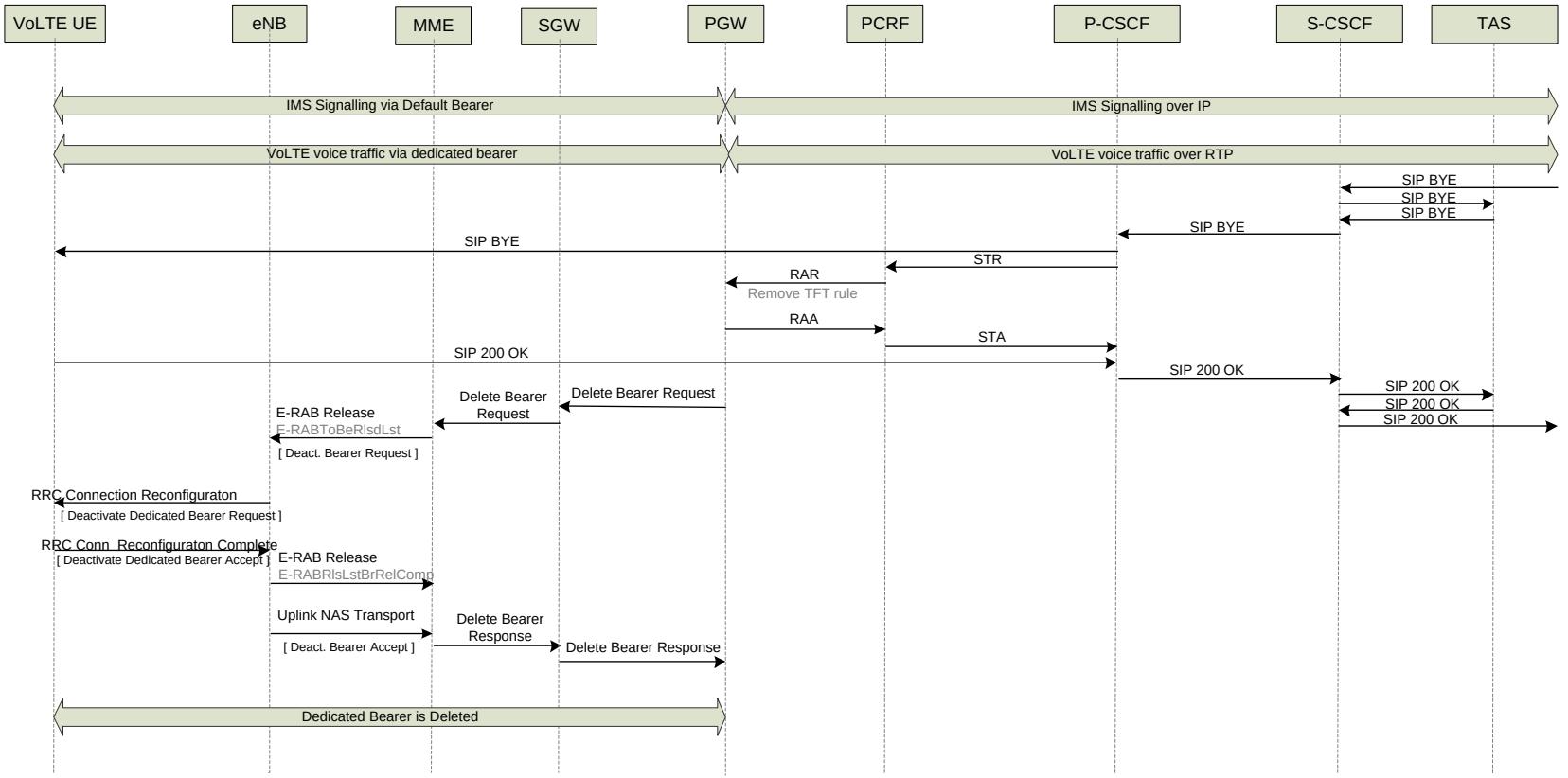

Figure 8: Basic VoLTE UE to VoLTE Call Clearing – Received message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 3.6.

3.2.6.3 Detailed Description

When a VoLTE UE terminates a voice call from LTE, it executes the normal mobile termination procedure as defined in 3GPP TS 23.228 [5] section 5.10.

A SIP BYE is received by the S-CSCF from the other party. The S-CSCF shall forward the SIP BYE to the TAS at this point where VoLTE supplementary services may have been invoked. The S-CSCF routes the SIP BYE to the P-CSCF which in turn forwards to the VoLTE UE. The VoLTE UE acknowledges the call clearing by sending a 200 OK.

On receiving the SIP BYE, the P-CSCF (IMS-ALG) frees off the media resources in the IMS-AGW if applicable. The P-CSCF also initiates a Session Termination Request to the PCRF to initiate the process of removing the dedicated bearer that was established for the voice traffic. The PCRF removes the binding between the stored subscription information and the IMS service information, and initiates a Re-Auth-Request to the PGW to remove the dedicated bearer for voice with the related QoS parameters (QCI=1, ARP) and the related traffic flow template.

The Delete Bearer Request, Bearer Release Request, and RRC Reconfiguration Request are utilised to remove the dedicated bearer utilised for voice traffic.

At this stage, the VoLTE UE has cleared the call and the dedicated bearer for voice traffic has been removed.

3.3 VoLTE-CS Interworking

Interworking of VoLTE services within the IMS domain and CS voice calls of a single Operator are in accordance with 3GPP specifications for IMS and CS Interworking. Please refer to TS 23.228 [5], 3GPP TS 29.163 [23] and 3GPP TS 29.235 [65] for further detailed information.

The procedures for the Circuit Switched Core Network are defined within 3GPP TS 23.205 [66] for ISUP/BICC and 3GPP TS 23.231 [67] for SIP-I.

The message sequences in sections 3.2.3 to 3.2.6 of this document apply, with the difference that the MGCF and IMS-MGW provide the interworking between the IMS signalling and media plane to the CS core network. The following sections document the interworking between VoLTE and the CS network via the MGCF/IMS-MGW. The interactions with PCC and EPC for the establishment of the dedicated bearer for voice are as detailed in sections 3.2.3 to 3.2.6.

3.3.1 Basic VoLTE UE to CS Call Establishment – Originating Side

3.3.1.1 General

For calls originating on VoLTE and breaking out to the CS network, the originating S-CSCF shall recognise that the termination is not within the VoLTE domain and shall invoke a BGCF to determine the target MGCF to break out to the CS network. The message sequence in section 3.3.1.2 details the interactions of the S-CSCF, BGCF and MGCF and builds on the message sequence in section 3.2.3.2 from where the S-CSCF propagates the SIP INVITE message to the terminating leg of the call.

3.3.1.2 Message Sequence

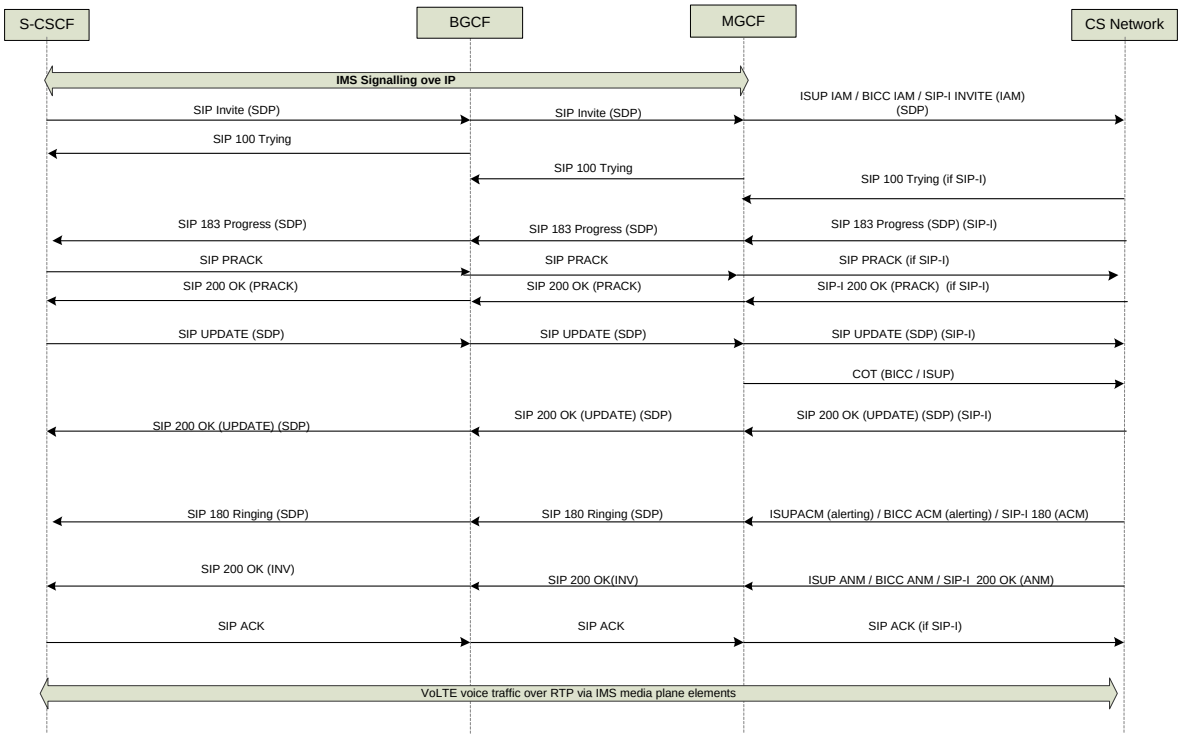

Figure 9: Basic VoLTE UE to CS Call Establishment – Originating Side

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [70].

NOTE: The BGCF may not remain in the signalling path having invoked the MGCF (see clause 5.6.2 of 3GPP TS 24.229 [9]).

3.3.1.3 Detailed Description

The S-CSCF determines that the Called-Party is within the operators CS network (i.e. ENUM/DNS lookup/internal configuration) and forwards the SIP INVITE to the BGCF.

The BGCF is responsible for selecting an appropriate MGCF for breaking out to the CS network. The BGCF may use ENUM/DNS or internal configuration data to analyse the Request-URI to determine the optimum MGCF to select. The Request-URI can be a TEL URI or SIP URI but will contain either an E.164 number or a telephone number qualified by a phone-context URI parameter. The BGCF forwards the INVITE to the selected MGCF.

The MGCF is responsible for inter-working to the CS network both in the control plane (IMS SIP to SIP-I/BICC/ISUP) and media plane via the IMS-MGW and shall follow the procedures of 3GPP TS 29.163 [23] (for ISUP/BICC) or 3GPP TS 29.235 [65] (for SIP-I). The IMS-MGW may be required to perform transcoding between AMR-NB/AMR/WB codecs and other codecs supported within the CS network (e.g. GSM-HR, GSM-FR, GSM-EFR, etc.).

The MGCF selects the outgoing route to the CS network (e.g. (G)MSC-S). The outgoing route to the CS network may be TDM or IP based and utilizes ISUP or SIP-I/BICC respectively. The route selection in the MGCF is based on ENUM/DNS or internal

configuration data. Having selected a route, the MGCF shall invoke an IMS-MGW to allocate and configure media resources for the call (see 3GPP TS 29.332 [35]).

The MGCF sends an ISUP IAM/BICC IAM/SIP-I INVITE (IAM) to the GMSC-S which in turn interrogates the HLR to discover location of the MSC-S that the user is currently registered on. Note that the MGCF may be co-located with a (G)MSC-S. The (G)MSC-S forwards the request to the MSC-S that the user is registered on and call establishment is progressed as defined within the 3GPP specifications.

Since the SDP offer from the originating leg indicates that QOS preconditions are desired but not yet met at the originating side, the MGCF shall (for BICC / ISUP) set the continuity indicator to "continuity check performed on previous circuit" / "COT to be expected" in the IAM message for ISUP/BICC respectively.

For ISUP/BICC, the MGCF shall send a 183 Progress message containing the SDP answer For SIP-I, the MGCF shall receive a 183 Progress message from the peer MSC containing the SDP answer. In both cases, the SDP answer contains a single voice codec, utilizes 100rel and indicates that QOS preconditions are also desired but not yet met at the terminating side. In addition, the SDP answer shall request confirmation of QOS preconditions being met at the originating side.

The 183 Progress (SDP) is sent to the originating leg via the BGCF/S-CSCF.

The MGCF receives a PRACK from the originating side of the call and responds with a 200 OK (PRACK) for BICC/ISUP routes. In the case of SIP-I routes, the MGFCF shall transit PRACK and 200 OK (PRACK).

The originating UE shall now send an UPDATE message with a new SDP offer confirming the selected voice codec and indicating that QOS preconditions have been met at the originating leg. The MGCF receives the UPDATE message and responds with a 200 OK (UPDATE) for BICC/ISUP routes and transits the UPDATE/200 OK (UPDATE) for SIP-I routes. The 200 OK (UPDATE) contains the SDP answer which indicates that QOS preconditions are also met at the terminating side. Since QOS preconditions are now met at both ends, the MGCF shall (for ISUP/BICC) send a COT message indicating "continuity check successful".

The terminating user in the CS network is now alerted and the MGCF receives an ACM (alerting) message from ISUP/BICC or a SIP 180 Ringing (ACM) message from SIP-I. The MGCF sends a SIP 180 Ringing message to the originating leg. This message shall not utilize 100rel. It is strongly recommended that the MGCF includes the P-Early-Media header in the SIP 180 (Ringing) message as described in 3GPP TS 29.163. At this point, the MGCF shall also ensure that backward media (e.g. ring tone, progress indications) are conveyed via the IMS-MGW..

The SIP 180 Ringing is forwarded to the VoLTE UE to indicate a ringing tone to the subscriber..

When the CS network indicates that the call has been answered, the MGCF sends a 200 OK (INVITE) message to the IMS network. This message is forwarded to the originating leg of the call and onto the VoLTE UE. The MGCF shall ensure that duplex media can be conveyed via the IMS-MGW at this point.

The VoLTE UE receives the 200 OK, and sends a SIP ACK message to acknowledge that the call has been established. The ACK is propagated through the IMS network to the MGCF. The ACK message is forwarded to the CS network for SIP-I routes.

At this stage, the call is established with voice traffic sent over the dedicated bearer between the VoLTE UE and the CS network via the IMS-MGW.

3.3.2 Basic VoLTE UE to CS Call Establishment – Terminating Side

3.3.2.1 General

For calls originating in the CS network and breaking into VoLTE, the call enters the VoLTE domain via the MGCF. The MGCF routes the call to the I-CSCF in order to determine the S-CSCF of the terminating user. The message sequence in section 3.3.2.2 details the interactions of the MGCF, I-CSCF and S-CSCF and builds on the message sequence in section 3.2.4.2 from where the S-CSCF is initially invoked with the SIP INVITE message for the terminating leg of the call.

3.3.2.2 Message Sequence

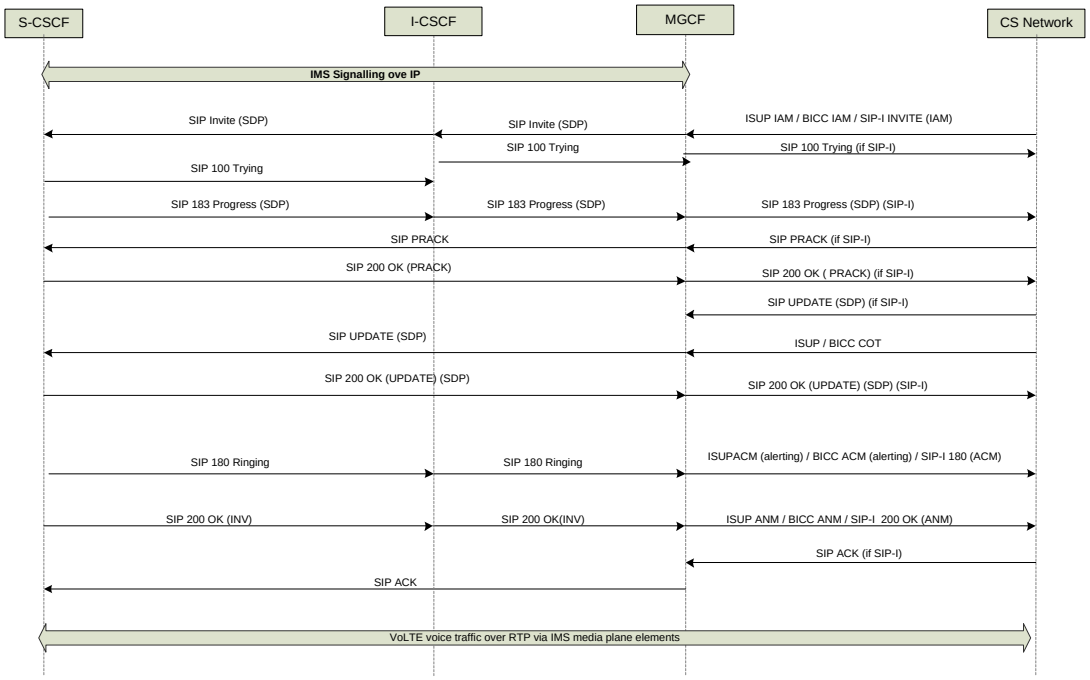

Figure 10: Basic VoLTE UE to CS Call Establishment – Terminating Side

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [70].

NOTE: The I-CSCF is a “stateful proxy” and remains in the signalling path only for the INVITE transaction.

3.3.2.3 Detailed Description

The CS Network initiates the call establishment by sending an ISUP IAM/BICC IAM/SIP-I INVITE (IAM) to the MGCF. The MGCF shall follow the procedures of 3GPP TS 29.163 [23] (for ISUP/BICC) or 3GPP TS 29.235 [65] (for SIP-I).

The MGCF invokes the IMS-MGW to allocate resources for the call and to potentially transcode between AMR-NB/AMR/WB codecs and other codecs supported within the CS network (e.g. GSM-HR, GSM-FR, GSM-EFR, etc.).

The target user will be identified via a telephone number for BICC/ISUP and via a SIP or TEL-URI for SIP-I. The MGCF will map the called party number of BICC/ISUP to a Request-URI which can either be a TEL URI or a SIP URI with “user-=phone” and shall contain either an E.164 number or else a national specific number qualified with a “phone-context” URI parameter as defined IETF RFC 3966 [68].

If overlap signalling is used from the ISUP/BICC CS network, then the MGCF shall determine when the complete number of address digits have been received (as specified in 3GPP TS 29.163 [23] and TS 29.235 [65]) prior to sending the INVITE message. It is noted that 3GPP TS 29.163 [23] does permit (as a network option) the INVITE to be sent prior to determining end of dialling. However, this option is not recommended to be used.

Contrary to 3GPP TS 29.163 [23] and 3GPP TS 29.235 [65], it is recommended that the MGCF sends a SIP INVITE indicating that QOS preconditions are desired but not yet met at the originating side. This occurs irrespective of whether the incoming ISUP/BICC IAM / SIP-I INVITE indicates that preconditions are not yet met (i.e. via continuity check indicator for ISUP/BICC or via SIP preconditions for SIP-I). This is done so that the message flows for an originating CS call align with those of an originating VoLTE UE. Furthermore, preconditions and SIP UPDATE are supported in IMS (see 3GPP TS 29.163 clause 7.2.3.2.1.2). In addition, the MGCF shall typically reserve multiple, codecs on the IMS-MGW but will eventually select one (based on the offer/answer exchange) and it is at this point that resource reservation is finalised at the originating side (in conjunction with precondition considerations in the CS network). Note that in figure 10, it is assumed that the incoming ISUP/BICC IAM / SIP-I INVITE indicates that preconditions are not yet met (i.e. via continuity check indicator for ISUP/BICC or via SIP preconditions for SIP-I).

The MGCF shall include a SUPPORTED header containing 100rel, precondition and P-Early-Media in the SIP INVITE message. The INVITE will also contain and SDP offer reflecting the media resources of the IMS-MGW. The SDP offer will contain multiple voice codecs (including AMR and AMR-WB) with the media stream set to “inactive” and that QOS preconditions are desired but not yet met at the originating side For voice calls ingressing the IMS, the MGCF should insert the media feature tag for IP Voice in Contact header (set to +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel") in order to enable the terminating S-CSCF to invoke the appropriate Application Server into the session.

The MGCF invokes the I-CSCF to enable the appropriate S-CSCF for the target user to be found.
The I-CSCF interrogates the HSS to identify the S-CSCF where the user is registered and forwards the INVITE to the S-CSCF. The S-CSCF invokes any VoLTE services as triggered by the initial filter criteria and routes the SIP INVITE to the AS and terminating P-CSCF as described in section 3.2.4.

Call establishment proceeds as in section 3.2.4 and the MGCF maps subsequent call establishment messages from the VoLTE network to the CS network.

A SIP 183 Progress (SDP) message is received from the terminating leg. This message shall utilize 100rel and the contained SDP answer contains a single voice codec and indicates that QOS preconditions are desired but not yet met at the terminating side. The MGCF interacts with the IMS-MGW to reflect the SDP answer by paring down the required codec list to that of the selected voice codec.

For SIP-I, the 183 Progress (SDP) message is forwarded to the peer MSC and the associated SIP PRACK message and 200 OK (PRACK) are transited from SIP-I to the terminating leg of the call via the MGCF.

For ISUP/BICC, the MGCF generates a SIP PRACK message and terminates the related 200 OK (PRACK) message.

For SIP-I routes, an UPDATE (SDP) message shall be received with a new SDP Offer. This is transited by the MGCF to the originating leg of the call. A 200 OK (UPDATE) message is received from the originating leg containing an SDP answer and passed through to SIP-I.

For ISUP/BICC, if a COT message is expected, then the MGCF awaits receipt of a COT message prior to sending the UPDATE message – else the MGCF generates an UPDATE (SDP) message immediately - with a new SDP Offer. This is sent to the terminating leg of the call. A 200 OK (UPDATE) message is received from the terminating leg containing an SDP answer and terminated at the MGCF.

The second offer / answer exchange has resulted in a single voice codec being selected, confirmation of preconditions having been met on both originating and terminating ends and the media stream set to active.

The terminating UE is alerted and a SIP 180 (Ringing) message is received from the terminating leg which is mapped to an ISUP/BICC ACM (alerting) or SIP-I 180 (ACM) message. This message does not use 100rel. The P-Early-Media header is not present in the 180 (Ringing) message, and so the MGCF shall apply ringing tone toward the CS network and shall inhibit the backward media path through the IMS-MGW. If the P-Early-Media header is present, then the MGCF enable a backward media path via the IMS-MGW to convey that media.

When the IMS network indicates that the call has been answered, the MGCF sends an ISUP/BICC (ANM) or SIP-I 200 OK (ANM) message to the CS network. The MGCF shall disconnect the ring tone (if previously applied at the IMS-MGW) and ensure that duplex media can be conveyed via the IMS-MGW at this point .

For SIP-I signalling, the MGCF will receive an ACK message from the CS network that is propagated to the IMS network. Otherwise, the MGCF shall generate an ACK message toward the IMS network.

At this stage, the call is established with voice traffic sent over the dedicated bearer between the VoLTE UE and the CS network via the IMS-MGW.

3.3.3 Basic VoLTE UE to CS Call Clearing - Initiated

3.3.3.1 General

This section describes the call clearing of an VoLTE UE to CS call where the release is initiated by the VoLTE UE. The message sequence in section 3.3.3.2 details the interactions of the S-CSCF, BGCF, MGCF and CS Network and builds on the message sequence in section 3.2.5.3 where the S-CSCF propagates the SIP BYE message to the other leg of the call.

3.3.3.2 Message Sequence

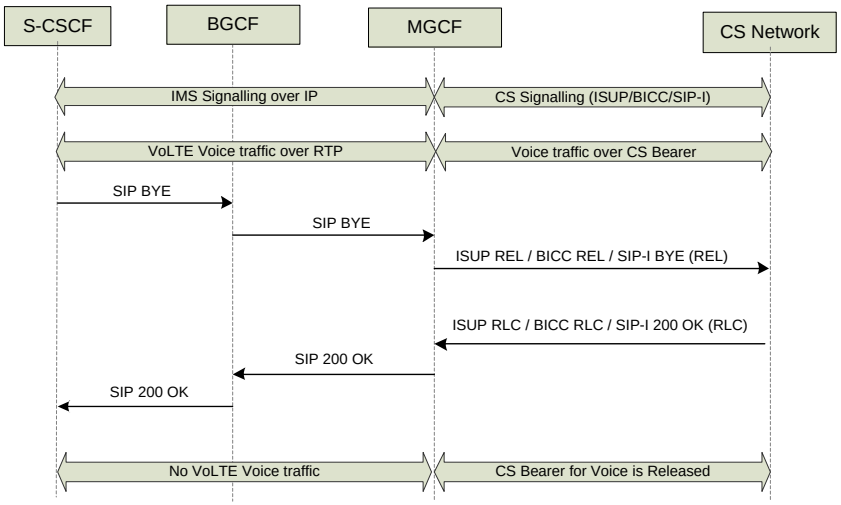

Figure 11: Basic VoLTE UE to CS Call Clearing - Initiated

NOTE: The BGCF may not be in the signalling path (see clause 5.6.2 of 3GPP TS 24.229 [9]).

3.3.3.3 Detailed Description

The call teardown is initiated by the VoLTE UE as described in section 3.2.5.2.

The S-CSCF propagates the SIP BYE message to the BGCF and onto the MGCF.

The MGCF releases the resources in the IMS-MGW and sends an ISUP REL/BICC REL/SIP-I BYE (REL) to the CS network.

On receipt of the ISUP RLC/BICC RLC/SIP-I 200 OK (RLC), the MGCF sends a 200 OK to the IMS network in response to the BYE.

At this stage, the VoLTE UE to CS call is released and the dedicated bearer has been torn down as described in section 3.2.5.2.

3.3.4 Basic VoLTE UE to CS Call Clearing - Received

3.3.4.1 General

This section describes the call clearing of an VoLTE UE to CS call where the release is initiated in the CS network. The message sequence in section 3.3.4.2 details the interactions of the S-CSCF, I-CSCF, MGCF and CS Network builds on the message sequence in section 3.2.6.3 where the S-CSCF receives the SIP BYE message from the other leg of the call.

3.3.4.2 Message Sequence

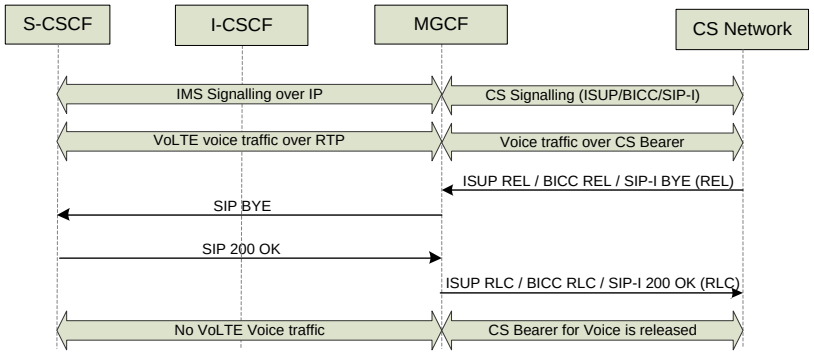

Figure 12: Basic VoLTE UE to CS Call Clearing - Received

NOTE: The I-CSCF is a “stateful proxy” and remains in the signalling path only for the INVITE transaction.

3.3.4.3 Detailed Description

The CS Network initiates the call teardown by sending an ISUP REL/BICC REL/SIP-I 200 OK (REL) to the MGCF.

The MGCF releases the resources in the IMS-MGW and sends a SIP BYE to the I-CSCF and onto the S-CSCF. The call release and release of the dedicated bearer at the UE side is as described in section 3.2.6.3.

The S-CSCF sends a 200 OK to the BYE to the I-CSCF and onto the MGCF.

The MGCF sends an ISUP RLC/BICC RLC/SIP-I 200 OK (RLC) to the CS network.

At this stage, the VoLTE UE to CS call is released and the dedicated bearer has been torn down as described in section 3.2.6.3.

3.4 Supplementary Services

3.4.1 General

GSMA PRD IR.92 [54] section 2.3 specifies a mandatory subset of MMTel supplementary services as defined by 3GPP TS 24.173 [8] for VoLTE. These are listed in Table 2.

Supplementary Service	3GPP Specification	Additional Information
Originating Identification Presentation	3GPP TS 24.607 [16]	N/A
Terminating Identification Presentation	3GPP TS 24.608 [17]	N/A
Originating Identification Restriction	3GPP TS 24.607 [16]	Recommended options are specified in IR.92 Section 2.3.6
Terminating Identification Restriction	3GPP TS 24.608 [17]	Recommended options are specified in IR.92 Section 2.3.7
Communication Forwarding Unconditional	3GPP TS 24.604 [13]	Recommended options are specified in IR.92 Section 2.3.8

Communication Forwarding on not Logged	3GPP TS 24.604 [13]	Recommended options are specified in IR.92 Section 2.3.8
Communication Forwarding on Busy	3GPP TS 24.604 [13]	Recommended options are specified in IR.92 Section 2.3.8
Communication Forwarding on not Reachable	3GPP TS 24.604 [13]	Recommended options are specified in IR.92 Section 2.3.8
Communication Forwarding on No Reply	3GPP TS 24.604 [13]	Recommended options are specified in IR.92 Section 2.3.8
Barring of All Incoming Calls	3GPP TS 24.611 [19]	Recommended options are specified in IR.92 Section 2.3.9
Barring of All Outgoing Calls	3GPP TS 24.611 [19]	Recommended options are specified in IR.92 Section 2.3.9
Barring of Outgoing International Calls	3GPP TS 24.611 [19]	Recommended options are specified in IR.92 Section 2.3.9
Barring of Outgoing International Calls – ex Home Country	3GPP TS 24.611 [19	Recommended options are specified in IR.92 Section 2.3.9
Barring of Incoming Calls - When Roaming	3GPP TS 24.611 [19]	Recommended options are specified in IR.92 Section 2.3.9
Communication Hold	3GPP TS 24.610 [18]	N/A
Message Waiting Indication	3GPP TS 24.606 [15]	Recommended options are specified in IR.92 Section 2.3.5
Communication Waiting	3GPP TS 24.615 [20]	Recommended options are specified in IR.92 Section 2.3.4
Ad-Hoc Multi Party Conference	3GPP TS 24.605 [14]	Recommended options are specified in IR.92 Section 2.3.3

Table 1VoLTE Mandatory Supplementary Services

VoLTE supplementary service configuration (i.e. XCAP root URI, XCAP APN) is performed using XCAP at the Ut reference point as described in GSMA PRD IR.92 [54] section 2.3.2. The APN for XCAP requests must be provisioned by the home operator in the UE as described in GSMA PRD IR.92 ([54]) section 4.3.1.Note that the XCAP APN is distinct from the well-known IMS APN.

3GPP has defined a generic baseline XML document (see 3GPP TS 24.623 [21]) which provides a flexible and extensible framework to enable the management of specific MMTel services via service specific extensions to the baseline document. There is also the capability to access an XML document in its entirety down to accessing a sub-set (including a single item) of an XML document. All UEs and Application Servers shall support the defined XML documents for the mandatory supplementary service set in Table 2.

Authentication at the XCAP Server via the Ut reference point for secure configuration of VoLTE supplementary services shall be performed as described in GSMA PRD IR.92 [54] section 2.2.2. It is recommended that the UE supports the Generic Authentication Architecture procedures for authentication.

3.5 ENUM/DNS

3.5.1 General

VoLTE subscribers shall be allocated and identified by a E.164 telephone number. The E.164 numbering standard has been adopted globally and provides a standardised interoperable numbering system upon which network operators can build networks and customer relationship management systems. Usage of ENUM is described in GSMA PRD IR.67 ([52]).

3.5.2 Number Portability

Historically, telephone numbers were allocated to operators in blocks of E.164 numbers typically based on dial code. Individual numbers were then allocated to their subscribers from within their block. Using a table it is possible to look up which operator owned the number, based on the dialling code. On this basis C7/TDM based service platforms used the E.164 based telephone number to route traffic.

The introduction of number portability in many countries changed this. It is no longer possible to determine which operator owns a number based on the dialling code. As a result, C7/TDM platforms generally request additional information about the full telephone number from a number registry or database before routing. This process is frequently called number portability correction and the information accessed is referred to as number portability data.

3.5.3 IP Service Routing

The VoLTE service is provided by IMS which uses URIs and IP addresses for routing traffic. IP addresses are associated with URIs through the DNS system. DNS enables the IP address associated with the target URI to be looked up during the routing process.

In the case where IP services like VoLTE employ an E.164 number as the subscriber identity the IP network platforms need to identify the target URI destination from the dialled E.164 number when routing traffic to that number. This can be accomplished by accessing an E.164/URI registry or database.

3.5.4 Number Resolution

It is required to resolve a dialled E.164 into a routable end destination address, correcting for the effects of Number Portability. Number Resolution is the process of determining from an E.164 number what network to direct traffic to and to what address. GSMA and IETF recommend that both the task of translating the E.164 number into a SIP URI and correcting for number portability is accomplished via a standardised number look up technology, ENUM.

3.5.5 ENUM

ENUM is a telephone look up or number resolution technology, standardised by the Internet Engineering Task Force (IETF) and Carrier ENUM is further specified by the GSMA in PRD IR.67 [52]. It enables number registries to be queried and return lists of end point information relating to a telephone number via a standard ENUM API.

ENUM registries can:

- Provide IP routable information against a E.164 phone number
- Provide a list of service/platform information against an E.164 number
- Provide the correct destination correcting for number portability

Benefits:

- ENUM is an open standard to enable routing of IP/IMS services using telephone numbers.
- ENUM can be applied to any/every IP service, e.g. Voice, Text, MMS, IM, and Video, etc. and so is architecturally efficient.
- The ENUM is an API within the IP family of protocols (an extension of DNS) and fits well with IP infrastructure.
- Number Resolution is required for internal and external routing. Using a standard is essential for interoperability where queries will take place to external ENUM data sources on a global basis.
- ENUM is agnostic of the type of network or interconnect medium an operator chooses to use.

3.5.5.1 ENUM Network Impact

When IP services are available and the network infrastructure is required to route a piece of traffic to an E.164 number there is uncertainty over whether the destination number is;

- Hosted by IMS technology or the pervasive legacy C7/TDM technology
- An original number allocated to the service provider
- An imported number from another service provider
- A number exported to another service provider

An ENUM query is performed to receive information about the end destination and enable it to take the correct routing decision. An ENUM query is designed to return a number portability corrected URI for a particular E.164 which the network can resolve to an IP address for routing.

3.5.5.2 ENUM Functionality

Figure 13 shows an example of how ENUM is used during the setup of a person to person session. In this general example the ENUM database is shown as a cloud, as there are options for the storage and management of ENUM data. The originating subscriber establishes a session towards the destination party. The originating infrastructure resolves the number before taking a routing decision by accessing an ENUM database. The ENUM database returns the URI associated with the destination subscriber. The originating infrastructure resolves the destination URI into an IP address via DNS. Routing takes place based on the destination IP address.

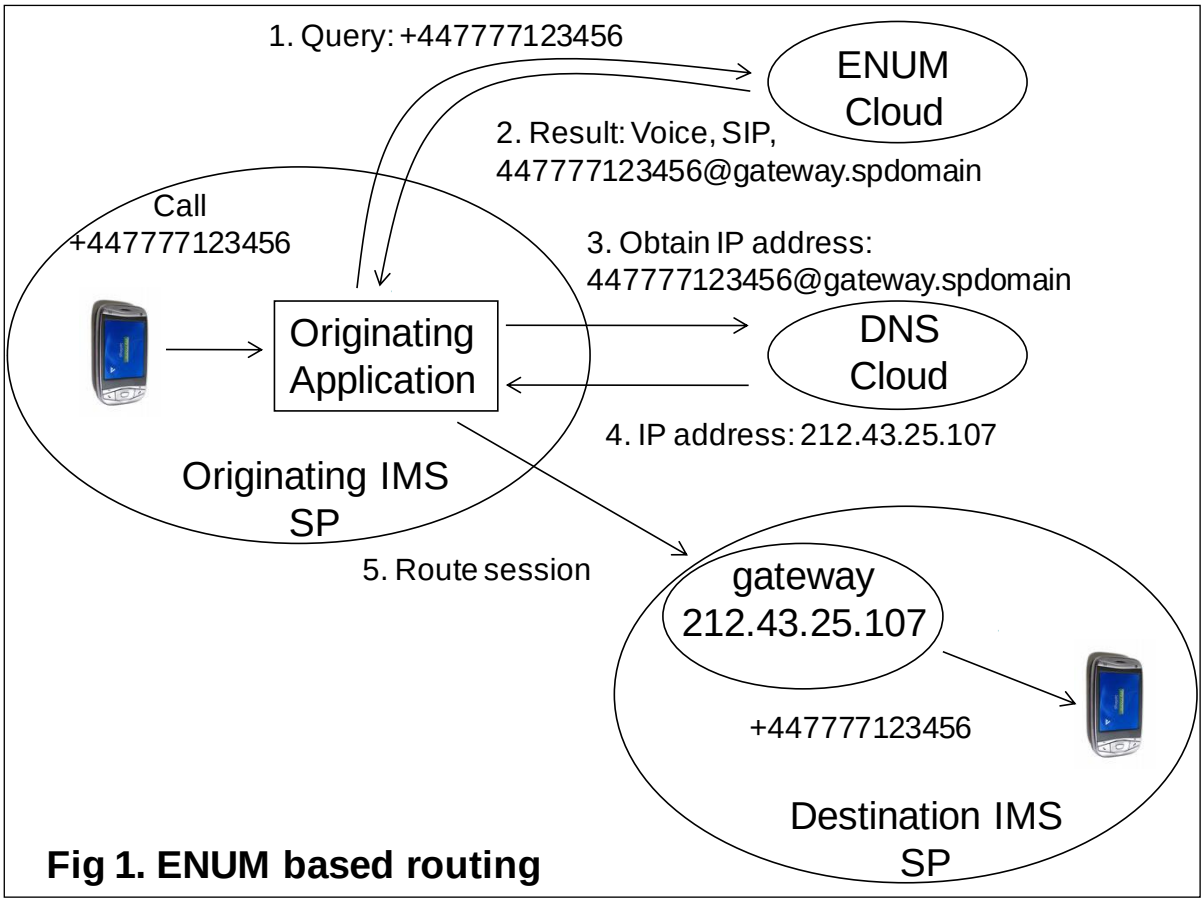

Figure 13: ENUM Based Routing

3.5.5.3 ENUM Registry Architecture

Subscribers can dial numbers to any destination in the world at any time. It is useful to classify routing scenarios as;

- Internal
- External National
- External International

Different strategies and regulations may apply to the associated ENUM approach.

In order to resolve numbers, operators need to arrange access to an ENUM registry, or registries, that contain the information for the above routing scenarios. Typically operators have

- Full knowledge of the numbers they serve
- Full, partial or no knowledge of the numbers ported in their country depending on local number portability procedures
- Little or no knowledge of the numbers existing and ported in other countries

As such operators should adopt a strategy whereby internal ENUM records can be accessed and external ENUM registries can be accessed.

3.5.5.4 Internal ENUM Registries

Typically an operator may wish to establish an ENUM registry for internal use. This may comprise of two elements, records concerning the subscribers it supports and a cache of frequently dialled external numbers. The IP switching infrastructure is connected to this registry in order to resolve numbers. In the event that a number is not present or cannot be

resolved by the local registry then the IP infrastructure needs to employ an alternative strategy to query an external registry system. The internal registry is populated by the operator. The operator associates URIs against its E.164 numbers in this registry that will result in successful internal routing. Cached results are provided from external sources and should be stored as received otherwise routing will be unsuccessful. The cache .time (also known as “time to live”) provided by external sources for returned results should be respected since routing based on out of date data could be unsuccessful e.g. cause a call set-up failure. The Internal database could be managed by the operator, outsourced as with other network components or be part of a national system depending on local number portability regulations. Selection of the best approach will vary from country to country and network to network and local analysis is required to select the right approach.

3.6 Diameter Signalling

3.6.1 General

The VoLTE architecture utilises Diameter interfaces between components of the EPC, PCC, and IMS core network. 3GPP has defined a number of Diameter Applications based on the Diameter Base Protocol is defined within IETF RFC 3588 [59].

3.6.2 Diameter Agents

In order to support scalability, resilience and maintainability of the Diameter interfaces, the usage of a Diameter Agent is recommended. The Diameter Agent reduces the mesh of different diameter connections within the network to aid in routing of Diameter messages, provides load-balancing functionality for handling of signalling congestion, and provides protocol interworking functionality (e.g. Diameter application AVP's, transport protocol, etc.).

Further description of the Diameter Agent is described within GSMA PRD IR.88 [53] section 3.1.3.

3.6.3 Diameter Transport

The Diameter Base protocol defines the clients must support either TCP or SCTP as the transport protocol, and that the servers and agents must support both TCP and SCTP.

A number of the Diameter interfaces defined by 3GPP (i.e. Cx, Sh, S6a, S9) have profiled this further by stating that SCTP must be supported by the relevant nodes. Whilst other Diameter interfaces defined by 3GPP (i.e. Gx, Rx) allow support of SCTP or TCP.

It is recommended that SCTP is utilised as the transport protocol across all Diameter interfaces utilised in the VoLTE architecture, or that a Diameter Agent is deployed to perform the interworking between SCTP and TCP.

3.6.4 Diameter Peer Discovery

To enable Diameter routing within the home network, a Diameter node needs to discover which peer to route messages to for a specific application. This may be performed by using manual configuration of Diameter nodes within each node. However by allowing for a dynamic discovery mechanism (NAPTR query), it allows for a simpler, scalable, and robust deployment.

GSMA PRD IR.88 [53] section 3.1.3.4 describes the peer discovery mechanism in further detail.

Note that the dynamic discovery mechanism becomes more necessary, as the scale of the connections increases and topology hiding becomes more important.

3.6.5 Diameter Capability Exchange

As the Diameter Agent acts as a proxy for the network elements supporting a Diameter interface, it must perform a Capability Exchange as defined within IETF RFC 3588 [59] to all

of its Diameter peers within the network. Therefore the Diameter Agent shall support the superset of all the Diameter interfaces required for VoLTE.

3.6.6 Diameter Routing

All Diameter enabled elements in a network shall route their requests and responses via the Diameter Agent. The Diameter Agent routes the requests/responses to the correct destination based on the host and realm identity in the message as follows:-

- If the Diameter Client knows the address/name of the Diameter Server (e.g. pre-configured), the request shall include both the Destination-Realm and Destination-Host and forward the request message to the Diameter Agent. The client will add its own Origin-Host and Origin-Realm information.
- If the Diameter Client does not know the address/name of the Diameter Server, it shall forward the request to the Diameter Agent which will determine the destination address/name by analysing the received Diameter Application ID, Destination Realm, and its internal routing table information established during peer discovery and capability exchange. The Diameter Agent shall insert the Destination-Host and forward the message to the destination node.

A Diameter Server shall store the Origin-Host and Origin-Realm within the request, to be used for future messages, in the respective destination host/realm parameters. The Diameter response message from the server shall include its own host/realm parameters in the Origin-Host and Origin-Realm, and forward the response message to the Diameter Agent which in turn proxies the response to the Diameter Client. The Diameter Client shall store the Host/Realm parameters for future usage.

The Diameter Agent may optionally overwrite the host/realm information (e.g. topology hiding) but this requires a mapping table to be maintained within the Diameter Agent and is not required for a single network deployment.

3.7 Traffic Management and Policy

3.7.1 General

In order to meet the requirements of the VoLTE services in regards to guaranteed bit-rate for the voice data, sensitivity to jitter and delay, operators need to implement a traffic handling policy. This requires a standardised mechanism that specifies the relative priority for the VoLTE service. It ensures that end-users receive a high level of Quality of Experience for VoLTE, by adapting the handling of the applications within the acceptable bounds of the Quality of Service characteristics.

In the VoLTE architecture, this is performed in two ways:-

- Policy and Charging Control (PCC)
- DiffServ

3.7.2 Policy and Charging Control

Policy and Charging Control functionality encompasses Flow Based Charging (including charging control and online credit control) and Policy control (e.g. gating control, QoS control, QoS signalling, etc.).

This is achieved by three logical network components; the Application Function (AF) – incorporated within the P-CSCF, the Policy Charging and Rules Function (PCRF), and the Policy Control Enforcement Function (PCEF) – incorporated within the PGW.

The P-CSCF provides information related to the control-plane signalling of a particular application to the PCRF. New application requests may invoke requests to the PCRF in order to modify or create new IP-bearers for that application.

The PCRF provides policy control decisions and flow based charging controls which are enforced by the PGW. The PCRF determines how a service data flow shall be treated, per-subscriber, in the PGW and ensures that the user plane traffic mapping and treatment is in accordance with the user's profile. The PCRF also receives information related to control-plane signalling and application control from the P-CSCF, which may result in a modification of policy rules at the enforcement level. It is also capable of feeding back information related to the user-pane to the application level, e.g. loss of bearer.

The PGW supports flow gating, rate limiting, policing, shaping, Differentiated Services (DiffServ) marking, and other features. The control of applying these functionalities is dependent on a per-subscriber basis and dependent on the policy rules received from the PCRF. In addition the PGW supports deep packet inspection (DPI) capabilities, QoS controls, and advanced reporting capabilities to the PCRF including support for volume-based reporting.

Through the usage of the PCC architecture, and the binding between the control-plane signalling over the default bearer and the user-plane media over a dedicated bearer is achieved with the related QoS enforced.

Policy rules within PCC are defined on the service data flow level by defining a Quality of Service rule to be applied to detect the type of service data flow and apply the correct QoS parameters to the session. 3GPP TS 23.203 [4] standardises a set of QoS Class Identifiers (QCI) for different services with related QoS parameters defined (i.e. resource type, priority level, packet delay budget, packet error loss rate).

<table>
<tr><th>QCI</th><th>Resource Type</th><th>Priority</th><th>Packet Delay Budget</th><th>Packet Error Loss Rate</th><th>Example Services</th></tr>
<tr><td>1</td><td rowspan="4">GBR</td><td>2</td><td>100 ms</td><td>10^{-2}</td><td>Conversational Voice</td></tr>
<tr><td>2</td><td>4</td><td>150 ms</td><td>10^{-3}</td><td>Conversational Video (Live Streaming)</td></tr>
<tr><td>3</td><td>3</td><td>50 ms</td><td>10^{-3}</td><td>Real Time Gaming</td></tr>
<tr><td>4</td><td>5</td><td>300 ms</td><td>10^{-6}</td><td>Non-Conversational Video (Buffered Streaming)</td></tr>
<tr><td>5</td><td rowspan="5">Non-GBR</td><td>1</td><td>100 ms</td><td>10^{-6}</td><td>IMS Signalling</td></tr>
<tr><td>6</td><td>6</td><td>300 ms</td><td>10^{-6}</td><td>Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)</td></tr>
<tr><td>7</td><td>7</td><td>100 ms</td><td>10^{-3}</td><td>Voice,
Video (Live Streaming) Interactive Gaming</td></tr>
<tr><td>8</td><td>8</td><td rowspan="2">300 ms</td><td rowspan="2">10^{-6}</td><td rowspan="2">Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)</td></tr>
<tr><td>9</td><td>9</td></tr>
</table>

Table 2 : Standard QCI Values and related QoS Parameters

VoLTE utilises QCI=5 for IMS Signalling on the default bearer and QCI=1 for conversational voice on dedicated bearers.

The access network (e.g. eNodeB) utilises the QCI specific parameters that control packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), that have been pre-configured by the operator. The QCI, and associated parameters, are also mapped to the relevant DSCP marking on IP packets at the transport layer.

3.7.3 DiffServ

DiffServ (Differentiated Services) is used to differentiate between different services utilising the same IP bearer, to enable IP-routers and other nodes to handle specific traffic in a differentiated way. For instance, IP packets that are related to a specific service may require a higher level of buffer management and packet scheduling mechanisms for the traffic that it carries.

In order to provide this functionality within a service-aware node, the IETF have defined an IP packet header field to allow these nodes to "mark" IP Packets with a class of service. The class of service is referred to as the DiffServ Code Point (DSCP). As the "marking" of these packets is performed at the IP layer, IP routers and other network components that are not service-aware can perform the relevant treatment of data traffic, dependent on the value of the DSCP value per IP packet. For example, the utilisation of DSCP may enable the VoLTE service that requires a low level of latency to be routed through an IP network with a higher priority compared to best-effort internet traffic. This is accomplished by all IP-nodes in the data path recognising the DSCP value, performing the relevant traffic management, without information of what the data traffic pertains to.

It should be noted that the usage of DiffServ is widely deployed within the industry, mobile and fixed networks, and forms a basis for base IP-routing network components (i.e. IP switches and routers).

3.7.4 Mapping between QCI and DiffServ

GSMA PRD IR.34 [48] section 6.2 describes the different traffic classes that are used. These are shown in Table 3.

	QoS Information			IP transport	
QCI	Traffic Class	THP	Signalling indication	Diffserf PHB	DSCP
1	Conversational	N/A	N/A	EF	101110
2					
3					
4	Streaming	N/A	N/A	AF41	100010
5	Interactive	1	Yes (see note)	AF31	011010
6			No	AF32	011100
7		2	No	AF21	010010

8		3	No	AF11	001010
9	Background	N/A	N/A	BE	000000

Table 3: EPC QoS information and mapping to DSCP

VoLTE utilises QCI=5 for IMS Signalling on the default bearer and QCI=1 for conversational voice on the dedicated bearer.

3.8 Session Border Controllers

The Session Border Controller (SBC) has primarily been deployed within the context of IP-Interworking at the edge of the Operators network for Interconnect to the IPX or direct connection to another Operator's network. Within the VoLTE architecture, SBC's are commonly used on the IMS NNI incorporating the IBCF/TrGW functionality. SBC's on the access to IMS are becoming more prevalent, incorporating specific IMS functionality i.e. P-CSCF, IMS-ALG, and IMS-AGW. It is important to understand that the SBC receives both the Control Plane signalling and the User Plane data for data sessions.

The SBC can be seen as the point for ingress and egress for the Network Operator, a signalling and user plane gateway. As part of the functions that the SBC provides are Security (i.e. Firewall, topology hiding), Control-plane Interworking between different protocols, Network Address Translation, Transcoding between different user plane data-types, load-balancing and routing, etc.

However, in terms of traffic management, SBC's provide the functionality of analysing the control plane signalling to ensure that operator policies (ingress and egress) are adhered to across a network interconnect. Dependent on the service-level aspect derived from the control plane signalling, and with Operator configuration, the SBC is capable of setting the correct DSCP value for that service.

Additionally, the majority of SBC's also incorporate a Deep Packet Inspection solution. In this respect, the SBC provides the functionality of analysing the class of service for data traffic on the IP Bearer. Therefore SBC's are capable of differentiating traffic (e.g. voice, video, internet, etc.) at the bearer level and setting the relevant DSCP accordingly, enabling the correct handling of IP-traffic via intermediate nodes, to ensure end-to-end Quality of Service from the Interconnect perspective.

3.9 Emergency Call

The VoLTE UE and network are required to support emergency calls in IMS as described in GSMA PRD IR.92 [54] section 5.2. However support of emergency calls in the CS domain may be a local regulatory requirement. Therefore, in areas where LTE radio coverage and/or IMS network is not available, the network shall be able to reject an IMS emergency attempt and the VoLTE UE shall support CS emergency calls as used today. GSMA PRD IR.92 [54] Annex A.5 describes this in further detail.

3.10 Lawful Intercept

The architecture for providing Lawful Intercept for VoLTE services is defined in 3GPP TS 33.107 [41] section 7A with call scenarios shown in Annex C. In a VoLTE deployment, the Access Session Border Controller (P-CSCF, IMS-ALG, IMS-AGW) may be used as the point of intercept, due to the available access to both the IMS signalling and the media.

3.11 Security

3.11.1 General

The security architecture for LTE is defined in 3GPP TS 33.401 [43].

3.11.2 Security Gateway

Within the VoLTE architecture the Security Gateway is an optional network node. It is particularly relevant for deployments where RAN sharing may be utilised. The Security Gateway is used to originate and terminate secure associations between the eNodeB and the Evolved Packet Core network. IPsec tunnels are established with pre-shared security keys, which can take a number of different formats. IPsec tunnels enforce traffic encryption, for added protection, according to the parameters exchanged between the two parties during tunnel setup. This enables secure communications between the eNodeB and EPC across the S1-MME, S1-U and X2 interfaces.

3.11.3 IMS Media Plane Security

IMS Media Plane Security is defined within 3GPP TS 33.328 [42]. It provides security for RTP and MSRP based media and is used in the following ways:-

- User plane security between UE and IMS access (IMS-ALG, IMS-AGW), commonly referred to as e2ae media protection.
- User plane security end to end between UE's, commonly referred to as e2e media protection.

For the VoLTE services using RTP, media plane security is not profiled in GSMA PRD IR.92 [54] but may optionally be provided utilising SRTP (Secure RTP) as defined in IETF RFC 3711 [60] / 3GPP TS 33.328 [42]. The key management solutions are described in 3GPP TS 33.328 [42].

3.12 SMS over IP

VoLTE architecture supports the delivery of SMS over IP as described in GSMA PRD IR.92 [54] section 2.5 and is based on the functionality and procedures defined in 3GPP TS 24.341 [12]. The VoLTE UE is required to support the SM-over-IP sender/receiver and an IP-SM-GW is required within the IMS core network.

Where interaction with legacy SMS services are required, these are implemented as described in GSMA PRD IR.92 [54] Annex A.7.

3.13 Support of Legacy Proprietary CS Services

The VoLTE Architecture and baseline 3GPP specifications do not provide a standardised solution to interwork with legacy proprietary services that are commonly utilised within Operators CS networks.

Three possibilities exist for legacy CS proprietary services within the VoLTE Architecture:-

1. Cease support of the legacy proprietary services for VoLTE users:- This may be regarded as being a sub-optimal approach as some services are required under local regulation and other services a deemed to provide distinct value-add to the end user.
2. Develop the legacy proprietary services within the TAS:- This approach may be regarded as being not cost-effective and the time required to develop each service, on a case by case basis, would not enable a timely deployment of VoLTE.
3. Develop interworking between the VoLTE architecture and the existing legacy proprietary CS network services:- A standardised approach would take time to agree on a solution and therefore reliance on proprietary solutions may be required. Potential proprietary solutions may involve the deployment of a gateway to interwork between the IMS SIP architecture and the legacy CS network (e.g. IM-SSF). This gateway may be collocated with the TAS.

3.14 Complementing VoLTE with 2G/3G Voice

3.14.1 SRVCC

As LTE radio access may not be deployed in a ubiquitous manner, the operator may wish to complement a VoLTE network with their existing CS radio access for voice.

In order to enable seamless voice service between VoLTE and CS voice, GSMA PRD IR.92 [54] Annex A describes how Single Radio Voice Call Continuity (SRVCC) procedures are used when performing a handover between LTE and GSM/UMTS coverage.

The enhanced SRVCC functionality defined within 3GPP Release 10 also supports the handover of calls that have a mid-call feature being applied (e.g. calls on hold, calls that are in a call waiting state), support for calls in alerting state and enhancements to minimise voice interruption delay and is therefore recommended for an SRVCC deployment.

3.14.2 PS Handover

As an alternative to SRVCC, PS Handover may be preferable in order to keep the user utilising VoLTE service in the IMS domain. GSMA PRD IR.58 [49] defines the profile IMS profile for Voice over HSPA (VoHSPA) and the description of the Inter-RAT PS handover to provide mobility to/from LTE in section 3.5.

3.14.3 IMS Service Centralization and Continuity

3GPP has standardised the principle for centralisation and continuity of services in IMS to provide consistency to the end user regardless of which access technology is utilised. This is further profiled within GSMA PRD IR.64 [50].

GSMA PRD IR.92 [54] Annex A.4 mandates the usage of the Ut interface for setting the supplementary service configuration when the UE is using the CS network for voice service. This implies that the services are centralised and calls anchored within the VoLTE IMS domain by using one of the solutions as described in GSMA PRD IR.64 [50] (e.g. an MSC-S enhanced for ICS, utilising CAPv2, or CS-interworking.

However, the initial deployments of VoLTE IMS networks may not offer service centralisation, with specific issues defined within GSMA PRD IR.64 [50] Annex A.

As VoLTE mandates Ut for supplementary service configuration, the network needs to ensure that supplementary service settings are the same in both VoLTE and CS networks. This can be done by one of the following two ways:

1. Avoiding synchronisation and accepting the limitation of a subscriber having to manually configure supplementary services in both domains.
2. Synchronization between the CS and IMS/MMTEL subscription data which ensures that the service settings in IMS (over Ut) are set the same as their CS service equivalents. This has been studied in 3GPP but finally no solution was standardized due to the complexity and different ways that such data is stored internally within the likes of the HSS/HLR and VoLTE MMTel AS. A potential solution could be to utilise User Data Convergence (UDC) architecture as defined within 3GPP TS 23.335 [75] for HLR/HSS integration.

3.15 Charging

VoLTE charging architecture for Online and Offline Charging is defined in 3GPP TS 32.240 [38] and 3GPP TS 32.260 [39] which defines the IMS Charging architecture. The Diameter protocol is utilised for the Ro interface for online charging and the Rf interface for offline charging.

VoLTE charging may be based on the utilisation of Charging Data Records (CDR's) generated by EPC and IMS nodes. The format and content of the CDR's for the SGW, PGW, P-CSCF, S-CSCF and the TAS are defined in 3GPP TS 32.298 [40].

3.16 Codecs

GSMA PRD IR.92 [54] has mandated AMR / AMR-WB codecs to be used for VoLTE and these codecs shall be implemented by all equipment manufactures to ensure good voice quality on VoLTE as well as facilitating inter-operability and avoiding transcoding. Other voice codecs may optionally be offered in addition to the AMR codecs.

3.17 IP Version & Transport

As described in GSMA PRD IR.92 [54] section 5.1, both IPv4 and IPv6 must be supported by the UE and network for VoLTE. On attaching to the network, the UE must request the PDN type (IPv4v6) – see section 3.2.3.1. If both IPv4 and IPv6 addresses are assigned for the UE, the UE must prefer IPv6 when performing P-CSCF discovery.

As recommended in GSMA PRD IR.92 [54], both UDP and TCP shall be supported for SIP message transport both by the UE and network. If UDP is used for SIP transport, implementations should avoid fragmentation by obeying clause 18.1.1 of IETF RFC 3261 [69] and swap over to TCP for large messages. Note that the transport change is done on per SIP message basis and not on a per SIP session basis.

3.18 Home eNodeB (HeNB)

It is also possible to deploy an eNode-B to provide Femtocell coverage. Such an element resides in the CPE and is termed a Home eNodeB (HeNB). This option is shown in figure 14 below.

HeNBs are usually connected to the EPC via both a SEG and HeNB GW. The HeNB GW serves as a concentrator for the C-Plane, specifically the S1-MME interface, between the HeNB and MME. The HeNB GW appears to the MME as an eNodeB and appears to the HeNB as a MME. The S1-U interface from the HeNB may also be terminated at the HeNB GW or may bypass the HeNB GW.

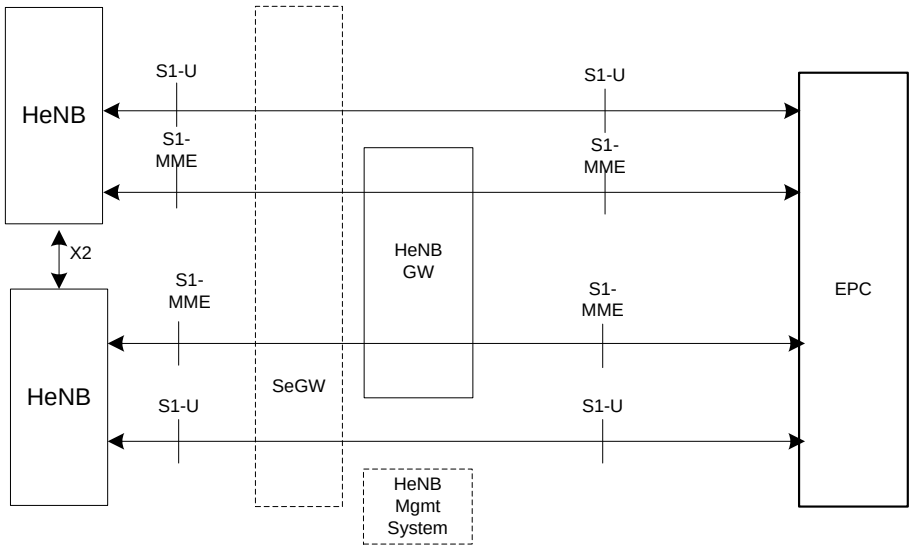

Figure 14: HeNB Architecture

4 VoLTE Implementation - Interconnect

This section builds on the single PMN scenario in section 3 and considers inter-operator VoLTE interconnect between PMNs. All users are attached and registered in their respective home networks (i.e. no roaming) and calls are established between users in different PMNs via the NNI.

Two ways for inter-connect are considered to be in scope, namely a bi-lateral interconnect and interconnect via an IPX.

This section describes the implementation for these scenarios.

4.1 General

The VoLTE architecture for an interconnect deployment is shown in Figure 15.

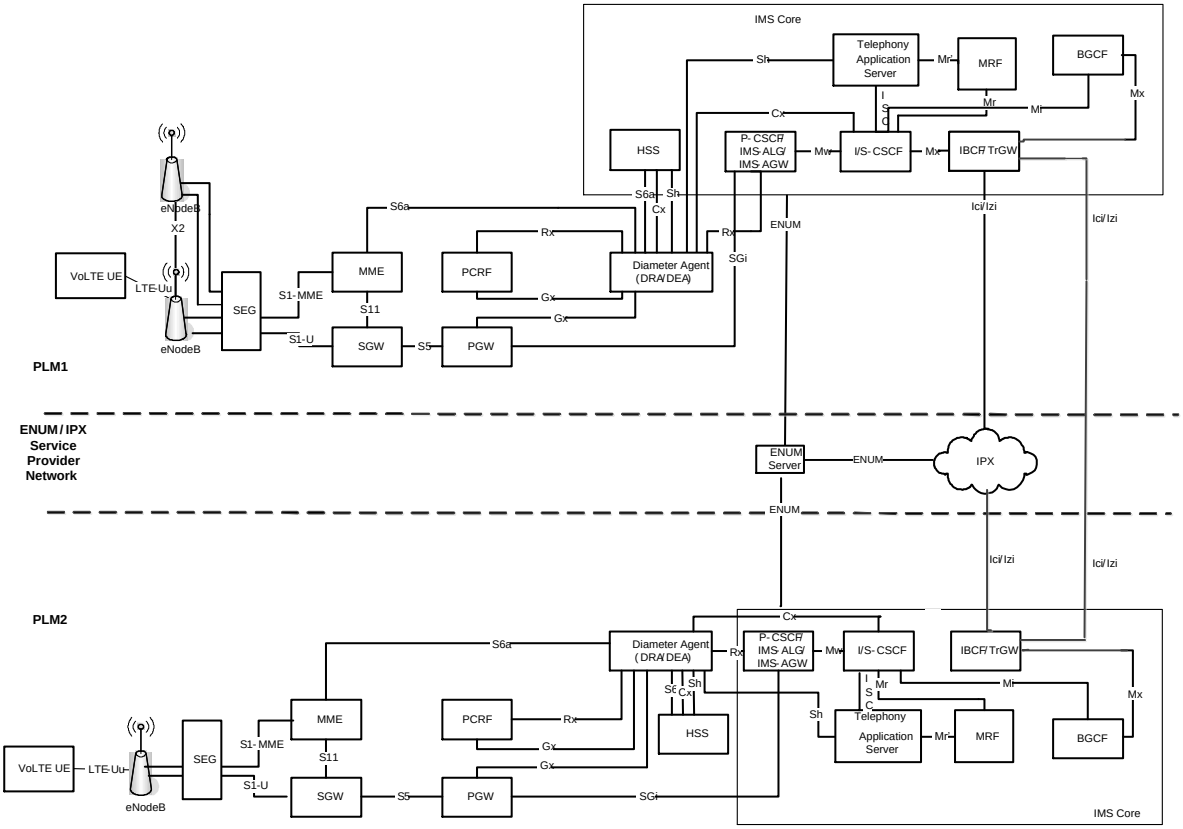

Figure 15: Interconnect PMN VoLTE deployment

NOTE: The Gm interface (UE to P-CSCF) is included in the Intra-PMN VoLTE deployment although not shown in the above figure.

NOTE: The Ut interface (UE to TAS) is included in the VoLTE architecture although not shown in the above figure.

4.2 VoLTE Interconnect

IMS interconnect is defined in 3GPP 29.165 [24].

Users are assumed to have attached and registered in their home network as shown in section 3. Calls are then established between users in different PMNs across the interconnect NNI.

The message sequences in sections 3.2.3 to 3.2.6 of this document apply, with the difference that the IBCF and TrGW provide the interworking between the IMS network and the NNI to the peer IMS network. The call flows in this section build on those in section 3 and document the additions/differences from sections 3.2.3 to 3.2.6 to interconnect with peer IMS networks.

4.2.1 Basic VoLTE UE to Peer IMS Call Establishment – Originating Side

4.2.1.1 General

For calls originating on IMS and breaking out to a peer IMS network, the difference is that the originating S-CSCF shall recognise (via internal configuration data or ENUM) that the termination is not within this IMS network and may optionally invoke the BGCF to determine the destination network and to invoke the IBCF. The message sequence in section 4.2.1.2 thus portrays the S-CSCF, BGCF and IBCF and may be combined with the flow in section 3.2.3.2 starting at the point at which the S-CSCF propagates the SIP INVITE message to the terminating leg of the call.

4.2.1.2 Message Sequence

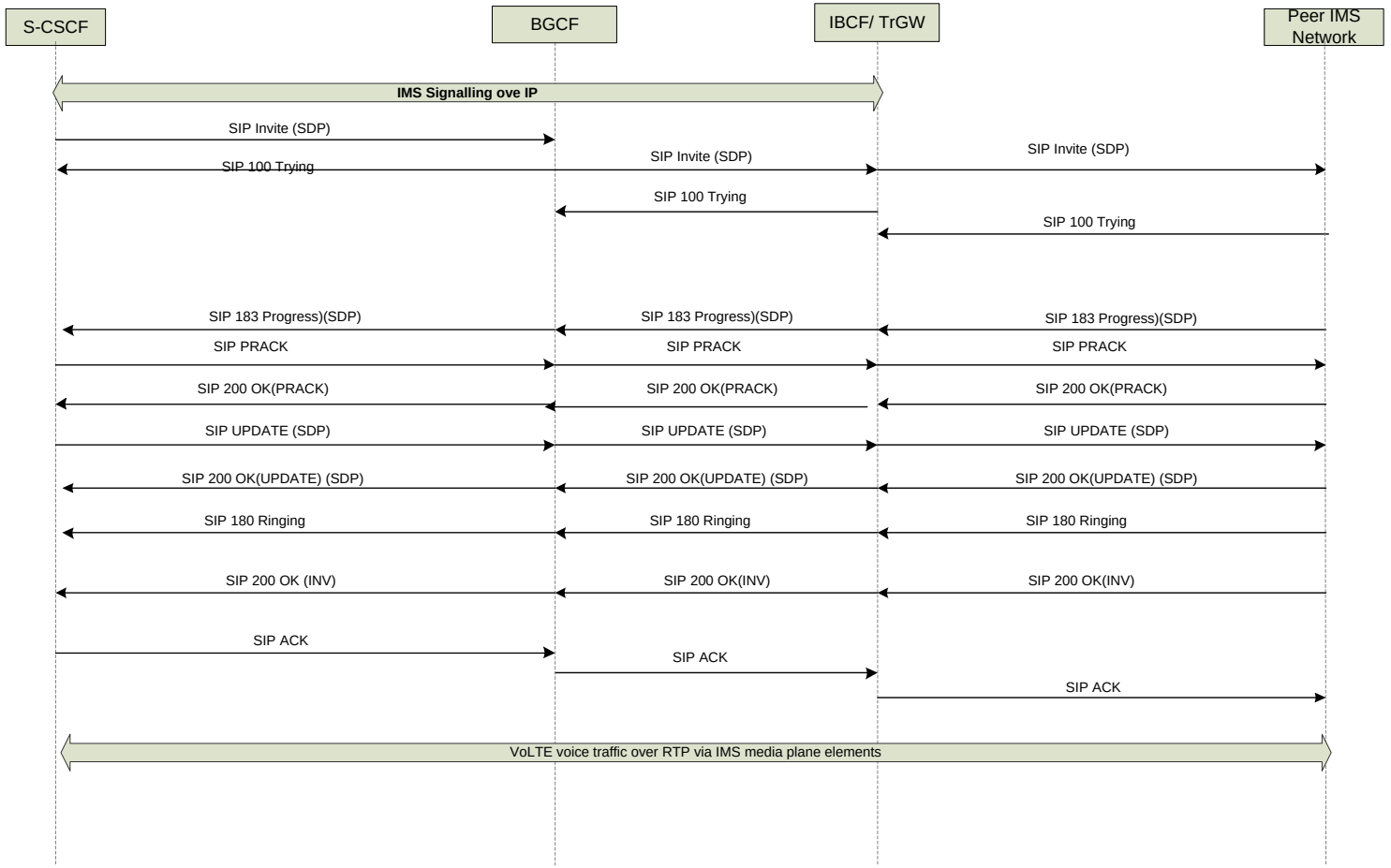

Figure 16: Basic VoLTE UE to Peer IMS Call Establishment – Originating Side

NOTE: The interaction with the PCC and the establishment of the dedicated bearer is as shown in figure 5.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [71].

NOTE: The BGCF may not remain in the signalling path. (see clause 5.6.2 of 3GPP TS 24.229 [9]).

4.2.1.3 Detailed Description

The S-CSCF determines that the Called-Party is not within this IMS network (i.e. ENUM lookup/internal configuration) and optionally forwards the SIP INVITE to the BGCF. Alternately, the S-CSCF may itself identify the correct IBCF as the egress point from this network. The rest of this section assumes that a BGCF is invoked by the S-CSCF.

The BGCF is responsible for selecting the appropriate control element for breaking out of this IMS network. The BGCF may use ENUM or internal configuration data to analyse the Request-URI to determine whether the destination is in a CS network or peer IMS network. In this case, the destination is in a peer IMS network and the BGCF is responsible for selecting the IBCF to handle the interconnect. The Request-URI can be a TEL URI or SIP URI but will contain an E.164 number The BGCF forwards the INVITE to the selected IBCF.

The IBCF is responsible for inter-working to the peer IMS network both in the control plane and media plane and shall follow the procedures of 3GPP TS 29.165 [24].

The IBCF selects the outgoing route to the peer network and controls one or more TrGWs over the Ix reference point (see 3GPP TS 29.238 [73]) to provide appropriate resources in the media plane. The selection in the IBCF is based on DNS or internal configuration data. Having selected a route, the IBCF shall invoke a TrGW to allocate and configure media resources for the call. The TrGW is an IP-IP GW and serves as a border element in the media plane in an IMS network.

The IBCF sends a SIP INVITE to the peer network, having modified the SIP headers as described in 3GPP TS 29.165 (e.g. Record-Route, Via, other local information that should not cross the trust boundary etc.) as well as overwriting the associated SDP to reflect the media pin-hole newly created on the TrGW.

The IBCF remains in the control path and transits all further SIP session establishment messages between the peer network and the home IMS network.

The IBCF transits the received 183 Progress (SDP) message followed by the associated PRACK and 200 OK (PRACK) messages (the 183 Progress message utilizes 100rel).

The IBCF transits the UPDATE (SDP) message and associated 200 OK (UPDATE) (SDP) message.
The IBCF uses the SDP offer/answer exchanges to modify the media pin-hole in the TrGW.

On receipt of a SIP 180 (Ringing) response from the peer network, the IBCF shall modify the TrGW to ensure a backward transmission path if the P-Early-Media header is present (and thus indicating that ring tone is being applied from the far end).

The 180 Ringing message is forwarded by the IBCF to the IMS network and is received by the S-CSCF and forwarded to the VoLTE UE to indicate a ringing tone to the subscriber. Note that the 180 Ringing message does not utilize 100rel.

When the peer network indicates that the call has been answered, the IBCF forwards the 200 OK (INVITE) message to its IMS network. This message is received by the S-CSCF

and forwarded to the P-CSCF. The IBCF shall ensure that duplex media can be conveyed via the TrGW at this point.

The VoLTE UE receives the 200 OK, and sends a SIP ACK message to acknowledge that the call has been established. The ACK is propagated through the IMS network to the IBCF and onto the peer network.

At this stage, the IMS-CS call is established with voice traffic sent over the dedicated bearer between the VoLTE UE and the peer network via the TrGW.

4.2.2 Basic VoLTE UE to Peer IMS Call Establishment – Terminating Side

4.2.2.1 General

For calls originating in a peer IMS network, the only difference is that the call enters the IMS network of the target user via an IBCF rather than a P-CSCF. The IBCF invokes an I-CSCF in order to determine the S-CSCF of the terminating user. The message sequence in section 4.4.2.2 thus portrays only the IBCF, I-CSCF and S-CSCF and may be combined with the flow in section 3.2.4.2 and starting at the point at which the S-CSCF is initially invoked with the SIP INVITE message.

4.2.2.2 Message Sequence

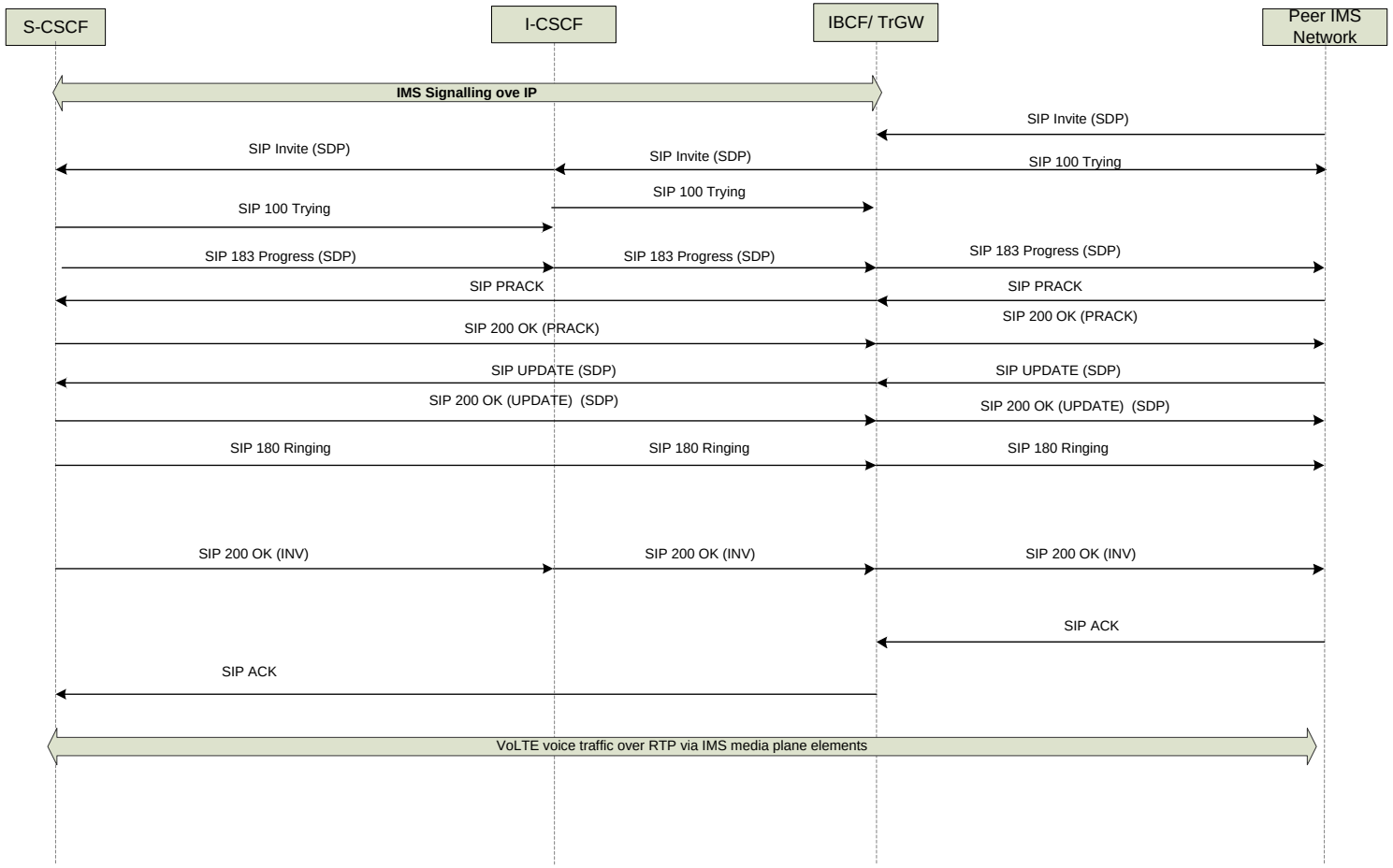

Figure 17: Basic VoLTE UE to Peer IMS Call Establishment – Terminating Side

NOTE: The interaction with the PCC and the establishment of the dedicated bearer is as shown in figure 6.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [71].

NOTE: The I-CSCF is a “stateful proxy” and remains in the signalling path only for the INVITE transaction.

4.2.2.3 Detailed Description

The peer IMS Network initiates the call establishment by sending a SIP INVITE to the IBCF. The IBCF shall follow the procedures of 3GPP TS 29.165 [24].

The IBCF invokes the TrGW over the Ix reference point (see 3GPP TS 29.238 [73]) to allocate media resources for the call.

The IBCF may modify the content of a number of the SIP headers in the SIP INVITE that are not required in the terminating network (e.g. Record-Route, Via etc.) as described in 3GPP TS 29.165 as well as overwriting the associated SDP to reflect the media pin-hole newly created on the TrGW.

The target user may be identified via a SIP or TEL-URI. In the former case, the SIP URI may contain a “user=phone” URI parameter and shall contain an E.164 number.

The IBCF invokes the I-CSCF to enable the appropriate S-CSCF for the target user to be found.
The I-CSCF interrogates the HSS to identify the S-CSCF where the user is registered and forwards the INVITE to the S-CSCF. The S-CSCF invokes any VoLTE services as triggered by the initial filter criteria and routes the SIP INVITE to the AS and terminating P-CSCF as described in section 3.2.4.

Call establishment proceeds as in section 3.2.4 and the IBCF forwards subsequent call establishment messages from the S-CSCF to the peer IMS network potentially modifying the content of SIP headers (e.g. Record-Route, Via, other local information that should not cross the trust boundary etc.) as described in TS 29.165 and modifying any SDP to reflect the media pin-hole in TrGW.

The IBCF transits the received 183 Progress (SDP) message followed by the associated PRACK and 200 OK (PRACK) messages (the 183 Progress message utilizes 100rel).

The IBCF transits the UPDATE (SDP) message and associated 200 OK (UPDATE) (SDP) message.
The IBCF uses the SDP offer/answer exchanges to modify the media pin-hole in the TrGW.

If the P-Early-Media header is present in the 180 (Ringing) message, then the IBCF shall ensure that backward media (e.g. ring tone, progress indications) are conveyed via the TrGW. This message does not utilize 100rel.

When the IMS network indicates that the call has been answered, the IBCF shall ensure that duplex media can be conveyed via the TrGW at this point.

At this stage, the call is established with voice traffic sent over the dedicated bearer between the VoLTE UE and the peer IMS network via the TrGW.

4.2.3 Basic VoLTE UE to Peer IMS Call Teardown - Initiated

4.2.3.1 General

This section describes the teardown of an interconnect call where the release is initiated by the VoLTE UE in this IMS network. The message sequence in section 4,2.3.2 portrays the S-CSCF, BGCF, IBCF and Peer IMS Network and may be combined with the flow in figure 7 and starting at the point at which the S-CSCF propagates the SIP BYE message to the terminating leg of the call.

4.2.3.2 Message Sequence

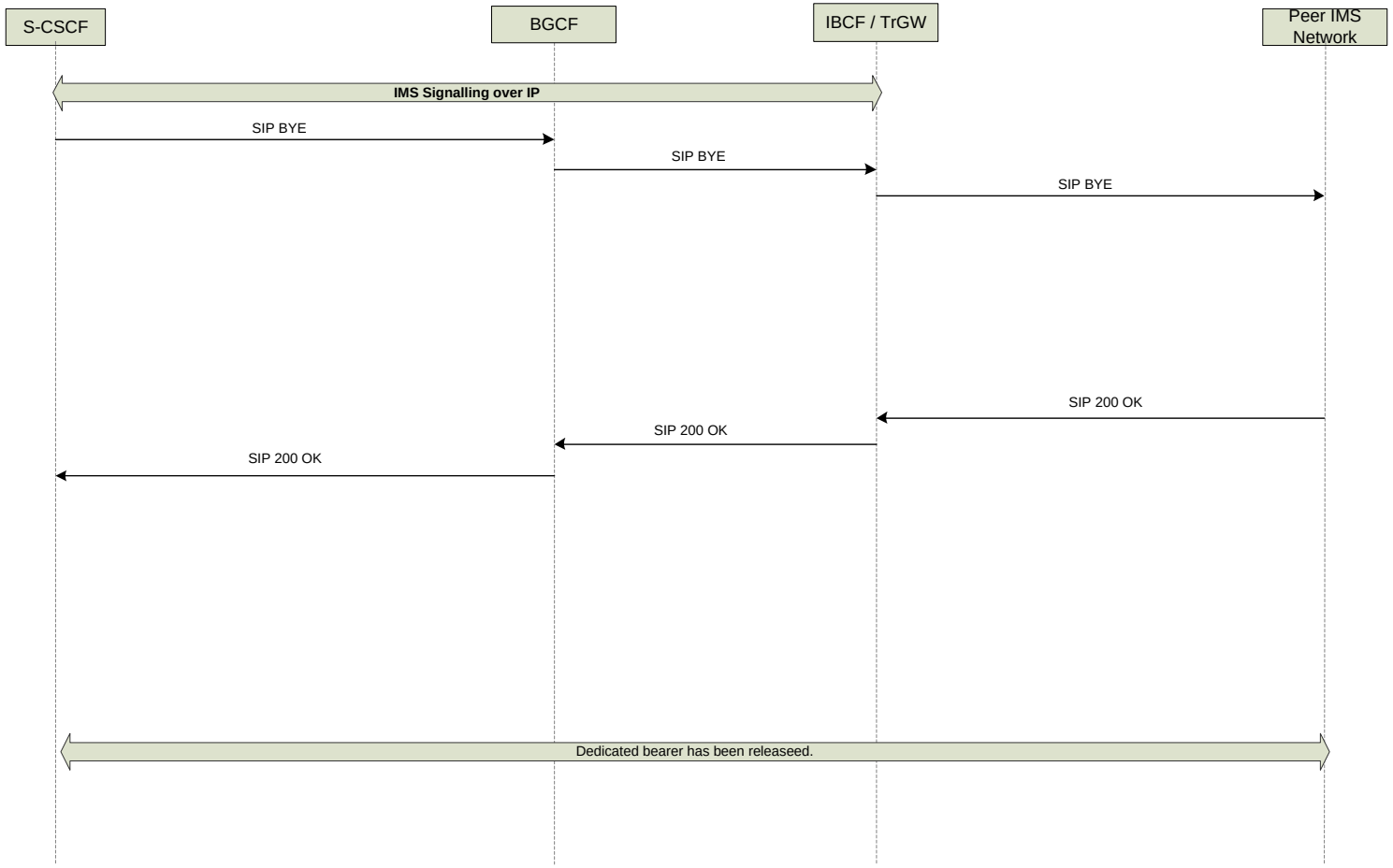

Figure 18: Basic VoLTE UE to Peer IMS Call Teardown – initiated

NOTE: The interaction with the PCC and the release of the dedicated bearer is as shown in figure 7.

NOTE: This figure shows a single offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [71]. A further offer/answer exchange could be used if required (e.g. if multiple codecs were returned in the SDP answer and the originating side wishes to specify a single codec). .

NOTE: The BGCF may not be in the signalling path. (see clause 5.6.2 of 3GPP TS 24.229 [9]).

4.2.3.3 Detailed Description

The call teardown is initiated in this IMS network via the VoLTE UE as described in section 3.2.6.2.

The S-CSCF propagates the SIP BYE message to the BGCF and onto the IBCF.

The IBCF releases the resources in the TrGW and sends a SIP BYE to the Peer IMS network (modifying SIP headers as described in TS 29.165).

On receipt of the 200 OK (BYE), the IBCF forwards the message to the IMS network (modifying headers as described in TS 29.165).

At this stage, the interconnect call is released and the dedicated bearer has been torn down as described in section 3.2.6.2.

4.2.4 Basic VoLTE UE to Peer IMS Call Teardown - Received

4.2.4.1 General

This section describes the teardown of an interconnect call where the release is initiated in the Peer IMS network. The message sequence in section 4.2.4.2 portrays the S-CSCF, IBCF and Peer IMS Network and may be combined with the flow in figure 8 and starting at the point at which the S-CSCF receives the SIP BYE message from the terminating leg of the call.

4.2.4.2 Message Sequence

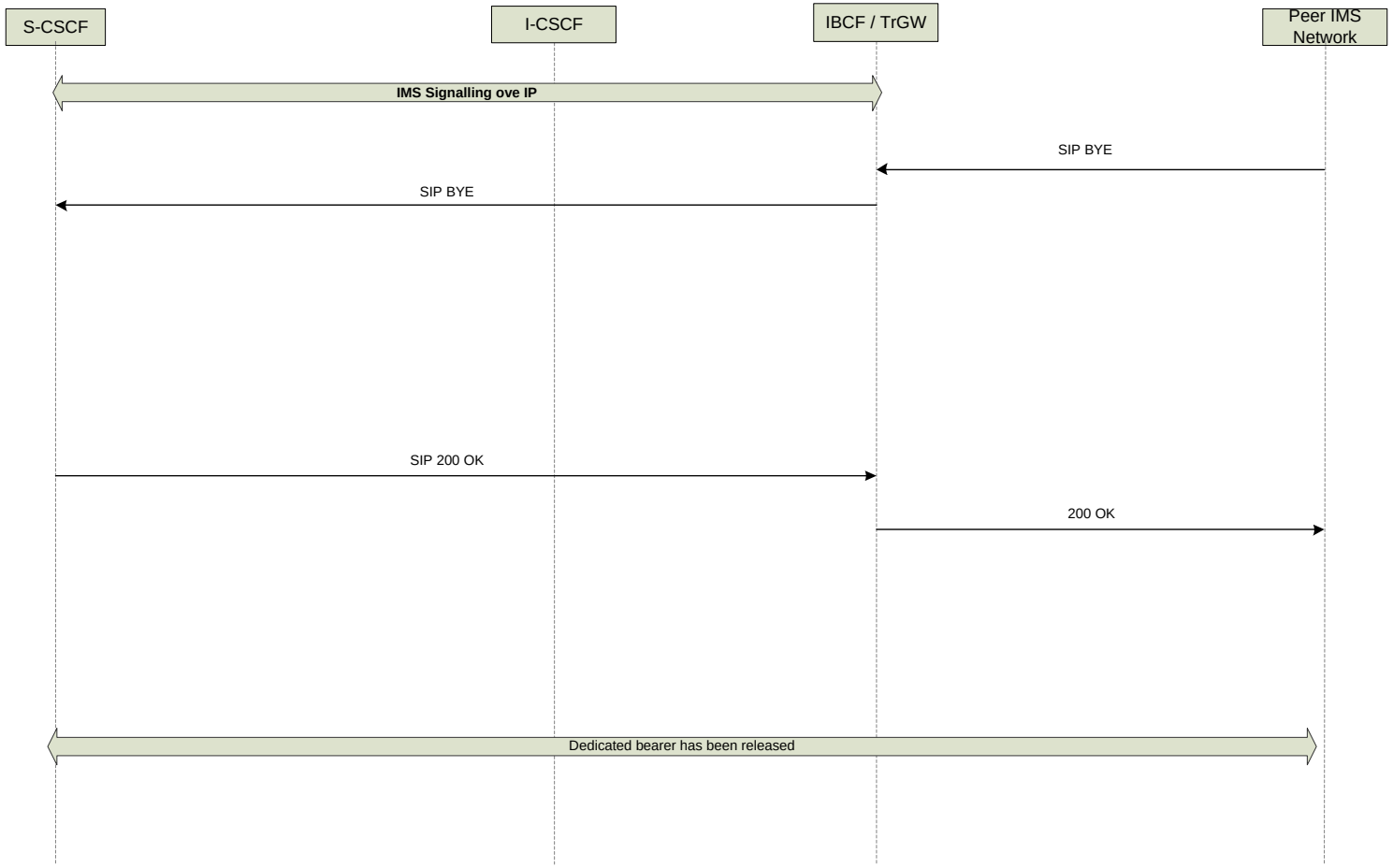

Figure 19: Basic VoLTE UE to Peer IMS Call Teardown - Received

NOTE: The interaction with the PCC and the release of the dedicated bearer is as shown in figure 8.

4.2.4.3 Detailed Description

The Peer IMS Network initiates the call teardown by sending a SIP BYE to the IBCF.

The IBCF releases the resources in the TrGW and forwards the SIP BYE to the S-CSCF (modifying headers as described in TS 29.165). The call release and release of the dedicated bearer at the UE side is as described in section 3.2.6.3.

The S-CSCF sends a 200 OK to the BYE to the IBCF.

The IBCF sends the SIP 200 OK to the Peer IMS network (modifying SIP headers as described in TS 29.165).

At this stage, the interconnect call is released and the dedicated bearer has been torn down as described in section 3.2.6.3.

4.3 Bi-lateral Interconnect

In this model, an IMS network has an IP route to its peer network. In architectural terms, the interconnect is realised via a point-point route between the border elements (IBCF/TrGW) in each network as described in 3GPP TS 29.165 [24]). The interconnect interface is realised via the Ici/Izi interfaces in the control/media plane respectively. In this scenario, both operators are responsible for screening of SIP/SDP traffic in accordance with the bi-lateral interconnection agreement.

4.3.1 Physical Configuration of Bi-lateral Interconnect

The physical interconnect may be realised via a direct leased line (e.g. Frame Relay or ATM based) or VPN connection (e.g. IPSEC connection) over the public internet. In either case, it is important that there is a SLA between the parties and that the connection is able to meet the requirements of that SLA. Such a SLA has been defined in PRD AA.80 [75] for IPX. However, the requirements for interconnect as defined for IPX are equally applicable to a bilateral interconnect.

4.3.2 Usage of ENUM/DNS

In order to be able to route calls between peer IMS networks, with a bi-lateral interconnect, translation between an E.164 number to SIP-URI and SIP-URI to IP address is required. This can be done via internal configuration data within network nodes or via ENUM.

When using ENUM, an ENUM look up within the the originating IMS network (e.g. from TAS, S-CSCF or BGCF) is used to retrieve the domain name of the terminating network. The Domain name is then together with configuration data used to determine the correct IBCF and the optimum IP Route to the target IMS Peer network.
In general, due to a combination of n/w transformation (i.e. porting of subscriber numbers from CS to IMS) and number portability, the correlation of destination telephone number and location (e.g. CS Network, peer IMS network etc.) is non-trivial and liable to be in a state of flux. The ENUM look up is constantly influenced by activities in other networks and thus may be centralised and managed by a trusted 3rd party (i.e. Carrier ENUM). Usage of ENUM is described in GSMA PRD IR.67 ([52]).

4.3.3 Usage of Session Border Controllers

4.3.3.1 General

The combination of an IBCF and TrGW realises a Session Border Control (SBC) at the edge of an IMS network and responsible for managing the Ici/Izi interfaces. The SBC checks the SIP/SDP to ensure conformance to the bi-lateral interconnection agreement.

4.3.3.2 Control Plane

The IBCF manages the control plane at an interconnect. Clause 6 of 3GPP TS 29.165 [24] describes procedures to be performed in the control plane although these procedures may be modified/extended for a given bi-lateral interconnection agreement. SBCs can also typically modify SIP signalling/headers in order to facilitate interworking between different implementations of SIP.

4.3.3.3 Media Plane

The TrGW manages the media plane at an interconnect, under the control of an IBCF. Clause 7 of 3GPP TS 29.165 [24] describes procedures to be performed in the medial plane. These include the creation of media pin holes to enable NAT of the media packets as well as policing the media flows to ensure that they are consistent with the associated control plane signalling and related bi-lateral interconnection agreement. DiffServ marking of media packets is also performed at the TrGW (under the control of the IBCF) – see section 3.7 for further information on Diffserv codepoints. Based on network policy and the bi-lateral agreement with the peer network, the TrGW may also perform transcoding. It is recommended that transcoding be avoided in the TrGW if possible.

4.4 IPX-Based Interconnect

The IPX is defined in GSMA PRD IR.34 [48] and provides an IP interconnect network to enable connectivity between Operator's IMS networks. Thus, the use of an IPX requires only a 1:1 relationship to be configured by an N/W Operator rather than 1:N relationships and many bilateral inter-connects to other peer networks. Therefore, an IPX based interconnect is the recommended option. In this scenario, the IPX can perform screening of SIP/SDP traffic on behalf of the Operator in accordance with the per-operator interconnection agreement.

4.4.1 Configuration of IPX-based Interconnect

IR.34 defines three modes for IPX based interconnect, namely :-

- Transport-Only Connectivity - , a bilateral agreement between Service providers using the IPX transport layer with guaranteed QOS (IPX-edge to IPX-edge).
- Bilateral Service Transit Connectivity - , a bilateral agreement between Service providers using the IPX Proxy Functions and IPX transport layer with guaranteed QOS end-end. This model provides the opportunity to include service based interconnect charging to the transport charging of the previous model
- Multilateral Service Hub Connectivity – this model provides multi-lateral interconnect with guaranteed end-end QOS and service based charging. Traffic may be routed from one Service Provider to many destinations via a single agreement with the IPX provider. The hub functionality is provided by IPX Proxies.

Due to the complexity associated with network transformation and number portability, as well as the emergence of multi-services via IMS, it makes sense in the long term to utilise the multi-lateral service hub IPX option. This option simplifies the interconnect mapping for the relatively many IPX clients as well as insulating the IPX clients from being directly impacted due to numbers being ported between destination networks as well as the introduction of new services.

4.4.2 Usage of ENUM/DNS

This is as for section 4.3.2.. In some cases, it may be possible to dispense with the ENUM dip the originating network due to all off-net calls being handed to the IPX as default. Given the flux of mapping destination addresses to destination networks, centralization of the ENUM data for inter-operator look-up is recommendedso as to avoid changes rippling through local configuration data as numbers become relocated (i.e. utilising Carrier ENUM). Usage of ENUM is described in GSMA PRD IR.67 ([52]).

4.4.3 Usage of Session Border Controllers

4.4.3.1 General

As for section 4.4.2.1,with the SBC (IBCF/TrGW) interfacing between then Operator and the IPX. The Operator may choose to outsource the deployment of the SBC to the IPX Provider, deploy an SBC within its own network or combine both.

Where an IPX deploys an SBC, the screening of SIP/SDP by the IPX on a per operator basis provides a more scalable approach than the bi-lateral case as the IPX Provider manages the inter-Operator connectivity. It is an operator policy decision as to the extent that its own SBCs perform SIP/SDP screening when such screening is being performed by the IPX.

4.4.3.2 Control Plane

As for section 4.4.2.2 but done on a per operator basis

4.4.3.3 Media Plane

As for section 4.4.2.3 but done on a per operator basis. .

4.5 CS Interconnect

It is also possible that a given endpoint resides in the CS Network of another operator. In this case, the call flows would be identical to those in section 3.3. This scenario is mentioned here only for completeness.

4.6 Charging

Charging within each network is as for section 3.15. In addition, each peer at an interconnect will also perform route accounting at the interconnect point to enable the relative call total in each direction to be billed appropriately. This mechanism is identical to the current mechanisms used at operator interconnect points in the CS Network.

5 VoLTE Implementation - Roaming

This section builds on the single PMN scenario in section 3 and considers inter-operator VoLTE roaming between PMNs. The roaming user attaches in a visited network and registers for IMS services in its respective home network. As recommended in GSMA PRD IR.65 [51], it is assumed that the local breakout model is used whereby the full EPC and P-CSCF are located in the visited network for the roaming user. The P-CSCF then interacts with the S-CSCF and TAS in the home network for the provision of VoLTE services. Local breakout also places requirements on the Diameter routing between the home and visited networks to convey the S6a and optionally S9 interfaces respectively.

Note:- S9 may be optionally used to convey Rx messages between the home and visited networks for dynamic policy control and the subsequent text and message flows assume dynamic policy control. The deployment of the S9 interface is determined on a bi-lateral operator agreement. It is also possible to use static policy control where the local configuration data is stored in the V-PCRF, in which case the S9 interaction does not occur. However, in this document, all message flows show S9 being utilised.

Note: The subsequent text and message flows in this section assume a separate P-CSCF and IBCF. However, it is also noted that the P-CSCF may be co-located with an IBCF (i.e. combined access and network side SBC).
This section describes the implementation for these scenarios.

5.1 General

The VoLTE architecture for a PMN deployment supporting roaming is shown in Figure 20.

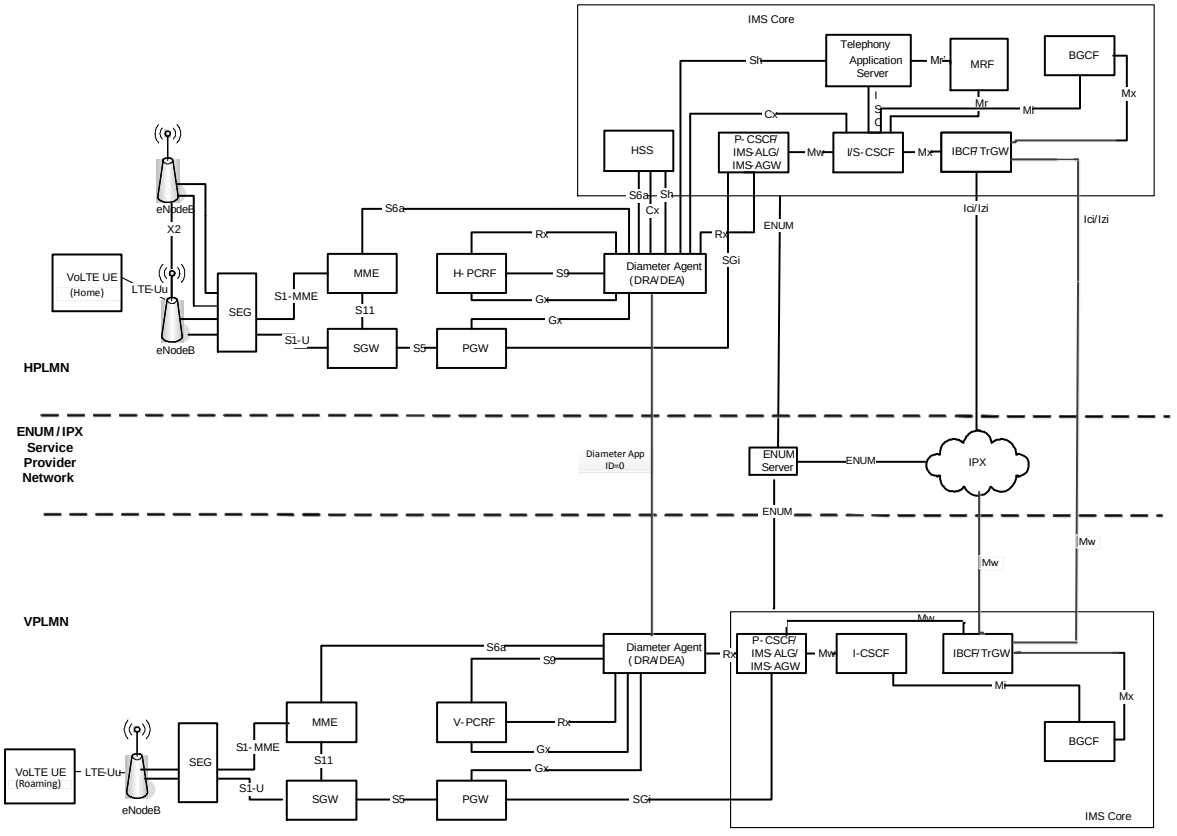

Figure 20: Roaming VoLTE deployment

NOTE: The Gm interface (UE to P-CSCF) is included in the Intra-PMN VoLTE deployment although not shown in the above figure.

NOTE: The Ut interface (UE to TAS) is included in the VoLTE architecture although not shown in the above figure.

5.2 VoLTE Roaming Basic Call Flows

The VoLTE basic call flows are in accordance with 3GPP specifications for E-UTRAN/EPC, IMS, and PCC. Please refer to 3GPP TS 23.401 [6], 3GPP TS 23.228 [5], and 3GPP TS 23.203 [4] respectively for further detailed information.

The following sub-sections define the additional requirements for the VoLTE service. References to specific functionality within GSMA PRDs (e.g. IR.92, IR.65, IR.80) and 3GPP specifications will be made within each sub-section. It is assumed that there is a roaming agreement between the home network of the UE and the visited network in which the UE is and appropriate configuration data has been set up in each network.

In particular, this section will highlight the key differences from the corresponding flows for a non-roaming UE as described in section 3.2 and (where possible) shall refer to text that is common for roaming and non-roaming scenarios.

5.2.1 Roaming VoLTE UE Attachment and IMS Registration

5.2.1.1 General

As section 3.2.1.1, apart from the UE roaming and thus attaching to a visited network.

5.2.1.2 Message Sequence

Figure 3 show the message sequences for the LTE Attachment and IMS Registration for a roaming UE.

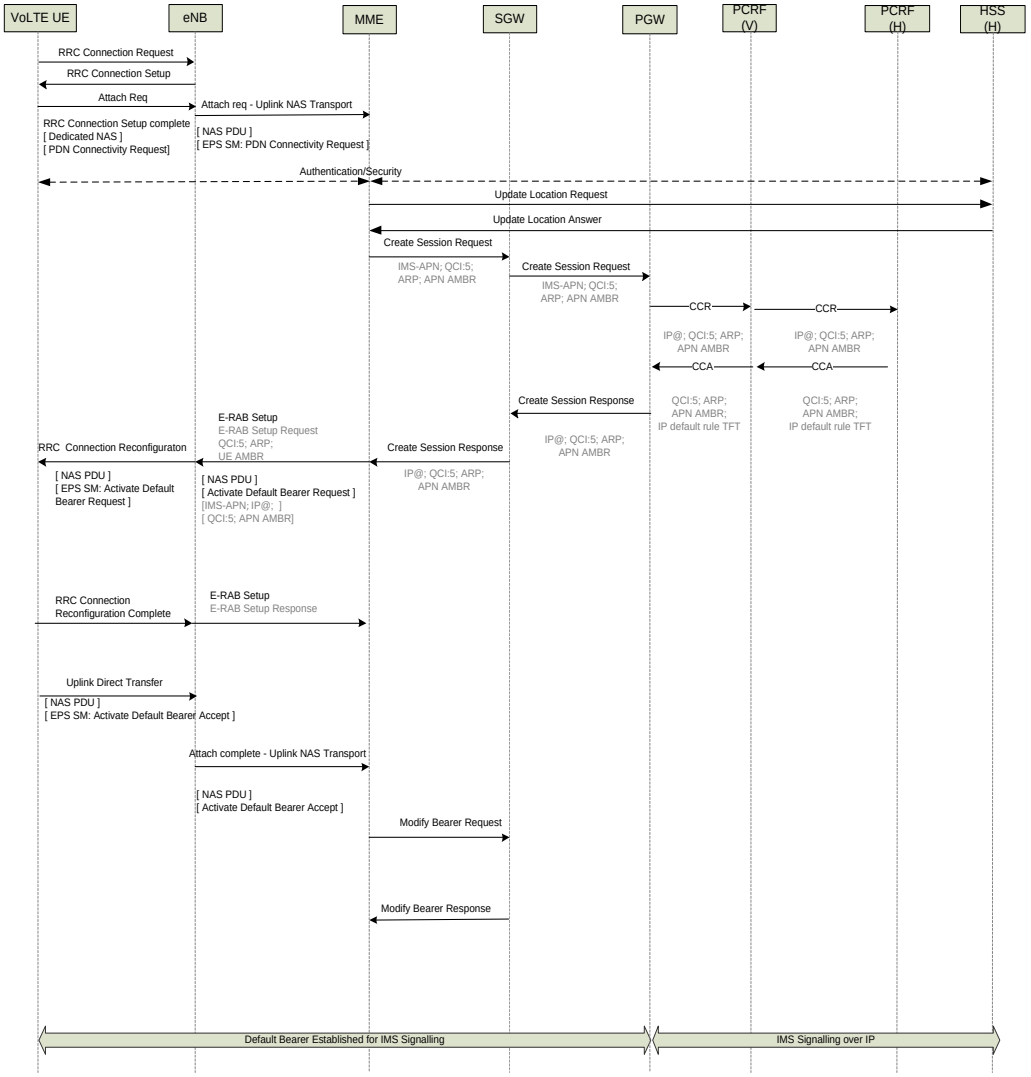

Figure 21: Roaming VoLTE UE Attachment

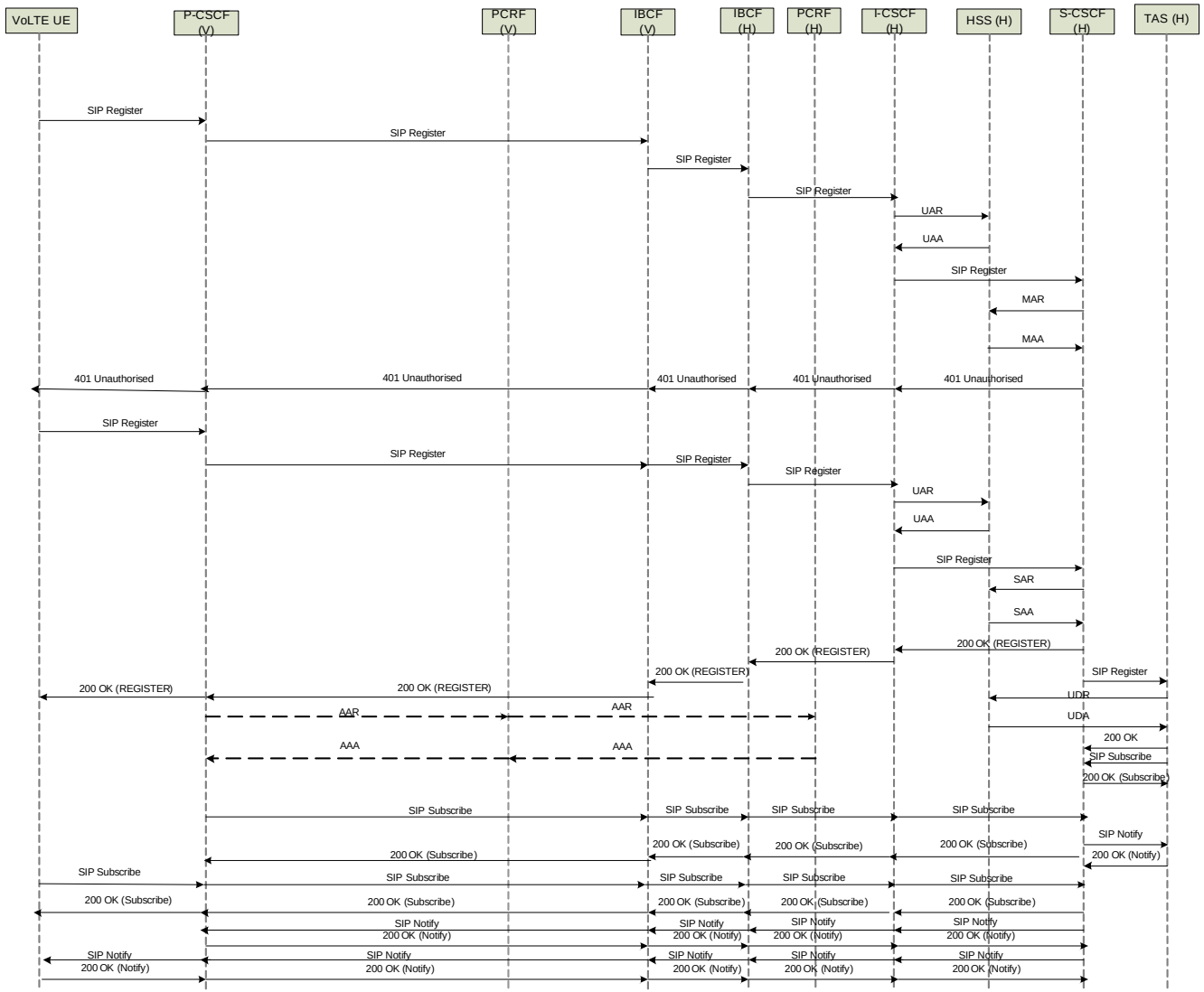

Figure 22: Roaming VoLTE UE Initial IMS Registration message sequence

NOTE: The Diameter Agents have not been included in this message sequence, although Diameter messages shall route via the Diameter Agents in the home and visited networks. Usage of Diameter Agents is described in section 3.6.

5.2.1.3 Detailed Description

5.2.1.3.1 Roaming VoLTE UE Attach

As section 3.2.1.3.1, with differences specific to the roaming scenario described in this section.

The UE has a list of foreign/visited networks to which it can attach. The UE initiates an attach to the eNodeB as in the single network scenario.

The MME shall validate that the UE is permitted to attach and shall send the Update Location to the HSS in the UE's home network. This message shall be sent via the DRA/DEA in each network.

As in the single network case, if the initial LTE attach is for VoLTE service, there shall not be an APN included in the attach request. The default APN configured in the HSS shall be set as the IMS-APN, and the HSS returns the IMS-APN name for establishment of the default bearer. If the initial LTE attach is not for VoLTE service (e.g. internet), the UE shall specify the IMS-APN in a subsequent PDN connection request as specified in clause 5.10.2 of 3GPP 23.401 [6]) and defined within IR.88 [53]. In either case, the APN-OI information is inserted by the MME which enables the UE to attach to a P-CSCF in the visited network.

The MME initiates a Create Session Bearer request to the SGW to create a default bearer for VoLTE IMS signalling as for the non-roaming case.

The PGW allocates an IP Address for the UE and utilises dynamic PCC to initiate a Credit Control Request to the PCRF (in the visited network) to obtain the default PCC rules for the default bearer to be used for IMS signalling. In the roaming scenario, the PCRF in the visited network notes that the IMSI is for a visiting UE and sends the CCR message to the PCRF in the corresponding home network. This message is used to request default QOS parameters from the home network and also to establish the S9 interface between the visited and home network PCRFs (see 3GPP TS 29.215 [27]). The home PCRF responds with a CCA message and returns the default QOS parameters and indicates that S9 is now established. The S9 interface shall be used to tunnel subsequent Rx messages between the PCRFs for session establishment and teardown. The CCA is forwarded to the PGW by the visited network PCRF.

Note :- The above description of the S9 interface assumes that dynamic policy rules must be exchanged between the home and visited network. It is also possible (as documented in GSMA IR.88 section 3.3. to use static policy control in which case Rx need not be tunnelled between the home and visited networks.

On receipt of the CCA from the visited network PCRF into the PGW, the default bearer is established as described for the non-roaming case.

At this stage, the roaming VoLTE UE is attached to the visited network via a default bearer that is established for IMS Signalling.

5.2.1.3.2 Roaming VoLTE UE Initial IMS Registration

As section 3.2.1.3.2, with differences specific to the roaming scenario described in this section.

The roaming VoLTE UE initiates as SIP REGISTER to the P-CSCF, which is located in the visited network.

The P-CSCF receives the SIP REGISTER request from the UE and inserts a Path header with a SIP-URI identifying the P-CSCF for routing, a P-Charging-Vector header with the icid-

value, a P-Visited-Network-ID to identify the P-CSCF's network domain. In the roaming case, the domain in Request-URI is recognised as being a foreign domain and the P-CSCF thus forwards the request to the IBCF via local configuration data or DNS as described in clause 5.2.2.1 of 3GPP TS 24.229 ([9]). .

The visited network IBCF passes the REGISTER message to its peer in the home network of the roaming UE. The IBCF may modify the SIP headers in the REGISTER message (e.g. for topology hiding) as described in 3GPP TS 29.165 [24]. In particular, the IBCF shall modify the Path header to add its own SIP-URI.

The REGISTER is received by the IBCF in home network of the roaming UE. The home network IBCF modifies the SIP REGISTER in a similar manner to its peer in the visited network. The IBCF passes the REGISTER to the I-CSCF.

As described in section 3.2.1.3.2, the I-CSCF queries the HSS to perform validation checks on the user identity and obtain the identity of the appropriate S-CSCF. The I-CSCF invokes the S-CSCF which retrieves authentication data from the HSS and sends a 401 Unauthorised response to the REGISTER.

The 401 Unauthorised response is transited via the IBCFs to the P-CSCF which modifies the response as described in section 3.2.1.3.2 and creates a temporary set of security associations prior to passing the response to the roaming UE.

As described in section 3.2.1.3.2., the UE re-sends the SIP REGISTER populated with the Authiorization header.

As in section 3.2.1.3.2, the P-CSCF checks the temporary security associations, and verifies the security related information received from the UE prior to forwarding the REGISTER to the IBCF.

The IBCF sends the REGISTER to its peer in the UE’s home network which invokes the I-CSCF. The I-CSCF uses the User Authorization Request message to retrieve the S-CSCF name stored within the HSS, and forwards the request to the relevant S-CSCF.

The S-CSCF validates the security parameters in the REGISTER message and then downloads user profile data from the HSS. The S-CSCF binds the P-CSCF address to the user’s contact (to be used to route future requests to the user) and returns a 200 OK response containing a SERVICE-ROUTE header.

The 200 OK (REGISTER) response traverses the IBCFs and is conveyed to the P-CSCF. In accordance with 3GPP TS 24.229, the IBCFs must not modify the SERVICE-ROUTE header and pass it on unchanged as received from the S-CSCF.

As in section 3.2.1.3.2, the P-CSCF changes the temporary set of security associations to a newly established set of security associations. It protects the 200 OK with these associations and sends the 200 OK to the VoLTE UE. All future messages sent to the UE will be protected using the security associations.

The P-CSCF optionally sends an AAR message to the PCRF to perform application binding to the default bearer (i.e. the P-CSCF is requesting to be informed in the event of the default bearer being lost/disconnected in order to trigger an IMS de-registration). In the roaming scenario, the visited network P-CSCF passes the message to the visited PCRF and onto home PCRF over the S9 interface if implemented. The AAA is sent back from the home network PCRF over S9, if implemented, to the visited network PCRF. The visited network PCRF sends the AAA onto the P-CSCF. Note that if application session binding is not performed, then IMS learns of the loss of the default bearer by other means (e.g. timeout when attempting to send a SIP message to the UE).

As in section 3.2.1.3.2, the UE changes the temporary security association to a newly established set of security associations that will be used for further messages to the P-CSCF.

As in section 3.2.1.3.2, 3rd party registration occurs from the S-CSCF to the TAS and the UE, P-CSCF and TAS shall subscribe to the registration event package to be notified of any change of registration state of the public user identity and be notified of the registration state via a SIP NOTIFY message.

The SUBSCRIBE and NOTIFY messages between the UE and P-CSCF to the S-CSCF shall be conveyed via the pair of IBCFs.

The VoLTE UE is now registered with the IMS network for VoLTE services, with SIP signalling being transported over the default EPC bearer. The signalling path from the UE to the S-CSCF in the home network traverses the P-CSCF and IBCF pair (as determined by the SERVICE-ROUTE header returned in the 200 OK (REGISTER) response.

5.2.2 Roaming VoLTE UE Initiated Detach and IMS Deregistration

5.2.2.1 General

As for the single network case, a roaming VoLTE UE shall automatically deregister from IMS before performing an LTE Detach, if the UE is not moving to another access technology that supports Voice over IMS.

5.2.2.2 Message Sequence

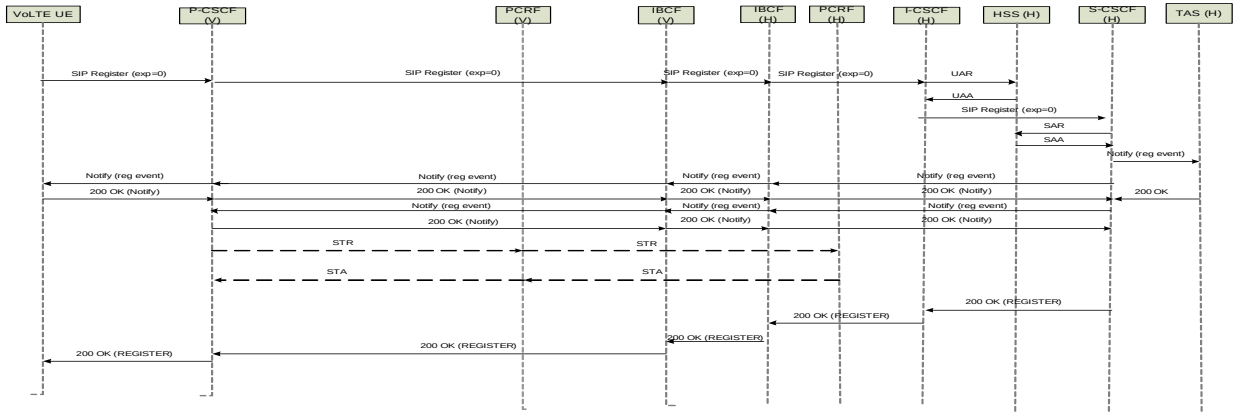

Figure 23: Roaming VoLTE UE IMS Deregistration message sequence

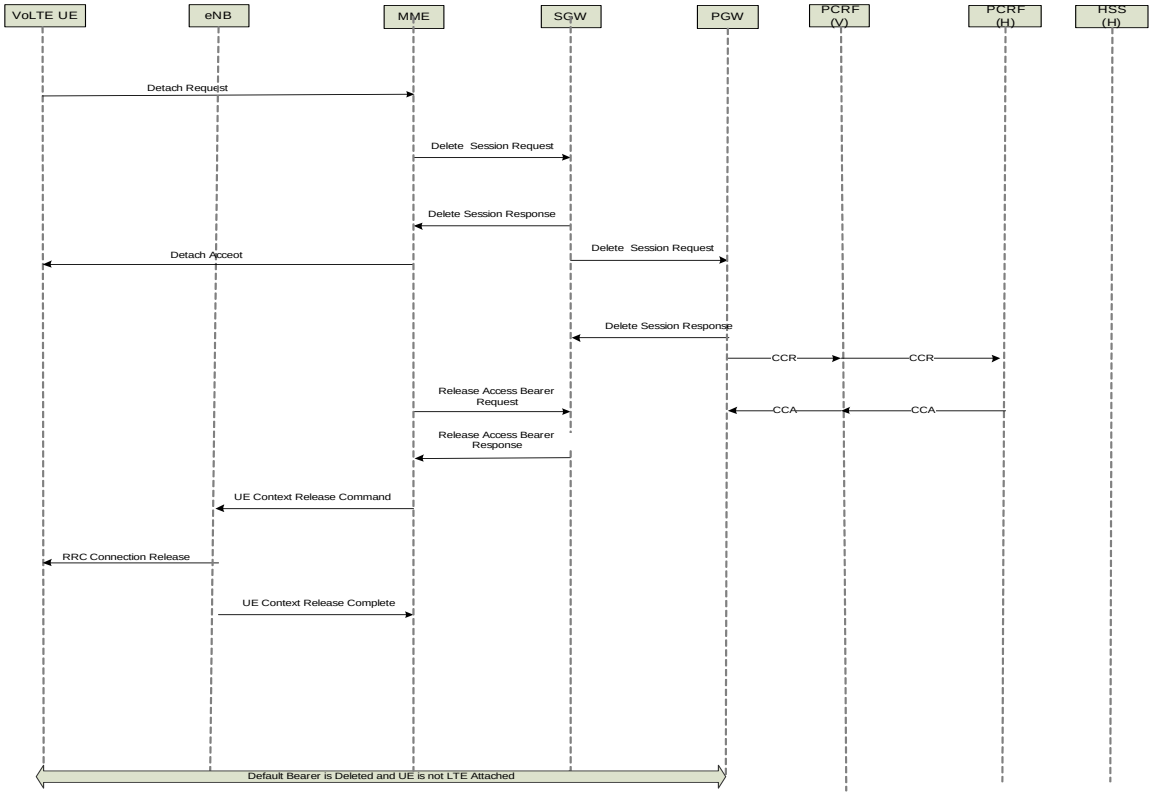

Figure 24: Roaming VoLTE UE Initiated Detach

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 5.6.

5.2.2.3 Detailed Description

5.2.2.3.1 IMS Deregistration (Roaming)

As section 3.2.2.3.1, with differences specific to the roaming scenario described in this section.

The SIP REGISTER (exp=0) message is forwarded to the I-CSCF via the P-CSCF and IBCFs. The I-CSCF uses the User Authorization Request to retrieve the S-CSCF name stored within the HSS and forwards the REGISTER (exp=0) to the S-CSCF.

The S-CSCF informs the HSS of the de-registration and the HSS shall keep the S-CSCF name associated to the public user identity for future use and to enable unregistered services to be applied (e.g. routing of a terminating voice call to voicemail) as in the single network case.

The S-CSCF shall send a SIP NOTIFY to the P-CSCF, TAS and VoLTE UE to notify them of the change of the registration state.

The P-CSCF, on being notified of the de-registration, optionally sends a STR message to the PCRF to remove the application binding to the default bearer (if application session binding was done previously). In the roaming scenario, the STR is sent over the S9 interface, if implemented, to the PCRF in the home network. The home network PCRF responds with a STA over S9 if implemented to the visited PCRF. The visited PCRF sends the STA to the P-CSCF. The P-CSCF shall also remove the security associations that were established between the P-CSCF and the UE as in the single network case.

The S-CSCF shall send a 200 OK to acknowledge the de-registration.

The P-CSCF shall forward the 200 OK to the UE.

On receiving the 200 OK responses, the UE shall remove all the registration details for the Public User Identity and delete the stored security associations. The UE shall consider the subscription to the registration event package as cancelled.

The roaming VoLTE UE is now de-registered from the IMS network for VoLTE services, no further SIP signalling is being transported over the default EPC bearer.

5.2.2.3.2 Roaming VoLTE UE Detach

The detach procedure is as described in section 3.2.2.3.2. Where the S9 interface is implemented, the CCR message from the visited network PCRF is forwarded to the home PCRF over S9. The CCR message shall also result in the termination of the S9 session between the visited and home PCRFs (see TS 29.215 [27]). The home PCRF shall respond with a CCA to the visited PCRF.

The default bearer is released as in the single network case and the VoLTE UE is no longer attached to the network.

5.2.3 Roaming VoLTE UE to VoLTE Call Establishment – Originating Side

5.2.3.1 General

As section 3.2.3.1 with differences specific to the roaming scenario described in this section.

The essential differences from the single network scenario are that the Mw reference point is conveyed via the IBCFs between the P-CSCF in the visited network and the S-CSCF in the home network. Where S9 interface is deployed, the Rx messages related to the establishment of the dedicated bearer are sent via the visited and home network PCRFs.

The interactions between the visited network PCRF and the EPC/UE are identical to the single network case. Therefore, the message flows in this section will show the SIP signalling and Diameter Rx and Gx signalling only – the latter to indicate the points at which the EPC is invoked. .

As for the single network case, a roaming VoLTE UE, shall perform call establishment by using the IMS network. The IMS Signalling shall be sent over the default bearer, and a new dedicated bearer shall be dynamically established for the voice traffic.

5.2.3.2 Message Sequence

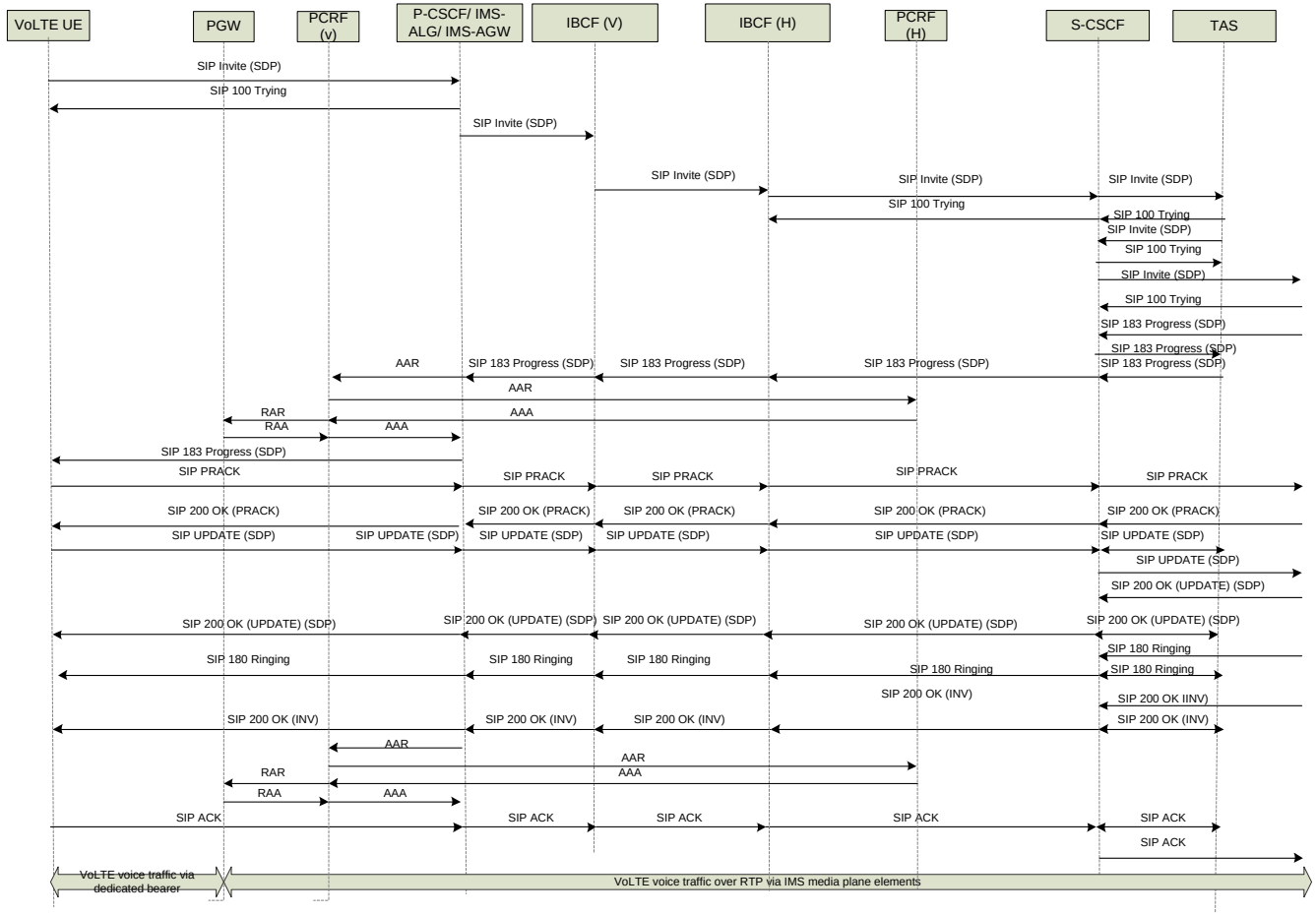

Figure 25: Roaming VoLTE UE to VoLTE UE Call Establishment - Originating Side message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 5.6.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [71].

NOTE: The figure shows the PCRF being invoked only once on receipt of the of the SDP answer (uplink & downlink configuration). It is also possible to invoke the PCRF twice, i.e. on receipt of both the SDP Offer (downlink configuration) and SDP Answer (uplink configuration). Both options are valid – see 3GPP TS 29.213 ([79]) annex B.

NOTE: The PRACK and 200 OK (PRACK) messages also traverse through the AS but this is not shown.

5.2.3.3 Detailed Description

As section 3.2.3.3 with roaming specific differences highlighted in this section.

The P-CSCF will also invoke the IMS-AGW over the Iq reference point (see TS 23.334 [74]) to provide appropriate resources in the media plane as for the single network scenario if an IMS ALG/AGW is deployed.

The P-CSCF may modify the SDP as for the single network case (if applicable) and forwards the SIP INVITE to the S-CSCF. In the roaming case, the S-CSCF is resident in the home network of the user. Therefore, the INVITE traverses the pair of IBCFs in the visited and home networks respectively prior to being received by the S-CSCF. Each IBCF shall invoke its respective TrGW to allocated media resources for the session and shall modify the SDP in accordance with the newly created media pin-holes. The IBCFs shall also modify the SIP headers as described in 3GPP TS 29.165.

On receipt of the INVITE, the S-CSCF behaves as for the single network case and invokes the TAS apply VoLTE supplementary services prior to invoking the terminating leg of the call. In this case, the S-CSCF determines that the Called-Party is within the home network (i.e. ENUM lookup/internal configuration) and routes the SIP INVITE to the I-CSCF to determine the terminating S-CSCF of the Called-Party (see section 3.2.4 for terminating call establishment to a non-roaming VoLTE UE).

The called party's VoLTE UE sends a 183 Progress (SDP) message with the SDP answer. This is received by the S-CSCF and forwarded to the visited network P-CSCF via the IBCFs in the home and visited networks. On receipt of a SIP 183 Progress response containing the SDP answer, each IBCF shall modify its TrGW to reflect the SDP answer and update the SDP answer to reflect the respective media pin-holes in the TrGWs. The 183 Progress (SDP) message is forwarded to the P-CSCF.

The SDP answer in the 183 Progress response shall indicate a single voice codec and that QOS preconditions are required but not yet met at the terminating side. As in the single network scenario, the P-CSCF uses the SDP answer to configure the IMS-AGW (if deployed) and sends the Authorize/Authenticate-Request message to the visited network PCRF with the related updated service information (IP address, port numbers, information on media-type) specifying the access facing IP address of the IMS-AGW.

The PCRF in the visited network sends the AAR message to its peer in the home network of the user via the S9 reference point if implemented. In this case, the home network PCRF authorises the request and responds to the visited PCRF with an Authorize/Authenticate-Answer (AAA) and both PCRFs associate the service information to the stored subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information. The visited network PCRF identifies the affected IP-CAN session (e.g. default bearer) that has been established during the LTE Attach procedure,

and initiates a Re-Auth-Request to the PGW to initiate the creation of a dedicated bearer as described in the single network scenario.

The PGW acknowledges the Re-Auth-Request to the visited network PCRF, which then acknowledges the Authorize/Authenticate-Request message sent from the P-CSCF. At this point the IMS SIP session and the dedicated bearer used for voice are bound together via PCC.

The PGW sends the Create Bearer Request to the SGW to create the dedicated bearer for VoLTE media as described in the single network scenario.

The P-CSCF forwards the SIP 183 Progress response to the VoLTE UE. This message shall also utilize 100rel and the UE shall generate a PRACK which is transited to the terminating side of the call via the IBCFs .

A 200 OK (PRACK) is received from the terminating side of the call via the IBCFs.

The VoLTE UE now sends a SIP UPDATE message containing a new SDP offer as in the single network case. This message is transited via the P-CSCF to the S-CSCF via the IBCFs and onto the terminating leg of the call.

A SIP 200 OK (UPDATE) message containing the SDP answer is sent from the terminating leg of the call to the S-CSCF and onto the VoLTE UE via the P-CSCF and IBCFs.

The terminating UE is now alerted and a SIP 180 Ringing message is sent from the terminating leg of the call. This message is received by the S-CSCF and sent through to the originating UE via the pair of IBCFs and P-CSCF. This message does not utilize 100rel. The P-Early-Media header is not present and so the UE will generate local ring tone to the subscriber.

When the called party's VoLTE UE has answered the call, it sends a 200 OK to the calling party VoLTE UE. This is received by the S-CSCF and forwarded to the P-CSCF via the IBCFs. Each IBCF shall ensure that duplex media can be conveyed via their respective TrGWs.

The P-CSCF sends an AAR message to the visited PCRF to enable the uplink and downlink media flows. This message is conveyed to the home PCRF over S9 if implemented. In this case, the home PCRF authorizes the request and responds with an AAA message to the visited PCRF which invokes the P-GW to enable the media flows. The visited network PCRF sends the AAA message to the P-CSCF. As in the single network scenario, the P-CSCF(IMS-ALG) also invokes the IMS-AGW (if deployed) to ensure that duplex media can be conveyed via IMS-AGW at this point.

The P-CSCF forwards the SIP 200 OK (INVITE) to the VoLTE UE.

The VoLTE UE receives the 200 OK, disconnects ring tone and sends a SIP ACK message to acknowledge that the call has been established. The ACK message is sent to the terminating leg of the call via the IBCFs.

At this stage, the VoLTE UE has a call established with voice traffic sent over the dedicated bearer and via the IMS-AGW and pair of TrGWs. Support of Robust Header Compression is mandated and described in GSMA PRD IR.92 [54] section 4.1.

.The IMS Signalling is sent over the default bearer.

5.2.4 Roaming VoLTE UE to VoLTE UE Call Establishment – Terminating Side

5.2.4.1 General

As section 3.2.4.1, with differences specific to the roaming scenario described in this section.

The essential differences from the single network scenario are that the Mw reference point is conveyed via the IBCFs between the P-CSCF in the visited network and the S-CSCF in the home network and that the Rx messages related to the establishment of the dedicated bearer are sent via the visited and home network PCRFs over the S9 reference point. The interactions between the visited network PCRF and the EPC/UE are identical to the single network case. Therefore, the message flows in this section will show the SIP signalling and Diameter Rx and Gx signalling only – the latter to indicate the points at which the EPC is invoked. .

As for the single network case, a roaming VoLTE UE, shall perform call establishment by using the IMS network. The IMS Signalling shall be sent over the default bearer, and a new dedicated bearer shall be dynamically established for the voice traffic.

5.2.4.2 Message Sequence

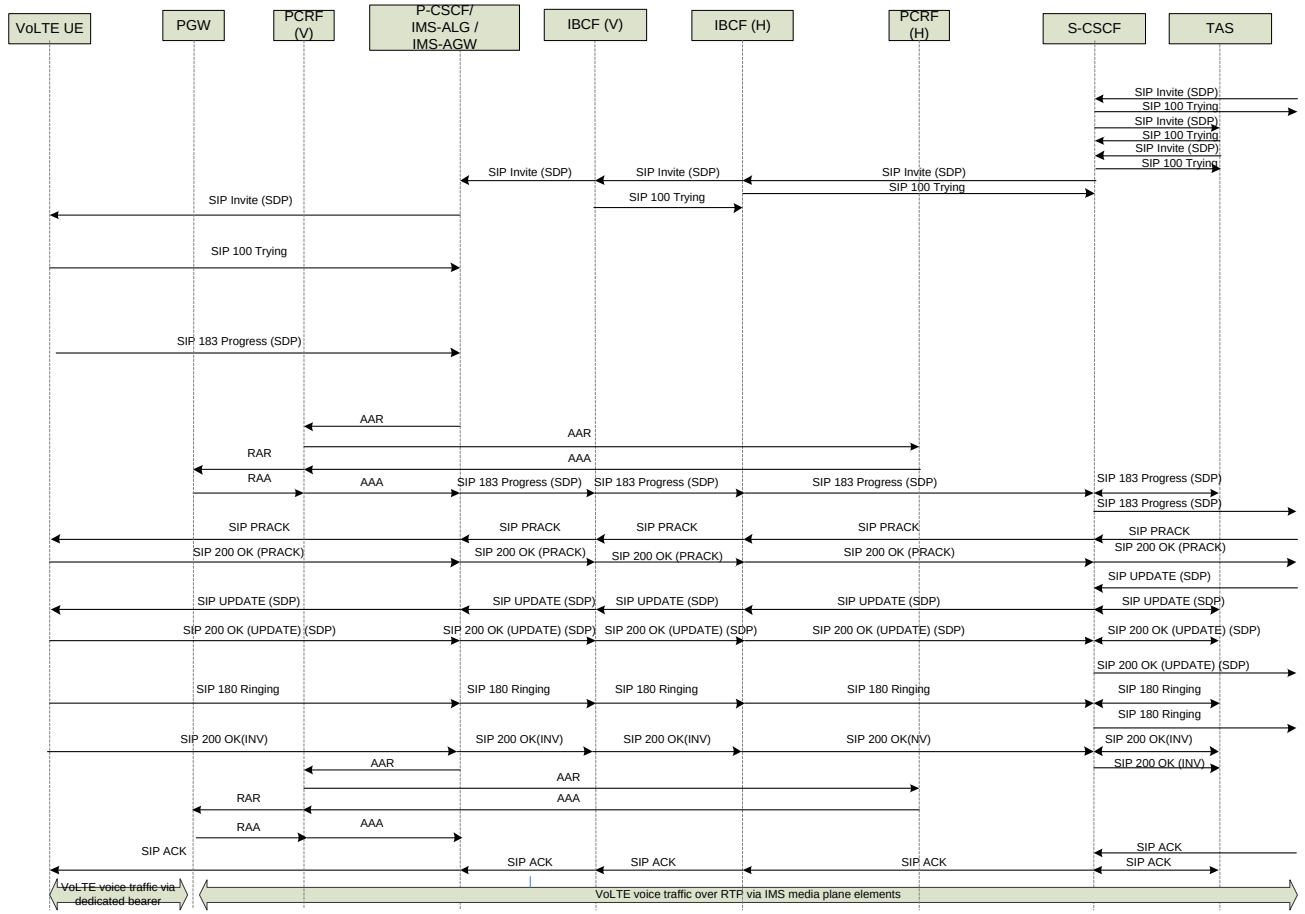

Figure 26: Roaming VoLTE UE to VoLTE UE Call Establishment – Terminating Side message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 5.6.

NOTE: This figure shows a double offer/answer exchange supporting preconditions and utilising the segmented status type as defined in RFC 3312 [71].

NOTE: The figure shows the PCRF being invoked only once on receipt of the of the SDP answer (uplink & downlink configuration). It is also possible to invoke the PCRF twice, i.e. on receipt of both the SDP Offer (downlink configuration) and SDP Answer (uplink configuration). Both options are valid - – see 3GPP TS 29.213 ([79]) annex B.

NOTE: The PRACK and 200 OK (PRACK) messages also traverse through the AS but this is not shown.

5.2.4.3 Detailed Description

As for section 3.2.4.3, with differences due to roaming highlighted in this section.

As in the single network scenario, the S-CSCF receives a SIP INVITE from the originating leg of the call, invokes VoLTE services and routes the INVITE to the P-CSCF that was associated to the subscriber during the IMS registration. In this case, the INVITE is forwarded to the P-CSCF in the visited network via the pair of IBCFs. Each IBCF shall invoke its respective TrGW to allocated media resources for the session and shall modify the SDP in accordance with the newly created media pin-holes. The IBCFs shall also modify the SIP headers as described in 3GPP TS 29.165.

As in the single network scenario, the P-CSCF (IMS-ALG) invokes the IMS-AGW (if deployed) to reserve resources for the media connection. The SDP address in the INVITE is over-written to reflect the media pin-hole created on the IMS-AGW.

As in the single network scenario, the P-CSCF forwards the SIP INVITE to the VoLTE UE. The VoLTE UE shall allocate resources for the call and sends a 183 Progress response containing an SDP answer with a single voice codec and indicating the preconditions are desired but not yet met at the terminating end. This message also utilizes 100rel. The P-CSCF updates the IMS-AGW (if deployed) with the SDP answer from the UE and sends the Authorize/Authenticate-Request message to the PCRF in the visited network with the related updated service information (IP address, port numbers, information on media-type) for the dedicated bearer. The AAR message is conveyed to the PCRF in the home network of the user via the S9 interface if implemented. In this case, the home network PCRF authorises the request and responds with an Authorize/Authenticate-Answer (AAA) message to the visited network PCRF and both PCRFs associate the service information to the stored subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information. The visited network PCRF identifies the affected IP-CAN session (e.g. default bearer) that has been established during the LTE Attach procedure, and initiates a Re-Auth-Request to the PGW to initiate the creation of a dedicated bearer as in the single network case. The visited network PCRF shall also subscribe to modifications related to the dedicated bearer in the PGW (e.g. LOSS_OF_BEARER, INDICATION_OF_RELEASE_OF_BEARER, etc.).

The PGW acknowledges the Re-Auth-Request to the visited network PCRF, which then acknowledges the Authorize/Authenticate-Request message sent from the P-CSCF. At this point the IMS SIP session and the dedicated bearer used for voice are bound together via PCC.

The PGW sends the Create Bearer Request to the SGW to create the dedicated bearer for VoLTE media as in the single network scenario.

On receipt of the AAA response from the visited network PCRF, the P-CSCF will convey the SIP 183 Progress (SDP) message to the S-CSCF in the user's home network via the IBCFs. The contained SDP reflects the address of the media pin hole in the IMS-AGW (if deployed). In turn, each IBCF shall modify its TrGW to reflect the SDP answer and update the SDP answer to reflect the respective media pin-holes in the TrGWs.

The PRACK message is transited from the originating side of the call via the IBCFs.

The terminating side sends a 200 OK (PRACK) in response to the PRACK which is conveyed via the IBCFs.

The originating leg now sends a new SDP Offer in a SIP UPDATE message. The new offer indicates that preconditions have been met at the originating side and that the media stream is now active. The UPDATE message is conveyed to the terminating UE via the S-CSCF, IBCF pair and the P-CSCF.

The terminating UE sends a SIP 200 OK (UPDATE) response containing the SDP answer.

The terminating UE notes that preconditions have been met at both ends, alerts the subscriber and sends a SIP 180 Ringing message to the P-CSCF. This message is transited to the originating leg of the call via the IBCF pair and S-CSCF. This message does not utilize 100rel. The P-Early-Media header is not present in the message.

When the call is answered, the VoLTE UE shall send a SIP 200 OK (INVITE) message to the P-CSCF. The P-CSCF sends an AAR message to the visited PCRF to enable the uplink and downlink media flows. This message is conveyed to the home PCRF over S9 if implemented. In this case, the home PCRF authorizes the request and responds with an AAA message to the visited PCRF which invokes the P-GW to enable the media flows. The visited network PCRF sends the AAA message to the P-CSCF. The P-CSCF(IMS-ALG) also invokes the IMS-AGW (if deployed) to ensure that duplex media can be conveyed via IMS-AGW at this point.

The SIP 200 OK (INVITE) message is forwarded to the S-CSCF via the IBCFs and then to the originating side of the call. On receipt of the 200 OK (INVITE), each IBCF shall ensure that duplex media can be conveyed via their respective TrGWs.

At this stage, the roaming VoLTE UE has a call established with voice traffic sent over the dedicated bearer via the IMS-AGW and pair of TrGWs. Support of Robust Header Compression is mandated and described in GSMA PRD IR.92 [54] section 4.1. The IMS Signalling is sent over the default bearer.

5.2.5 Roaming VoLTE UE to VoLTE UE Call Clearing - Initiated

5.2.5.1 General

A roaming VoLTE UE, shall perform call clearing by using the IMS network. The IMS Signalling shall be sent over the default bearer, and the dedicated bearer that was dynamically established for the voice traffic shall be removed.

5.2.5.2 Message Sequence

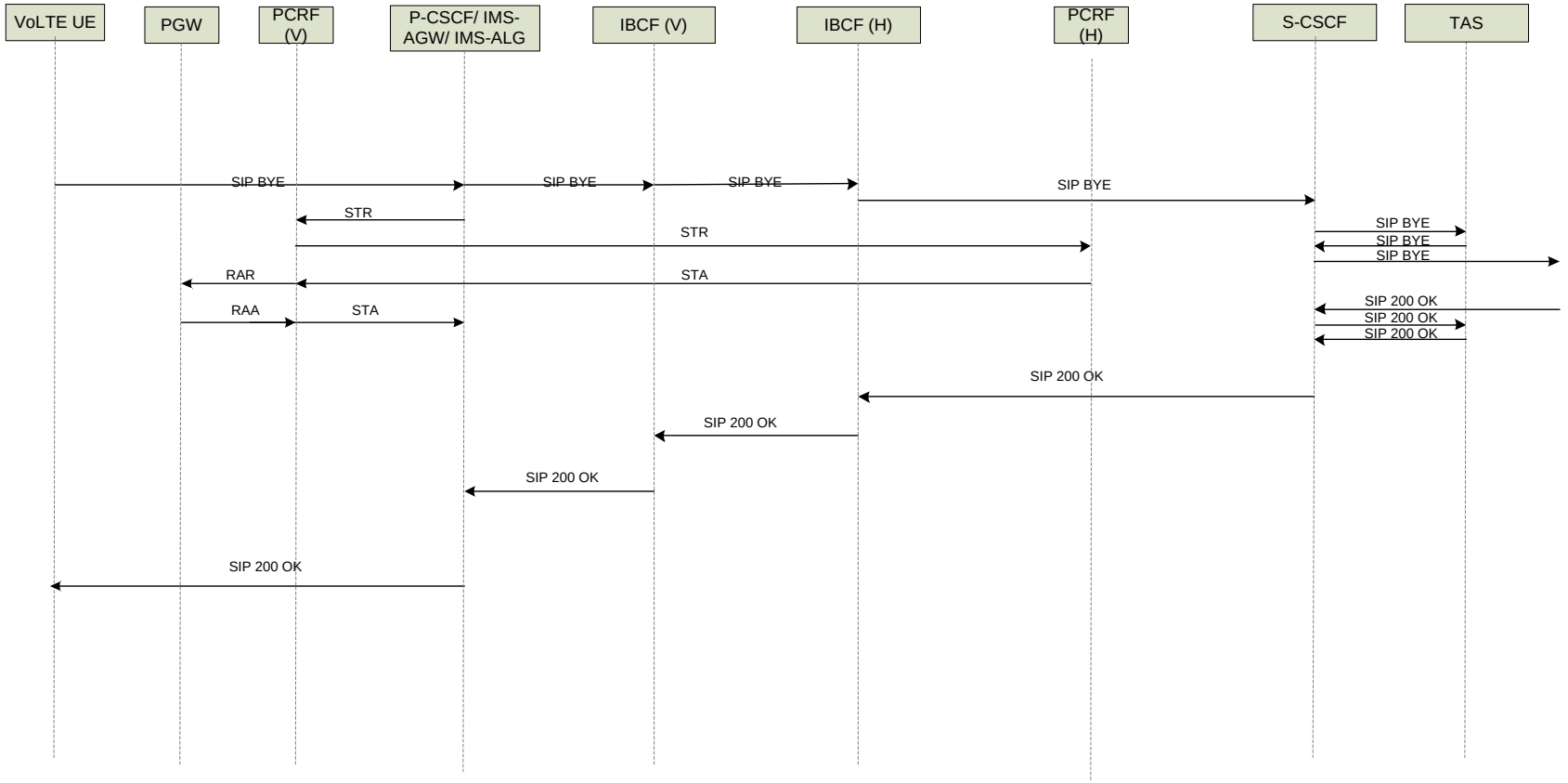

Figure 27: Roaming VoLTE UE to VoLTE UE Call Clearing – Initiated message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 5.6.

5.2.5.3 Detailed Description.

As section 3.2.5.3, with additional details specific to roaming added in this section.

The VoLTE UE sends a SIP BYE message to the P-CSCF. The P-CSCF (IMS-ALG) releases the resources in the IMS-AGW and issues

A Session Termination Request to the PCRF in the visited network. The Session Termination Request is sent to the PCRF in the home network of the user which responds with a Session Termination Answer message over the S9 interface if implemented. The V-PCRF and optionally the H-PCRF (if S9 is implemented) remove the binding between the stored subscription information and the IMS service information, and the visited network PCRF initiates a Re-Auth-Request to the PGW to remove the dedicated bearer as in the single network case. .

The P-CSCF forwards the SIP BYE message to the S-CSCF in the home network of the user via the IBCFs. The IBCFs will free off any media resources allocated in their respective TRGws. The S-CSCF routes the SIP BYE to the S-CSCF of the other party. The other party acknowledges the SIP BYE with a 200 OK.

The 200 OK (BYE) is signalled back to the UE via the IBCFs and P-CSCF.

At this stage, the VoLTE UE has cleared the call and the dedicated bearer for voice traffic has been removed.

5.2.6 Roaming VoLTE UE to VoLTE Call Clearing - Received

5.2.6.1 General

A roaming VoLTE UE, shall perform call clearing by using the IMS network. The IMS Signalling shall be sent over the default bearer, and the dedicated bearer that was dynamically established for the voice traffic shall be removed.

5.2.6.2 Message Sequence

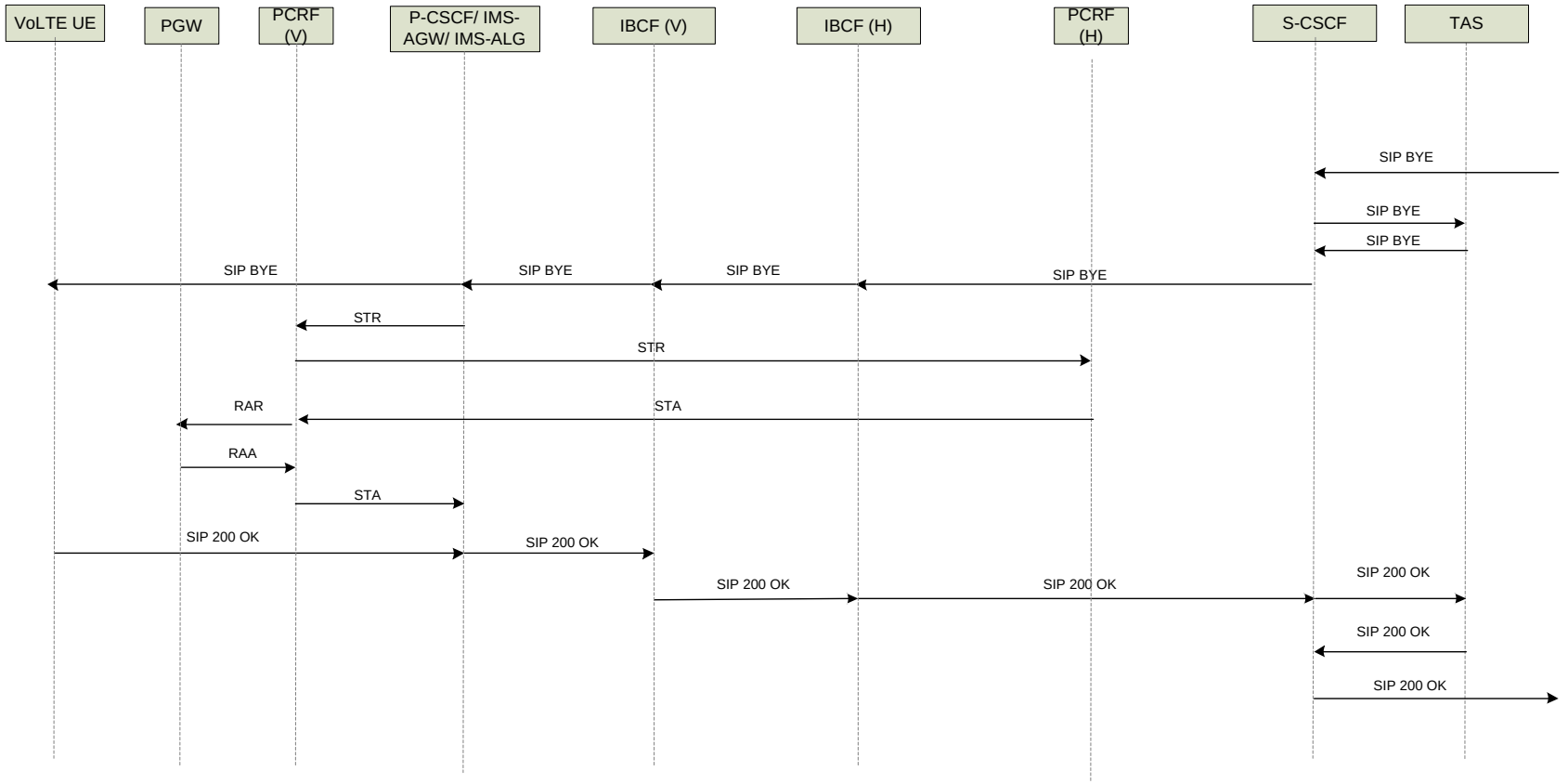

Figure 28: Roaming VoLTE UE to VoLTE Call Clearing – Received message sequence

NOTE: The Diameter Agent has not been included in this message sequence, although Diameter messages shall route via the Diameter Agent. Usage of Diameter Agents is described in section 5.6.

5.2.6.3 Detailed Description

As section 3.2.5.3 with additional details specific to roaming added in this section..

A SIP BYE is received by the S-CSCF from the other party. The S-CSCF shall forward the SIP BYE to the TAS as in the single network case. The S-CSCF routes the SIP BYE to the P-CSCF in the visited network via the IBCFs. The IBCFs shall free off any media resources allocated to the call in their respective TrGWs. The P-CSCF forwards the BYE to the VoLTE UE. The VoLTE UE acknowledges the call clearing by sending a 200 OK.

On receiving the SIP BYE, the P-CSCF (IMS-ALG) frees off the media resources in the IMS-AGW. The P-CSCF also initiates a Session Termination Request to the V-PCRF to initiate the process of removing the dedicated bearer that was established for the voice traffic. The V-PCRF sends the Session Termination Request to its peer in the user's home network over the S9 interface if implemented. In this case, the PCRF in the user's home network responds with a Session Termination Answer to the visited network PCRF. The V-PCRF and optionally the H-PCRF (if S9 implemented) remove the binding between the stored subscription information and the IMS service information. The visited network PCRF and initiates a Re-Auth-Request to the PGW to remove the dedicated bearer for voice

The 200 OK (BYE) is signalled back to the terminating leg of the call via the IBCFs and S-CSCF.

At this stage, the VoLTE UE has cleared the call and the dedicated bearer for voice traffic has been removed.

5.3 Roaming Architecture for Voice over IMS with Local break-out (RAVEL)

As recommended in GSMA PRD IR.65 [51], it shall also be possible to utilize VPMN Routing to replicate the CS charging model for VoLTE roaming scenarios as recommended in GSMA PRD IR.65 ([51]) and described in 3GPP TS 23.228 ([5]), TS 24.229 ([9]) and TS 29.165([24]).

To apply this functionality, loopback routing procedures are required whereby the SIP session signalling can be looped back from the home network to the visited network whilst the media is anchored in the visited network. From that point, both the signalling and media are routed to the terminating party's home network as per current roaming CS routing principles.

In addition to the roaming architecture in figure 19, the Transit & Roaming Function (TRF) is required within the visited network to handle the looped back routing between the visited and home networks of the originating party prior to forwarding the session request to the home network of the terminating party. The procedures required for this are as follows:-

- The P-CSCF inserts the Feature-Caps header field with the "+*g.3gpp.trf"* header field parameter set to the URI of the TRF.
- The IBCF in the visited network initiates OMR procedures (see 5.3), which also must be supported in all other IBCFs that are traversed along the signalling loop. The HPLMN decides, based on local policy whether loopback routing shall be applied. If so, then the HPLMN routes the INVITE request back to the TRF in the visited network including a Feature-Caps header field with a "+*g.3gpp.loopback"* feature-capability indicator.
- The IBCFs traversed on during the loop-back will by means of the OMR procedures determine that a media short-cut can be establish, and thus that media shall not be anchored in the corresponding TrGWs.The TRF routes the SIP INVITE to the home network of the destination party via the IBCFs and ensures that OMR procedures are not further activated.

- When 200 OK (INVITE) is sent along the signalling loop from the TRF in the VPLMN via the S-CSCF in the HPLMN and back to the P-CSCF in the VPLMN, the traversed IBCFs will be informed that a media short cut is established and that no media will pass through the respective TrGWs. IBCFs that previously have not become aware of this (in particular IBCFs between P-CSCF and S-CSCF) will release the allocated media resources in the corresponding TrGWs.
- If loop-back routings shall not be applied, The HPLMN terminates the OMR procedures to ensure that media anchoring in the HPLMN will occur..

In VPMN Routing, Optimal Media Routing (OMR) us used to determine the optimal media path between the visited network of the originating party and terminating network without passing through the home network of the originating party.

5.4 Optimal Media Routing

When VPMN routing as recommended in GSMA PRD IR.65 ([51]) is supported, The OMR procedures described in 3GPP TS 29.079 ([77]) must also be supported. The Reason for applying OMR for VPMN routing is, to maintain the media path in the visited network and avoid needlessly tromboning the media path via the home network. Note that the signalling shall always be conveyed to the home network,
The respective IBCFs through which the IMS signalling traverses would support the SDP *visited-realm* media attribute extensions defined in 3GPP TS 24.229 ([9]) resulting in OMR being recognized as being applicable and resulting in media being negotiated to flow between the respective IMS-AGWs.

The message flows documented in sections 5.2.3 are unchanged by OMR. However, if OMR is applicable, then the IBCF frees off the media resources in the TrGW during session establishment which means that there is subsequently no need for the IBCF to communicate with the TrGW during session teardown.

See annex C of 3GPP TS 29.079 ([77]) for example message flows illustrating OMR.

5.5 Diameter Signalling

Roaming introduces the added complexity of there being an additional capability required to provide a PMN-edge Diameter function to reduce the export of network topologies and support scalability and resilience. Such a Diameter Edge Agent is described in GSMA PRD IR.88 [53] section 3.1.3.

The Diameter Edge Agent needs to discover which peer to route messages to for a specific application to enable Diameter routing between networks. This may be done manual configuration of Diameter nodes within each node. However a dynamic discovery mechanism (NAPTR query), would allow for a simpler, scalable, and robust deployment. GSMA PRD IR.88 [53] section 3.1.3.4 describes the peer discovery mechanism in further detail.

The Diameter Edge Agents use application id=0 in their Capability Exchange to indicate that all applications are supported. This approach enables new applications to be added in each network without impacting on the Diameter Edge Agent.

The roaming scenario requires Diameter messages needing to be routed between the respective Diameter Edge Agents. As in the single network scenario, all Diameter enabled elements in a network shall route their requests and responses via the local Diameter Agent. For the roaming scenario, the Diameter Agent routes the requests/responses via the local Diameter Edge Agent based on the realm identity in the message.

A Diameter Edge Agent may apply topology hiding to reduce the export of topology information across a network boundary. The Diameter Edge Agent may optionally overwrite the host/realm information but this requires a mapping table to be maintained within the Diameter Edge Agent.

5.6 Traffic Management and Policy

Dynamic or static policy control may be applied between the home and visited networks. For dynamic policy control, Rx messages are sent between the visited network PCRF and home network PCRF via the S9 interface. For static policy control, rules are configured locally in the V-PCRF.

In terms of DiffServ marking, TrGWs are present in the end-end media path and are thus able to modify the DSCPs under the control of the IBCF. It is expected that DSCP settings by the IBCF are consistent with table 4.

5.7 Session Border Controllers

For the roaming scenario, both signalling and media traverse the network boundary between the visited and home networks via network side SBCs performing the role of an IMS IBCF/TrGW and providing capabilities such as topology hiding, firewall, NAT traversal etc.

It is also noted that is possible for an access and network side SBC to be co-located in a single physical element. In this case, the message flows documented in section 5 may be simplified as a single element would provide the IMS P-CSCF/IMS-ALG/IMS-AGW and IBCF/TrGW functions such that messages between the P-CSCF and IBCF (in the control plane) and IMS-AGW and TrGW (in the media plane) would be internal to that element.

5.8 IMS Emergency Call

For a roaming UE, there is a requirement for the emergency call to be connected to a PSAP in the visited network. The P-CSCF in the visited network shall recognise the emergency service URN (see RFC 5031 [78]) and route the request to an E-CSCF in the visited network. The requirements of IMS emergency calls are discussed in 3GPP TS 23.167 ([79]) and the procedures of the E-CSCF are described in section 5.11 of 3GPP TS 24.229 ([9]).

Note that if IMS Emergency Call is not supported, then CS Emergency Call is required.

5.9 Lawful Intercept

For the roaming scenario, the Access Session Border Controller (P-CSCF/IMS-ALG/IMS—AGW) in the visited network is a mandatory point of intercept (see 3GPP TS 33.107 [41] section 7A). .

5.10 Security

For the roaming scenario, additional security is required between the Diameter Edge Agents. See section 6.5.1 of GSMA PRD IR.88 ([53]). .

5.11 Charging

For VoLTE calls in the roaming scenario with local break-out with the P-CSCF in the visited network, then the VPMN is service aware and there is scope for service based charging to be deployed between the visited and home networks and to apply flow based charging mechanisms. However, this is topic is still under study and it is likely that charging rates for voice will (for the moment) continue to be independent of the underlying technology.

6 Implementation Guidelines

This section provides the highlights of the issues discovered during Interoperability testing (IOT) and Operators commercial deployments. It contains the guidelines for the VoLTE related protocol implementations in order to achieve seamless interoperability of VoLTE products and accelerate their time-to-market (TTM).

The section is separated in 5 main sections:-

- Open Implementation Issues
- VoLTE Device Implementation Guidelines
- LTE/EPC Implementation Guidelines
- VoLTE IMS Implementation Guidelines
- Other Implementation Guidelines

6.1.1 Open Implementation Issues

Ref. ID	Title	Priority	Category	Status
ID_Other_01	Diameter signalling overload and congestion	Critical	Other	On-going work in 3GPP based on IETF work. Recommendation to deploy a Diameter Agent.

6.1.2 VoLTE Device Implementation Guidelines

6.1.2.1 Downloadable VoLTE Client non-compliancy – Requirement for VoLTE UE support of an Embedded IMS stack

Title	Downloadable Client non-compliancy – Requirement for UE support of Embedded IMS stack
Reference ID	ID_Device_01
Priority	Critical
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	a) Some downloadable VoLTE clients are not providing information required for VoLTE authentication and services (e.g. IMSI in the IMS private ID, IMEI, etc.). Utilisation of downloadable clients not able to provide the correct QoS.
Status	Closed
Detailed Description	Some downloadable VoLTE clients are non-compliant to the capabilities described within GSMA PRD IR.92 [54]. Therefore the required registration, security mechanisms, and applied QoS are failing, without having to provide proprietary solutions in the network.
Solution	Downloadable VoLTE clients must be compliant with GSMA PRD IR.92 [54] and the capabilities described within. The recommendation is for the UE to use native VoLTE functionality

	(with an embedded IMS stack) pre-installed on device.

6.1.2.2 VoLTE UE exceeds the link MTU-size – IP Layer fragmentation – Packets dropped

Title	VoLTE UE exceeds the link MTU-size – IP Layer fragmentation – Packets dropped
Reference ID	ID_Device_02
Priority	High
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	IP fragmentation may occur between the UE and the PGW if the UE sends packets that exceed the maximum link MTU size that is supported in the network as part of IP configuration. IP fragmentation is not recommended by 3GPP due to significant transmission overhead. If the UE exceeds the limit and IP fragmentation is not supported in the EPC, the result is packet loss.
Status	Closed
Detailed Description	3GPP TS 23.060 [3] Annex C provides information related to Link MTU considerations. The maximum size of the link MTU size is currently set to 1500 octets. Taking into account the headers for GTP packets that may be further encapsulated within an IPSec tunnel, the overall UE link MTU size is set at 1358 octets. The link MTU size of the network can be requested by the UE in the Protocol Configuration Options (PCO) during LTE Attach. This enables the UE to discover the link MTU size and be compatible with the network IP configuration. It has been discovered that not all UE's request the link MTU size, and regularly exceed this limit when sending SIP messages (e.g. particularly in downloadable clients). If the network does not support procedures for IP fragmentation, then the packets are discarded which in turn results in loss of VoLTE functionality.
Solution	VoLTE UE's shall request the link MTU size from the network (requested in the PCO during attach) and utilise this value when transmitting data packets. NOTE: For IPv6 implementations, the link MTU size is present in the IPv6 Router Advertisement.

6.1.2.3 VoLTE UE's not supporting GBA for Ut Authentication

Title	VoLTE UE's not supporting GBA for Ut Authentication
Reference ID	ID_Device_03
Priority	High
Date Submitted	08/07/2013
Date Modified	08/07/2013

Overview	Support of GBA on VoLTE devices requires the support of alternative mechanisms for authentication of the Ut interfaces used for Supplementary Service configuration.
Status	Closed
Detailed Description	GSMA PRD IR.92 [54] section 2.2.2 recommends that the UE supports the Generic Authentication Architecture procedures for authentication, alternative procedures as defined in 3GPP TS 24.623 [21] may also be used.
Solution	GSMA recommends the support of GAA for Ut interface authentication. As an interim solution for systems where Generic Authentication Architecture is not supported, the VoLTE UE and TAS shall support HTTP authentication and TLS as defined in RFC 2617 [57] and IETF RFC 2246 [56] according to ETSI TS 183 038 [47].

6.1.3 LTE/EPC Implementation Guidelines

6.1.3.1 Incorrect LTE Cause Code causing UMTS/GSM roaming failure

Title	Incorrect LTE Cause Code causing UMTS/GSM roaming failure
Reference ID	ID_LTE/EPC_01
Priority	Critical
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	Whilst a Home Network Operator and a Visited Network Operator may have an established UMTS/GSM roaming agreement, LTE roaming may not yet be available. Without LTE roaming enabled between the Home Network Operator and the Visited Network Operator, UMTS/GSM inbound roamers with LTE-capable UMTS/GSM handsets may be restricted from roaming on to the UMTS/GSM network unless and until manual re-selection of the UMTS/GSM network is made. Without LTE Roaming enabled the access control in the Visited Network rejects the LTE Attach request with an applicable cause code to allow the device to select another Radio Access Technology for the same PNM (e.g. UMTS/GSM). The issue specified above is caused by a non-recommended LTE attach reject cause code being returned by some LTE networks, to roaming subscribers. The result is that handsets will not attempt to roam onto the UMTS/GSM network and therefore access is restricted to the roaming subscriber, even though an existing roaming relationship for UMTS/GSM exists. GSMA PRD IR.88 [53] (LTE Roaming Guidelines) recommends LTE networks should return #15 (no suitable cells in tracking area), however a number of LTE networks are returning #11 (PLMN not allowed) or #14 (EPS services not allowed in this PLMN).
Status	Closed
Detailed Description	1. A handset tries to attach to LTE access as the first Radio Access Technology in the visited network (normal behaviour of LTE-capable handsets).

	2. As the LTE network has not implemented LTE-LTE roaming with the HPMN of the roaming subscriber, the LTE MME returns an attach reject with a cause value, e.g. #11 (or #14). 3. As the handset received cause code #11 (or #14), the handset stores the LTE MCC-MNC into its forbidden PMN list (or its forbidden PMN for GPRS service list). 4. The handset will never initiate a Location Update or a GPRS Attach to the VLR/SGSN of the UMTS/GSM Network which is broadcasting the same MCC-MNC, because the MCC-MNC is already stored in forbidden PMN list (or forbidden PMN for GPRS service list). 5. As the result of above steps, unless and until the roaming subscriber manually re-selects the UMTS/GSM Network, the handset remains out-of-service in case of no other UMTS/GSM Network available (or packet data does not work while voice/SMS may work).
Solution	If the VPMN (broadcasting the same MCC-MNC as its UMTS/GSM network) already has an existing roaming agreement for other Radio Access Technologies with the HPMN, the LTE Attach reject cause code should be changed to #15 at its earliest possible timeframe. NOTE: This behaviour is described in GSMA PRD IR.88 [53] section 6.1.1.

6.1.3.2 User Location Information, TimeZone, Cause Code is not reported when VoLTE call is dropped.

Title	Updated User Location Information, TimeZone is not reported to EPC in user bearer release and UE context release scenarios, and RAN/NAS Cause Code is not reported to IMS Application Server when VoLTE call is dropped
Reference ID	ID_LTE/EPC_02
Priority	High
Date Submitted	08/07/2013
Date Modified	17/02/2014
Overview	When a VoLTE dedicated bearer or session is dropped, an operator will not get current ULI/TimeZone nor the real failure cause in the S-CDRs and P-CDRs, nor at IMS level, and then will not be able to make performance analysis, User QoE analysis and proper billing reconciliation.
Status	Closed
Detailed Description	When an ERAB or a data session is dropped, an operator may need to get the most up-to-date ULI information as well as detailed RAN and/or NAS cause codes information from the access network to be included in the S-GW and PDN GW CDRs for call performance analysis, User QoE analysis and proper billing reconciliation. Also, for IMS sessions, the operator may need to get the above information available at P-CSCF. ULI and UE Time Zone: a) An operator may be only interested in where the ERAB or the data session is established and where it is released or dropped. Intermediate ECGI information may not be too much of

	interests. Using Location Reporting procedure would not be easy because it only provides an on-demand mechanism (or reporting at any cell change). Moreover, the eNB does not provide the ECGI in current ERAB Release Response, ERAB Release Indication, UE Context Release Request and UE Context Release Complete messages; b) The Delete Bearer Command and Release Access Bearer Request messages currently don't contain ULI and UE Time Zone, which makes impossible for the SGW and PGW to get this information for their CDRs without requiring significant PCRF and PGW state machine changes (PGW and PCRF have to keep their connection alive, and PCRF has to wait for PGW before replying to the P-CSCF). See below implementations details; c) For VoLTE UEs, if a call is dropped due to RF conditions, the VoLTE UE has no way to give the last seen ECGI to the P-CSCF over the Gm interface, therefore this information should be added to Gx IPCAN Session messages where missing. Further implementation details for ULI and Time Zone: - At specific UE or EPC events such as UE-initiated Detach, MME/SGSN-initiated Detach, HSS-initiated Detach procedure, UE or MME requested PDN disconnection, ULI and TimeZone are systematically provided to PCRF in the IPCAN Session Termination. - However, at other specific UE or EPC events such as MME Initiated Dedicated Bearer Deactivation, whereas ULI and Time Zone are available in the MME when the procedure starts, they are not provided immediately to the PGW and the PCRF. They are delayed to the next PCEF-PCRF exchange, and provided only if the PCRF has required it. This was specified for the introduction of NPLI feature and significantly impacts PGW and PCRF state machine. - There is a need for simple mechanism, not requiring full NPLI implementation, by which ULI and UE Time Zone are provided to PCRF in an existing IPCAN Session Modification upon a loss of bearer.
Solution	Change Requests to 3GPP specifications to add the ULI, TimeZone and Cause Codes to the relevant messages have either been done or are in the process of being done (expected completion date of June 2014) for 3GPP R12 onwards.

6.1.4 VoLTE IMS Implementation Guidelines

6.1.4.1 Compatibility of MGCF with VoLTE services utilising MMTel ICSI

Title	Compatibility of MGCF with VoLTE services utilising MMTel ICSI
Reference ID	ID_IMS_01
Priority	High
Date Submitted	18/07/13
Date Modified	17/02/2014
Overview	3GPP TS 29.163 [23] does not mandate that the MGCF include the MMTEL ICSI in the INVITE message. This causes an issue as the target S-CSCF looks for this information in the iFCs when invoking the

	MMTEL Application Server. When calls arrive from the CS network at the MGCF, it can be assumed that for voice calls that MMTEL services are applicable and thus the ICSI should be included and set to identify VoLTE.
Status	Closed
Detailed Description	For voice calls ingressing to IMS via the MGCF, it can be assumed that VoLTE services based on MMTel are applicable and thus the ICSI needs to be included in order to enable the terminating S-CSCF to invoke the appropriate Application Server into the session, The current tables in 3GPP TS 29.163 [23] focusses on deriving/mapping between legacy information in SIP-I/BICC/ISUP to IMS SIP and does not include MMTel aspects. It is believed that the absence of the ICSI is an oversight due to it being a pure IMS concept. The ICSI can be set up for all ingress sessions to the MGCF with “m=audio” in the related SDP. The MGCF should set the media feature tag for IP Voice in Contact header (set to +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"). In addition, the MGCF is acting as a proxy for the originating (CS) user and thus should mimic the behaviour of an originating UE as described in clause 5.1.2A.1.1 of 3GPP TS 24.229 [9].
Solution	Change request to 3GPP CT3 to change 3GPP TS 29.163 [23] agreed and this behaviour is mandated as defined in section 7.2.3.2.2.5 of 3GPP TS 29.163 [23]. GSMA recommends that deployed MGCF's insert the ICSI within relevant messages.

6.1.4.2 Correct support of dynamic codecs

Title	Correct support of dynamic codecs
Reference ID	ID_IMS_02
Priority	High
Date Submitted	18/07/13
Date Modified	18/07/13
Overview	Some endpoints do not properly support dynamic payloads for codecs. Specifically, they mandate/.assume that AMR be payload type 96 at all times rather than allowing dynamic codecs to be correctly assigned a number from the dynamic number range.
Status	Closed
Detailed Description	Codecs that use dynamic payload numbers should be able to be assigned to any of the permitted numbers from the dynamic range as described in RFC 3550 [58] and (from AMR) RFC 4867 [61]. .
Solution	Endpoints should implement dynamic payload mapping properly and make no assumptions about fixing integer values to represent dynamic payload types.

6.1.4.3 Indication of Early media support

Title	Indication of Early media support
Reference ID	ID_IMS_03
Priority	High
Date Submitted	18/07/13
Date Modified	18/07/13
Overview	There is not a single consistent way to indicate support of early media. Sometimes the P-Early-Media header is used, other implementations use analysis of the SDP. This inconsistency can cause issues when required to set up early dialogs and media.
Status	Closed
Detailed Description	The P-Early-Media header (defined in RFC 5009 [63]) was defined as an explicit mechanism in SIP to indicate the support/presence of early media. However, some implementations still do not support this header and also specifications have (for historical reasons) been vague and allowed its support to be optional rather than mandatory. This has led to a situation where the support of the P-Early-Media is sporadic which can lead to inter-operability issues when support of early media is required.
Solution	All VoLTE endpoints and elements should support the P-Early-Media header.

6.1.4.4 Assorted MGCF SIP Issues

Title	Assorted MGCF SIP Issues
Reference ID	ID_IMS_04
Priority	High
Date Submitted	18/07/13
Date Modified	18/07/13
Overview	Assorted issues highlighted regarded non-compliance of MGCFs.
Status	Closed
Detailed Description	The highlighted issues include the following:- • Inconsistent use & support of the SIP ROUTE header, • Support of only TEL URIs and no support of SIP URIs with user=phone, These issues are likely to have arisen due to legacy implementations being evolved to become a MGCF.
Solution	MGCFs should correctly support the highlighted issues.

6.1.4.5 Support of legacy CS Services

Title	Support of legacy CS Services
Reference ID	ID_IMS_05

Priority	High
Date Submitted	18/07/13
Date Modified	18/07/13
Overview	CS networks support a large number of legacy services. With the advent of IMS and service provision via a Telephony AS, concern has been expressed regarding service equivalence.
Status	Closed
Detailed Description	In order to achieve the cited capability, there is a need to replicate the (more) intelligent routing capability existing in MSC Servers. In the IMS context, this capability is inherently more difficult to realize due to the more fragmented nature of the overall architecture. The VoLTE Architecture and baseline 3GPP specifications do not provide a standardised solution to interwork with legacy proprietary services that are commonly utilised within Operators CS networks. A number of possibilities exist for legacy CS proprietary services within the VoLTE Architecture:- 1. Cease support of the legacy proprietary services for VoLTE users: 2. Develop the legacy proprietary services within the TAS 3. Develop interworking between the VoLTE architecture and the existing legacy proprietary CS network services Refer to clause 3.13 for further details of the above.
Solution	It is expected that the solution will vary between operators and based on the nature of the services and the optimum option selected.

6.1.4.6 Support wildcard PSIs in HSS

Title	Support wildcard PSIs in HSS
Reference ID	ID_IMS_06
Priority	High
Date Submitted	18/07/13
Date Modified	18/07/13
Overview	HSSs have been observed that do not support wildcarded PSIs. Such support is needed for dial-in conferencing.
Status	Closed
Detailed Description	For dial-in conferences, the conference URIs must be realized as wildcarded PSIs within the IMS network for proper SIP request routing to be successful.
Solution	HSSs should provide support for wildcard PSI's.

6.1.4.7 SIP Overload Control

Title	SIP Overload Control
Reference ID	ID_IMS_07

Priority	High
Date Submitted	19/07/2013
Date Modified	17/02/2014
Overview	Whilst most equipment provides for interpretation and remapping of SIP Causes, there is still an issue around network congestion controls tied to specific numbers (tele-voting) and the need for some standardized way in SIP to put backward controls on specific destinations.
Status	Closed
Detailed Description	Legacy control protocols (e.g. BICC, ISUP) employ mechanisms to enable an overload condition to be signalled as part of a session rejection to enable the rate of future session requests to be reduced (e.g. ISUP ACC). In addition, legacy nodes are also able to apply network level services such as Call Gapping to prevent a focussed overload to a given destination number (e.g. tele-voting). In the IMS world, similar mechanisms are required in order to protect the network from load spikes.
Solution	Legacy services such as Call Gapping should be realized in IMS via a network level service on the AS. At the current time, there is no agreed mechanism is SIP to convey an overload condition although work is currently on-going in the IETF in the SOC WG and an informational IETF RFC 6357 [64] has been published discussing SIP overload design considerations. There are also a number of current internet drafts in progress (draft-ietf-soc-load-control-event-package-13, draft-ietf-soc-overload-control-14 & draft-ietf-soc-overload-rate-control-07). These drafts have been agreed as SIP overload control mechanisms by 3GPP and referred to in 3GPP TS 24.229 section 4.12 in Rel11. The work in IETF should be monitored and reviewed when complete and published as RFCs. These mechanisms for SIP overload control should be implemented.

6.1.4.8 XML Complexity for MMTel Services

Title	XML Complexity for MMTel Services
Reference ID	ID_IMS_08
Priority	High
Date Submitted	25/07/2013
Date Modified	25/07/2013
Overview	Concern was expressed at the complexity of the XML that is used for the configuration of the MMTel services over the XCAP Ut reference point.
Status	Closed
Detailed Description	As stated in section 3.4.1, a flexible and extensible XML document structure has been defined to support the management of XML services. This includes the (generic) capability to access a given XML document in its entirety as well as accessing a sub-set of the document

	(e.g. interrogating the destination address for the CFU supplementary service).
Solution	All UEs and Application Servers shall support the XML documents defined for the mandatory set of VoLTE services (see section 3.4.1).

6.1.4.9 SIP Fragmentation

Title	SIP Fragmentation
Reference ID	ID_IMS_09
Priority	High
Date Submitted	25/07/2013
Date Modified	17/02/2014
Overview	Related to section 6.1.2.2, the MTU for SIP messages can also be exceeded in the IMS core. On occasion, these messages have become fragmented over UDP transport.
Status	Closed
Detailed Description	Even if the link MTU is not exceeded by the UE (see section 6.1.2.2), SIP messages become extended as they traverse the chain of IMS elements (e.g. VIA and RECORD-ROUTE headers growing in length) and thus SIP fragmentation can occur if the MTU is exceeded and UDP transport is used. The SIP, as defined in IETF RFC 3261 [70], does discuss this issue in clause 18.1.1. and recommends that UDP is not used if the message is within 200 bytes of the MTU or if the message exceeds 1300 bytes and the MTU is unknown.
Solution	Implementations must avoid SIP fragmentation by obeying clause 18.1.1 of RFC 3261 and swapping over to TCP for the transport of large messages. Note that the transport change is done on a per SIP message basis and not on a per session basis.

6.1.5 Other Guidelines

6.1.5.1 Diameter signalling overload and congestion

Title	Diameter signalling overload and congestion
Reference ID	ID_Other_01
Priority	Critical
Date Submitted	08/07/2013
Date Modified	17/02/2014
Overview	Diameter requests are being dropped at the server due to queue overload resulting in lack/degradation of VoLTE service.
Status	Open
Detailed Description	The existing overload control mechanisms in the Diameter base protocol are too limited to efficiently prevent and react to signalling

	overload. These limitations are even more critical in large scale networks in which multiple Diameter nodes, from various vendors, are in the signalling path. Solutions for Diameter overload prevention, detection, and overload mitigation are required.
Solution	The IETF DiME working group has defined "Diameter Overload Control Requirements" (draft-ietf-dime-overload-reqs-01) with proposed solutions for "Diameter Overload Control Application" (draft-korhonen-dime-ovl-00.txt) and "A Mechanism for Diameter Overload Control" (draft-roach-dime-overload-ctrl-01). 3GPP have completed a Release 12 Study Item on Diameter Overload Control Mechanisms to leverage the work within IETF and provide solutions for Overload Indication, Load-balancing, message retransmission, message throttling, message prioritisation and application prioritisation. See 3GPP TR 29.809 [36]. 3GPP are now defining normative solutions, based on the IETF work, which should be monitored and enacted within VoLTE deployments when normative work has been agreed. In the interim, proprietary mechanisms may also exist, e.g. within the implementation and deployment of a Diameter Agent (see section 3.6.2).

6.1.5.2 Diameter Charging Interfaces (Rf and Ro) not Supported

Title	Diameter Charging Interfaces (Rf and Ro) not Supported
Reference ID	ID_Other_02
Priority	Medium
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	The network readiness for support of Diameter Rf and Ro interfaces for Online and Offline Charging is not available. This has led to interim solutions.
Status	Closed
Detailed Description	As Diameter Rf and Ro interfaces are not supported in some networks, interim solutions have been deployed for charging. These include direct CDR generation (often using the MSC's CDR format to prevent billing domain changes) on each IMS node, other interfaces for online charging (e.g. CAMEL, Radius, etc.). There is an expectation that the IMS network shall be able to provide all information that is currently provided in a MSC-generated CDR, resulting in proprietary solutions to enable cause codes to be captured (in CDRs, etc.) in a manner consistent with CS domain networks.
Solution	Interim solutions may apply, with the view for deployment of Rf and Ro interfaces for Online and Offline charging.

6.1.5.3 Lack of support for ENUM

Title	Lack of support for ENUM
Reference ID	ID_Other_03
Priority	Medium
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	Lack of ENUM support causes issues for support of Mobile Number Portability and resolving E.164 numbers to a routable SIP URI.
Status	Closed
Detailed Description	Support of ENUM is required for resolving E.164 numbers to routable SIP URI's within the VoLTE architecture. On a VoLTE call between two Operator's networks, lack of support for ENUM in the originating network may result in the terminating network performing sub-optimal routing, i.e. trying to route a call to a non-IMS subscriber before having to perform a breakout to the terminating CS network. Lack of support for the usage of ENUM is leading to proprietary solutions for performing Mobile Number Portability.
Solution	The recommendation is that ENUM is supported within the VoLTE architecture.

6.1.5.4 IMS Lawful Intercept interfaces not defined

Title	IMS Lawful Intercept interfaces not defined
Reference ID	ID_Other_04
Priority	Medium
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	The IMS Lawful Intercept X1, X2 and X3 specifications are not defined. This leads to prolonged deployment of solutions as IMS vendors and LI vendors must agree on the interfaces to be used within each network deployment.
Status	Closed
Detailed Description	The IMS Lawful Intercept X1, X2 and X3 specifications are not defined. This leads to prolonged deployment of solutions as IMS vendors and LI vendors must agree on the interfaces to be used within each network deployment.
Solution	3GPP may define the X1, X2, X3 interfaces, although standardisation may be a lengthy process. In the interim, IMS vendors and LI vendors must perform integration on a per network basis to perform interception at the A-SBC/P-CSCF as described in section 3.10.

6.1.5.5 Support for (e)SRVCC requires 3GPP Release 10

Title	Support for (e)SRVCC requires 3GPP Release 10
Reference ID	ID_Other_05
Priority	Medium
Date Submitted	08/07/2013
Date Modified	08/07/2013
Overview	Support of 3GPP Release 10 functionality is not readily available which is inhibiting the deployment of (e)SRVCC.
Status	Closed
Detailed Description	Whilst VoLTE describes the support of SRVCC as described in GSMA PRD IR.92 [54] section A.3 which is based on 3GPP Release 8 (with Release 9 aspects to support Emergency Call), there is a view that this solution is not robust enough for handover between LTE coverage and UMTS/GSM coverage. The enhanced SRVCC functionality defined within 3GPP Release 10 also supports the mid-call feature during SRVCC handover, support for calls in alerting state and enhancements to minimise voice interruption delay. Some HSS deployments do not support 3GPP Release 10, and the resultant Sh interface usage to allow the update of the STN-SR in the HSS.
Solution	Support of 3GPP Release 10 eSRVCC is recommended to complement VoLTE with CS voice, or to utilise Inter-RAT PS Handover as described in section 3.14.

6.1.5.6 Other Diameter Issues

Title	Other Diameter Issues
Reference ID	ID_Other_06
Priority	High
Date Submitted	19/07/2013
Date Modified	19/07/2013
Overview	A number of Diameter related issues were highlighted:- • Inconsistent use of Diameter AVPs in requests (primarily on whether to include the Destination-Host AVP) and related to the addition of a DRA to a deployed network, • Some Diameter Servers do not allow multiple TCP / SCTP connections from a single Origin-Host, which leads to having to use multiple Origin-Host identities on a single network element. • Use of proprietary Diameter AVPs
Status	Closed
Detailed Description	The deployment of a Diameter Agent (see section 3.6.2) is recommended. However, with a DRA present, there are options as to whether to include the Destination-Host AVP and perform realm based routing.

	It is undesirable and more complicated to have to use multiple Origin-Host identities (e.g. HSS that supports multiple Diameter applications) on a single network element. As a related point, it is also undesirable for such an element to require multiple TCP/SCTP connections rather than use a single connection and advertise multiple Diameter interfaces via the Capability Exchange mechanism.
Solution	It is recommended to deploy a DRA as per section 3.6.2. Network elements need only include a Destination-Host AVP when it is available (e.g. pre-configured, obtained via a previous request/answer exchange). The DRA shall support the routing of Diameter messages when the Destination-Host AVP is not present. As indicated in IETF RFC 3588 [59], a given Diameter instance of the peer state machine must not use more than one transport connection to communicate with a given peer, unless multiple instances exist on the peer, in which, case a separate connection per process is allowed. This means that a given Origin-Host may only be used on a single connection. Also, it is noted that the use of a DRA provides a point of inter-working to enable inter-operability between Diameter elements both at a transport and application level. Use of proprietary AVPs should be deprecated where possible (i.e. standard AVP in existence to perform a given function). VoLTE service does not rely on proprietary AVPs as standardised AVPs have been defined for VoLTE functionality. Where proprietary AVPs are included in Diameter messages, these should be defined as optional and discarded by elements where they are not supported without rejecting the message.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	05/12/2013	This PRD was reviewed and approved by FCPLT in December 2013	FCPLT	Dave Hutton & Wayne Cutler GSMA
1.1	26/03/2014	CR1001 VoLTE Service Description and Implementation Guidelines and CR1002 VoLTE Service Description and ImplementationGuidelines	FCPLT	Dave Hutton & Wayne Cutler GSMA

Other Information

Type	Description
Document Owner	GSMA Future Communications Programme
Editor / Company	David Hutton / GSMA, Wayne Cutler / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.