Technical Report

TR-493
IMS for 5G-RG Architecture

Issue: 1
Issue Date: March 2024

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

Issue History

Issue Number	Approval Date	Issue Editor	Changes
1	March 2024	Roland Schott, Deutsche Telekom	Original, Issue #1

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor: Roland Schott, Deutsche Telekom
Jörgen Axell, Ericsson

Work Area Director(s): Christele Bouchat, Nokia
Manuel Paul, Deutsche Telekom

Project Stream Leader(s): Roland Schott, Deutsche Telekom

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document contains the architecture for IMS for 5G-RG Wireless Wireline Convergence (WWC).

It provides an architectural overview regarding IMS on a 5G-RG to enable a voice service via 5G wireless or wireline access in combination with an IMS core respectively.

The 5G-RG architecture includes the set of functions and interfaces that realize the use cases defined by BBF.

It references the relevant standardization documents of GSMA, 3GPP and IETF.

The first issues of the IMS for 5G-RG architecture document focuses on the architecture providing a basic consumer voice service. Selected message flows are part of the document for illustration. This document is complementary to the IMS for 5G-RG Requirements document [36]. Latter includes a list of requirements that needs to be implemented for the voice service. The architecture document also depicts important use case like emergency calls and covers aspects of Service Base Architecture (SBA) of 3GPP.

1 Purpose and Scope

1.1 Purpose

The advent of 5G is seen by operators as an opportunity to converge the fixed and mobile side of their networks beyond structural convergence, where fixed and mobile functions coexist over a shared infrastructure (e.g., Cloud CO). In particular, functional convergence provides a single control plane for wireline and wireless sessions.

With TR-470 of the Wireless-Wireline Convergence (WWC) Working Area of Broadband Forum the basis of a converged architecture was created enabling wireline customers to get access via the 5G Core systems and functionalities. The benefit for the operators is to converge and merge their wireless and wireline infrastructure.

Until now Wireless-Wireline Convergence (WWC) activity has not covered the part of voice communication on the 5G-RG.

The purpose of this document is to describe the 5G-RG architecture including the aspect of voice communication. In legacy infrastructure the fixed voice IMS service is working differently from the mobile IMS following different specifications and supplementary services. Therefore, it is required to develop an architecture and specification that allows to run wireline IMS services with a 5G converged IMS Core.

One aspect to be considered is that operators would like to offer a service that is similar to existing services. The reasons are that the operators want to be able to offer the customer the usual scope of services to avoid special cancellation rights or that pure mobile operators want to offer wireline services with their infrastructure requiring the common fixed line phone services and applications that are used by the customer. Another aspect is that the wireline IMS offers additional products especially in the business environment.

Therefore, the working text needs also to cover all these aspects.

The architecture document describes the 5G-RG IMS architecture for residential services in a first step and architecture aspects for business services secondly.

The intention is to provide support for the following classes of devices connected to a 5G-RG:

- Voice Band Data devices such as fax terminals and point-of-sale terminals
- POTS handsets
- Business Services (e.g., PBX), this may include supporting and interworking external SIP clients and supporting multiple services

ISDN BRI and PRI support is out of the scope.

The purpose will be to define a 5G-RG behavior to support PSTN simulation in the context of voice in the 5G system.

According to ITU-T definition PSTN/POTS simulation could potentially provide PSTN/POTS-like service capabilities that fulfil the end-users need. However, there is no guarantee that PSTN/POTS simulation can provide all features that have been available to the PSTN/POTS user. Simulated PSTN/POTS may provide additional new features and capabilities that have not been available to the users of PSTN/POTS.

The Broadband Forum follows and profiles 3GPP and GSMA specifications ensuring 5G-RG voice interoperability with the 5G IMS mobile Core.

Fixed and mobile services might be created on different Application Servers (AS). Convergence of services in one AS is out of scope of the work of Broadband Forum and might be the task of other standardization bodies or the vendors themselves.

The Broadband Forum works in cooperation with 3GPP to define how fixed voice services can be integrate with the 5G IMS Core.

This document serves as a guide to the WWC architecture IMS architecture on 5G-RG. It is related to the 5G-RG requirements and data model defined in BBF.

The purpose of this document is to deliver an architecture overview of the 5G-RG describing the integration of IMS functions into a 5G-RG and the already defined functions by BBF WWC. It is also related to the required interface specification or protocol translations in case these are required to ensure voice communication or deviate from existing standards.

1.2 Scope

This document describes the 5G WWC architecture. It is a companion of the following BBF suite of documents:

TR-124 - 5G-RG Requirements

WT-181 – Data model support for 5G-RG

TR-470 5G Wireless Wireline Convergence Architecture

WT-494 IMS for 5G-RG Residential Voice Requirements

TR-069 CPE WAN Management Protocol Amendment 6 Corrigendum 1

TR-369 The User Services Platform

as well as the 3GPP documents TS 23.228 [9] and TS 23.316 [8].

NG.114 (IMS Profile for Voice, Video and Messaging over 5GS) of GSMA [23] and the IMS survey of BBF members regarding IMS on 5G-RG are the baseline for this architecture document profiling a NG.114 like document for fixed. The combination of both NG.114 and operator input are the starting point for this document. The aspects of GSMA NG.114 that are required by operators for PSTN/POTS simulation are included as well as features not covered in NG.114. Additionally, the CODECs that are required to be supported are part of the description of this document.

BBF 5G WWC specification-work results in different phases of deliverables. This is the first issue of the document and adds:

- IMS functional building block into the 5G-RG architecture
- Interface specification between IMS and ATA (Analogous Telephony Adapter)
- Description to ACS (Autoconfiguration Server) for IMS relevant configurations
- Handling of emergency services
- E2E architecture overview regarding 5G-RG, IMS and 5G Core
- Interworking of IMS with the converged 5G IMS Core
- Basic IMS registration mechanisms

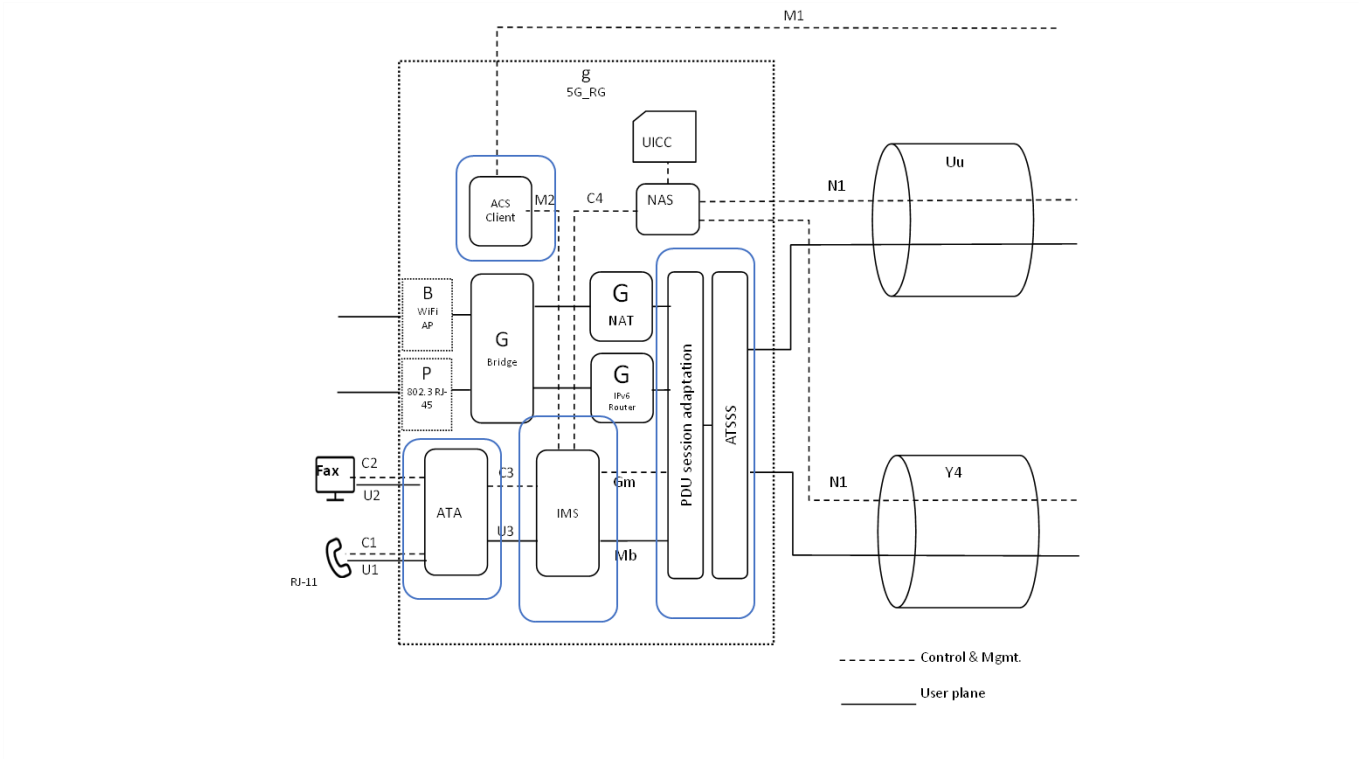
- Mapping of voice communication into PDU sessions and radio bearers
- Handling of connectivity issues and robustness
- Handling of security mechanisms like AKA Digest or TLS
- QoS aspects and references to existing documents for voice communication
- Interface communication between IMS and NAS
- Used voice CODECs
- Signaling Compression [36]
- Use cases, clarification, and guidance

In this document, it is assumed that the AGF and 5G Core are operated by the same network operator, while the rest of the wireline access network may be operated by a 3rd party access wholesale operator. Latter is relevant for pure mobile operators offering their voice services via a leased wireline. Other wholesale scenarios, including AGF and 5GC operated by different operators, are for further study.

The document only focuses on the communication of a wireline IMS client to the converged 5G IMS Core. Consideration of non-3GPP devices within the customer LAN are out of scope of this document. Figure 1 describes the scope of work for IMS within the 5G-RG architecture and end-device respectively.

Focus is on:

- 5G-RG related IMS Parts
- Internal and external Interfaces



ACS	Autoconfiguration Server
ATA	Analogous Telephone Adapter
ATSSS	Access Traffic Steering, Switching and Splitting
IMS	IP-Multimedia Subsystem
PDU	Protocol Data Unit

Figure 1: Scope of IMS Architecture Work within 5G-RG

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [10].

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-69 Amendment 6 Corrigendum 1	CPE WAN Management Protocol Amendment 6 Corrigendum 1	BBF	2020
[2] TS 22.101	Service aspects; Service principles	3GPP	R16

[3]	TS 23.003	Technical Specification Group Core Network and Terminals, Numbering, addressing and identification (Network architecture) Network architecture	3GPP	R16
[4]	TS 24.008	Mobile radio interface Layer 3 specification; Core network protocols	3GPP	R16
[5]	TS 23.501	System architecture for the 5G System (5GS)	3GPP	R16
[6]	TS 23.502	Procedures for the 5G System (5GS)	3GPP	R16
[7]	TS 23.503	Policy and charging control framework for the 5G System (5GS); Stage 2	3GPP	R16
[8]	TS 23.316	Wireless and wireline convergence access support for the 5G System (5GS)	3GPP	R16
[9]	TS 23.228	IP Multimedia Subsystem (IMS); Stage 2	3GPP	R16
[10]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[11]	RFC 8147	Next-Generation Pan-European eCall	IETF	2017
[12]	TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode	3GPP	R16
[13]	TS 23.167	IP Multimedia Subsystem (IMS) emergency sessions	3GPP	R16
[14]	TS 23.237	IP Multimedia Subsystem (IMS) Service Continuity; Stage 2	3GPP	R16
[15]	TS 23.334	IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures descriptions	3GPP	R16
[16]	TS 24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)	3GPP	R16
[17]	TS 24.237	IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) service continuity	3GPP	R16
[18]	TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS)	3GPP	R16
[19]	TS 29.514	5G System; Policy Authorization Service	3GPP	R16
[20]	TS 29.562	5G System; Home Subscriber Server (HSS) services	3GPP	R16
[21]	TS 29.513	5G System; Policy and Charging Control signaling flows and QoS parameter mapping	3GPP	R16
[22]	TS 24.228	Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP);	3GPP	R16
[23]	NG.114	IMS Profile for Voice, Video and Messaging over 5GS v5.0	GSMA	November 2022
[24]	RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	IETF	June 1999

[25] RFC 3261	SIP: Session Initiation Protocol	IETF	June 2002
[26] RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)	IETF	June 2002
[27] RFC 3550	RTP: A Transport Protocol for Real-Time Applications	IETF	July 2003
[28] RFC 4566	SDP: Session Description Protocol	IETF	July 2006
[29] RFC 6151	Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms	IETF	March 2011
[30] RFC 7616	HTTP Digest Access Authentication	IETF	September 2015
[31] RFC 8760	The Session Initiation Protocol (SIP) Digest Access Authentication Scheme	IETF	March 2020
[32] TS103 625	ETSI TS 103 625 V1.3.1 (2023-03)	ETSI	2023
[33] EENA	https://eena.org/our-work/eena-special-focus/advanced-mobile-location/	EENA	
[34] Android	https://www.android.com/safety/emergency-help/emergency-location-service/	Android	
[35] IR.92	IMS Profile for Voice and SMS, Version 15	GSMA	2020
[36] TR-494	IMS for 5G-RG Residential Voice Requirements	BBF	2024
[37] TR 21.905	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications	3GPP	R16

2.3 Definitions

The following terminology is used throughout this Technical Report.

5G-RG	An RG acting in a role of a 3GPP UE towards the 5GC and exchanges N1 signaling with the 5GC.
5G System (5GS)	A system consisting of 5G Access Network (AN), 5G Core Network and UE or 5G-RG.
ACS	Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
ATSC	Advanced Television Systems Committee. Digital television standards, primarily adopted in North America.
Hybrid Access	Access that utilizes both wireline access networks and wireless access networks. From the perspective of an RG, 5G-RG or UE. This can either be exclusive or simultaneous access.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
3PCC	3rd Party Call Control
5GC	5G Core Network
5G NR	5G New Radio
5G-RG	5G Residential Gateway
5GS	5G System
AAA	Authentication, Authorization and Accounting
AAA	AA-Answer (Authorization and Authentication)
AAR	AA-Request (Authorization and Authentication)
A-BGF	Access Border Gateway Function
ACR	Anonymous Communication Rejection
ACS	Auto-Configuration Server
AGF	Access Gateway Function
AGW	Access Gateway
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AML	Advanced Mobile Location
AMR	Adaptive Multi-Rate
AMR-WB	Adaptive Multi-Rate Wideband
AN	Access Network
API	Application Programming Interface(s)
APN	Access Point Name
AS	Application Server
ATA	Analogous Telephone Adapter
ATSSS	Access Traffic Steering, Switching and Splitting
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
B2BUA	Back to Back User Agent
BBF	Broadband Forum
BGCF	Breakout Gateway Control Function
BRI	Basic Rate Interface

CDIV	Communication Diversion
CFU	Call Forwarding Unconditional
CK	Ciphering Key
CLIP	Call Line Identification Presentation
CLIR	Call Line Identification Restriction
Cloud CO	Cloud Central Office
CMR	Codec Mode Request
CPE	Customer Premises Equipment.
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNN	Data Network Name
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual Tone Multifrequency
E-CSCF	Emergency Call Session Control Function
EMTEL	Emergency Telecommunications Subcommittee
ePCO	Extended Protocol Configuration Options
eSIM	embedded SIM
ESInet	Emergency Services IP Network
ETSI	European Telecommunications Standards Institute
EVS	Enhanced Voice Services
FMC	Fixed Mobile Convergence
FN-RG	Fixed Network Residential Gateway
FPGA	Field Programmable Gate Array
FQDN	Fully Qualified Domain Name
GMLC	Gateway Mobile Location Centre
GPS	Global Positioning System
GRUU	Globally Routable User agent URI
GSMA	GSM (Groupe Speciale Mobile) Association
GSMA PDR RCC	GSMA Permanent Reference Document Research Computing Centre
GPU	Graphical Processor Unit
HELD	HTTP Enabled Location Protocol
HSM	Hardware Security Module
HSS	Home Subscriber Server
HTTP/HTTPS	Hypertext transfer protocol / Hypertext transfer protocol secure

IANA	Internet Assigned Numbers Authority
I-BCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
ICSI	IMS Communication Service Identifier
ID	Identifier
iFC	Initial Filter Criteria
IK	Integrity Key
IMC	IMS Credentials
IM CN	IP Multimedia (IM) Core Network (CN)
IMEI	International Mobile Equipment Identity
IM MGW	IP-Multi-Media Gateway
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP-Multi-Media Subsystem
IMS AGW	IMS Access Gateway
IMS AKA	IMS Authentication and Key Agreement
IMSI	International Mobile Subscriber Identity
IP-PBX	Internet Protocol Private Branch Exchange
IPSec	Internet Protocol Security
IRS	Implicit Registration Set
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services (IMS) Subscriber Identity Module
JSON	JavaScript Object Notation
LRF	Location Retrieval Function
LS	Location Server
MAA	Multimedia Authentication Answer
MAR	Multimedia Authentication Request
MGCF	Media Gateway Control Function
MGW	Media Gateway
MGWC	MGW Controller
MMTel	MultiMedia Telephony (Application Server)
MRB	Multimedia Resource Broker
MRF	Media Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSAN	Multi-Service Access Node

MSISDN	Mobile Subscriber Integrated Services Digital Network Number or Mobile Station Integrated Services Digital Network Number
MSRP	Message Session Relay Protocol
MTSI	Multimedia Telephony Service for IMS
MWI	Message Waiting Indication
NAS	Non-Access Stratum
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NBA	NASS Bundled Authentication
NENA	National Emergency Number Association
NG-RAN	Next Generation Radio Access Network
NR	New Radio
P-ANI	P-Access Network Information
PAU	P-Associated-URI header
PCC	Policy and Charging Control
PCF	Policy Control Function
PCM	Pulse Code Modulation
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol
PDU	Protocol Data Unit
POTS	Plain Old Telephone Service
PRACK	Provisional Response ACKnowledgment
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PUI	Public User Identity
QoS	Quality of Service
RAN	Radio Access Network
RAND	Random Challenge
RCS	Rich Communication Services
RDF	Routing Determination Function
RES	Response
RFC	Requests for Comments
RTP	Real-Time Transport Protocol
SA	Security Association
SAA	Server Assignment Answer

SAR	Server Assignment Request
SBA	Service Based Architecture
SBC	Session Border Controller
SBI	Service Based Interface
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMF	Session Management Function
SMS	Short Message Service
TAS	Telephony Application Server
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFO	Tandem-Free Operation
TLS	Transport Layer Security
TR	Technical Report
TrFO	Transcoder-Free Operation
TrGW	Transition Gateway
TS	Technical Specifications
TSN	Time Sensitive Networking
UAA	User Authorization Answer
UAR	User Authorization Request
UDP	User Datagram Protocol
UDUB	User Determined User Busy
UE	User Equipment
UICC	Universal Integrated Circuit Card
ULI	User Location Information
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
UPF	User Plane Function
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USIM	Universal Subscriber Identity Module
UUID	Universally Unique IDentifier
VoNR	Voice over New Radio

W-5GAN	Wireline 5G Access Network
WA	Work Area
W-AGF	Wireline Access Gateway Function
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WT	Working Text
WWC	Wireless Wireline Convergence
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language
XRES	Expected Response

3 Technical Report Impact

3.1 Energy Efficiency

TR-493 has considered the optimization of energy consumption (in terms of electricity requirements for GPU/FPGA and cooling requirement for heat generated by CPU intensive tasks) by specifying measures to avoid or reduce transcoding in the IMS network.

3.2 Security

Security has been considered by incorporating guidelines from GSMA/3GPP related to authentication/authorization/interface security.

3.3 Privacy

SIP privacy related features as defined by IETF SIP RFCs are included or referenced in this document.

4 Functions and Interfaces

The overall architecture for the 5G-RG attached to the 5GC network is shown in Figure 2: Overall Architecture Figure 2.

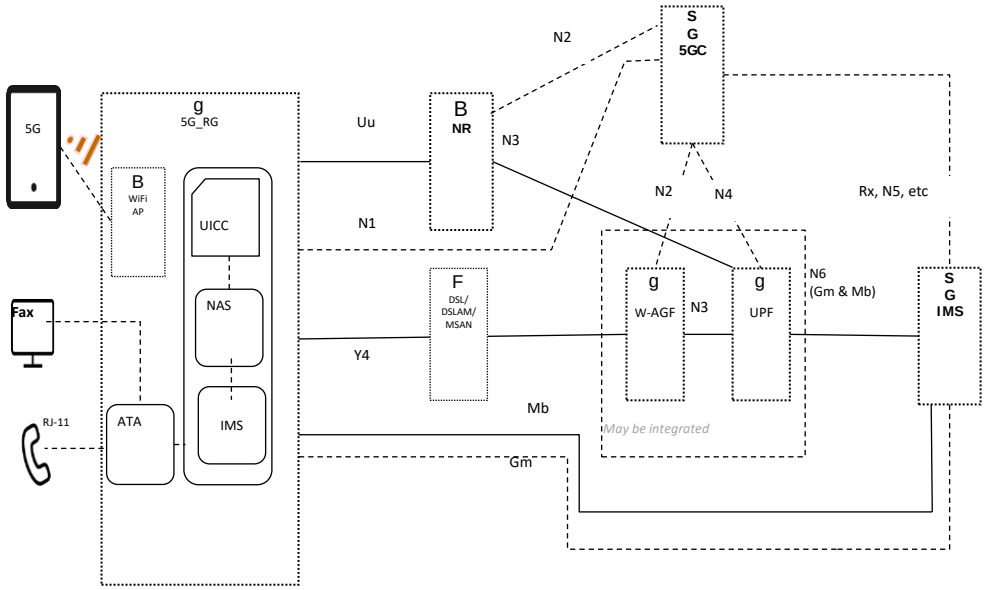


Figure 2: Overall Architecture

The functions (listed in alphabetical order) are:

5G-RG 5G Residential Gateway. A 5G-RG is an RG that has been augmented with 5G capabilities such as QoS handling, a NAS stack, and possibly additional capabilities such as multi access PDU with ATSSS, etc. The 5G-RG has the 5G specific requirements described in the '5G-WWC' requirements of BBF TR-124i6 and subsequent amendments. A 5G-RG supports FN-RG WAN requirements in case it cannot operate as a 5G-RG due to lack of 5G WWC support on the network side.

5GC 5G Core. The 5G Core hosts all of the non-access functions of the 5G System. The documents TS 23.501 [5], TS 23.502 [6] and TS 23.503 [7] provide a stage 2 description of the 5G System. TS 23.316 [8] describes the specific 5GC requirements to support the architecture discussed here.

DSL//Fiber/Coax Any of the access technologies over which the 5G-RG is connected to the core network.

IMS IP Multimedia Subsystem. IMS hosts the service-related nodes and interfaces.

NR NR is 5G radio node receiving the radio signals from the connected 5G-RG.

UPF User Plane Function. Handles the application traffic, i.e., both Gm and Mb interfaces towards the IMS.

W-AGF Wireline access gateway function. Connects the DSL/DSLAM/MSAN to the 5G network

The set of interfaces relevant to this set of functions are:

Gm Reference Point between a UE and a P-CSCF or between an IP-PBX and a P-CSCF as described in 3GPP TS 23.228 [9] clause 4.4.

Mb Reference Point used for IMS media transport to IP network services as described in TS 23.003 0 clause 6a.7.14.

N1 Reference point between UE and the AMF, as described in TS 23.501 0 clause 4.2.7.

N2 Reference point between the (R)AN and the AMF as described in TS 23.501 0 clause 4.2.7.

N3 Reference point between (R)AN and the UPF as described in TS 23.501 0 clause 4.2.7.

N4 Reference point between the SMF and the UPF as described in TS 23.501 0 clause 4.2.7.

N5 Reference point between the PCF and an AF or TSN AF as described in TS 23.501 [5] clause 4.2.7.

N6 Reference point between the UPF and a data network as described in TS 23.501 [5] clause 4.2.7.

Uu Radio interface between RAN and UE as described in TR 21.905 [37]. In general, Uu refers to the radio interface between the UE and gNodeB.

Y4 Reference point between the 5G-RG and the W-AGF which transports the user plane traffic and the N1 NAS protocol.

The 5G-RG gateway can be decomposed in interfaces and function as illustrated in Figure 3.

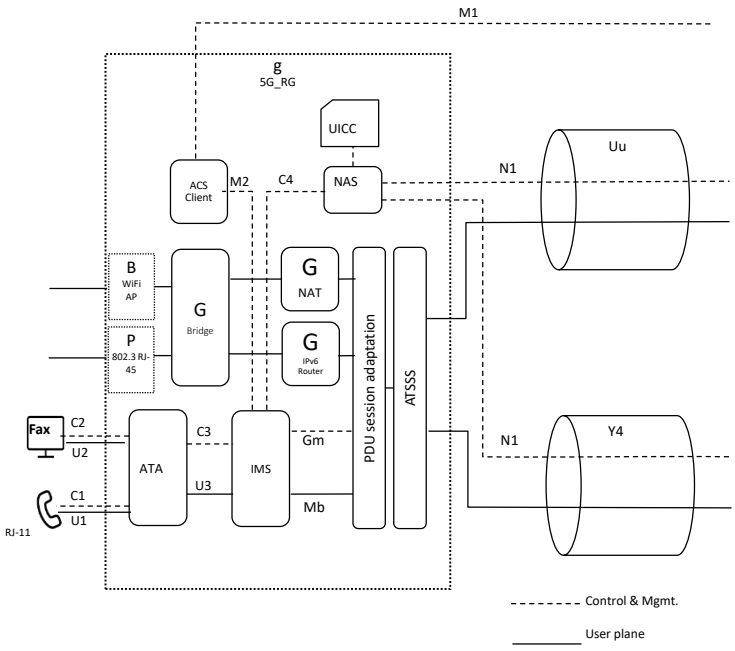


Figure 3: 5G-RG internal Architecture

The interfaces related to Figure 3 are:

C1 Control POTS handset and ATA (assumed to be DTMF)

C2 Voice band data device and ATA (assumed to be DTMF)

C3 Control between ATA and IMS Client

C4 Control between IMS Client & NAS

M1 Management between ACS client and ACS

M2 Management between TR-69/369 mgmt of IMS client

U1 Media transport between POTS handset and ATA

U2 Media transport between voice band data device and ATA

U3 Media transport between ATA and IMS client

5 Introduction

The 5G-RG specification describes the access and transport to 5G Core. Since voice service will still be a mandatory feature in future, the intention is to bring the voice and IMS capability on the 5G-RG. It is important to understand that the IMS service set for wireline and wireless have different requirements.

The 5G-RG needs to be attached to the 5G Core using mobile access.

Phase 1 is focusing on the integration of a wireless IMS voice client on the 5G-RG.

This document gives an overview of the basic IMS architecture, the interworking with other layers and the relevant components yielding to architectural requirements.

Further developments like ATSSS or business voice services are also topics of the 5G-RG IMS architecture to be considered in phase 2.

6 IMS Basics

6.1 Overview of IMS Architecture

The basic IMS signaling architecture being relevant for 5G-RG is described in Figure 4. The User Equipment (UE) embodies the SIP User using the SIP (Session Initiation Protocol) for signaling a voice connection. The P-CSCF (Proxy Call Session Control Function) and the S-CSCF (Serving Call Session Control Function) are representing the Call Control for the signaling. The voice features for example CLIP (Call Line Identification Presentation), CLIR (Call Line Identification Restriction) or number normalization are provided by the Application Server (AS) to which the UE is anchored and connected, respectively. The HSS (Home Subscriber Sever) is the data base where the UE registration data is stored. Since classical TDM networks (GSM or PSTN) are already in place we still have a Media Gateway (MGW) and Media Gateway Controller (MGWC) to establish connections to these kinds of networks. For the 5G-RG the Gm (call control) interface reference point is defined by 3GPP. The media i.e., the voice packets are transported as RTP packets between IMS AGW (Access Gateway) between the voice customers. In that sense the control and user plane are separated. The IMS offers voice connectivity and exchange to other IMS networks or legacy Circuit Switched networks.

For the 5G-RG the Ut interface is not used because the advanced service configuration of Ut is not needed in our case.

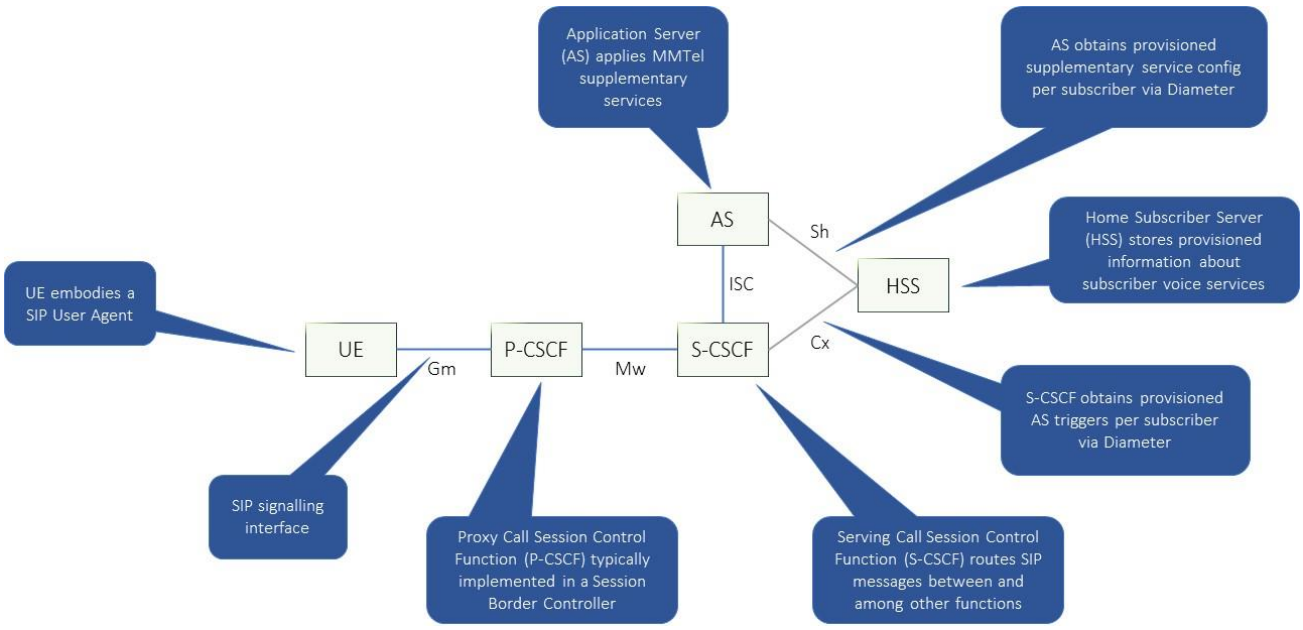
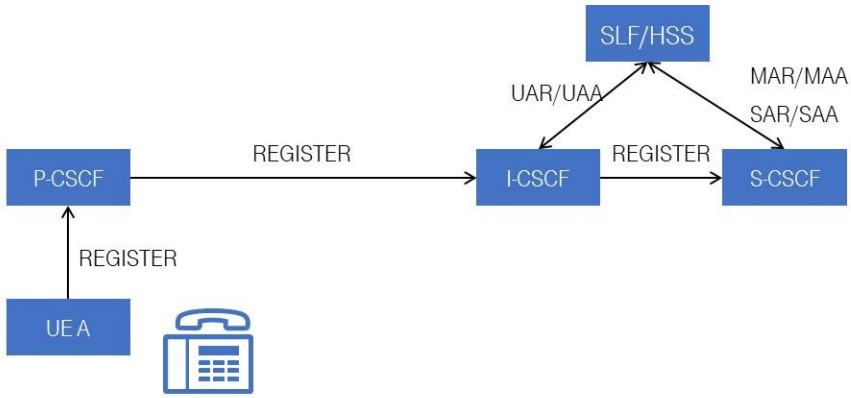


Figure 4: IMS basic Architecture

6.2 IMS Registration

Before an IMS UE or client respectively can make a phone call, the UE needs to register in the IMS network. In general, the REGISTER request is sent to the I-CSCF (Interrogating Call Session Control Function). The UE is registered in the S-CSCF being the SIP registrar and stores data in the HSS (Home Subscriber Server) the database for IMS. With the registration the UE is assigned to an S-CSCF. Figure 5 shows the registration process and the initial registration respectively. During the registration period the UE will send some re-registration messages to ensure that it is still registered in the IMS.



- Before a subscriber can make a phone call, a registration at the IMS must take place.
- The registration process also includes authentication and authorization of the participant in the IMS network.

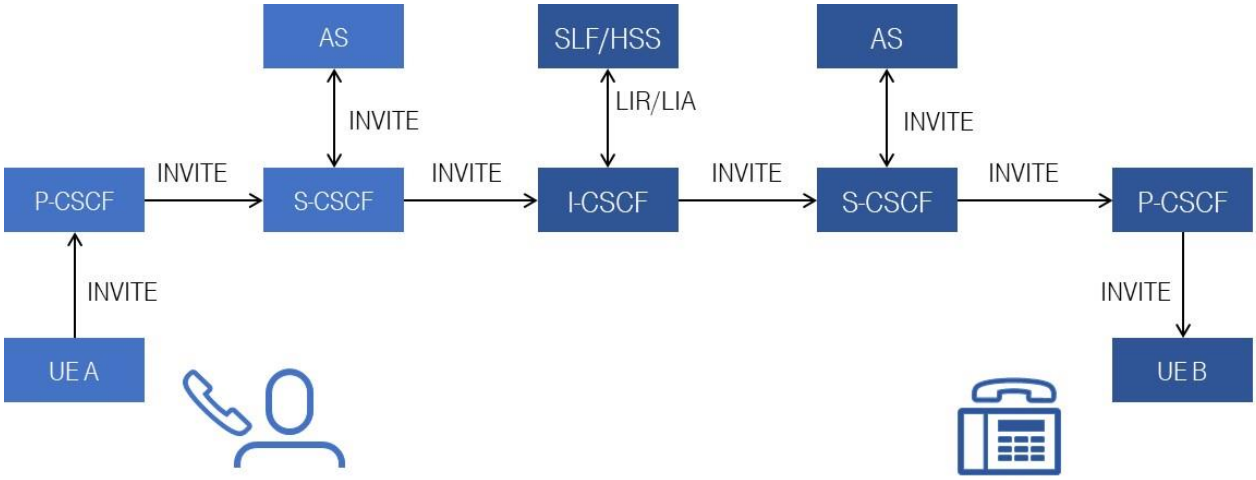
AS: Application Server
SLF: Subscriber Locator Function
HSS: Home Subscriber Server
P-/I-/S-CSCF: Proxy-/Interrogating-/Service-Call Session Control Function
MAR/MAA: Multimedia-Auth-Request, Multimedia-Auth-Answer
SAR/SAA: Server-Assignment-Request , Server-Assignment-Answer
UAR/UAA: User-Authorization-Request, User-Authorization-Answer
UE: User Equipment

Figure 5: IMS Registration

6.3 IMS Basic Call

As mentioned above the IMS works like a telephone switch. In case a UE sets up a call, the UE of A-party sends a SIP INVITE message to the B-party it wants to set up a call, see Figure 6.

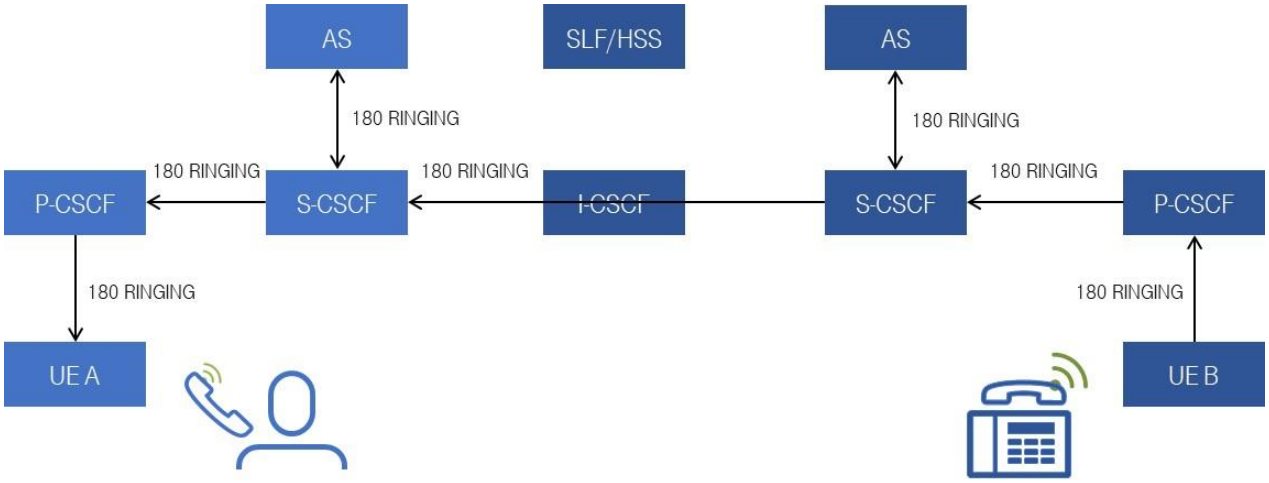
The UE of the B-party signals alerting to the terminal of A-party by SIP 180 RINGING message. The device from A-party generates a ringtone. This procedure works in the early session phase before the call is finally established. The device of the B-party is ringing, see Figure 7. As soon as the user B has picked up the phone, the call is established. This is signaled by a SIP 200 OK message. The voice connection is active now and both parties can start their voice communication. The voice media is running via another protocol named RTP between IMS components named AGW as mentioned above, but not shown for simplification reasons in Figure 8. P-CSCF controls the IMS AGW. The here illustrated pictures show the basic principle of IMS in mobile and fixed network. It is also valid for IMS interconnection to other IMS operators, although we have additional IMS components being part of the call flow for the latter use case.



- Participant A dials number of B.
- Terminal device from A signals call setup via the voice platform to terminal device from B.

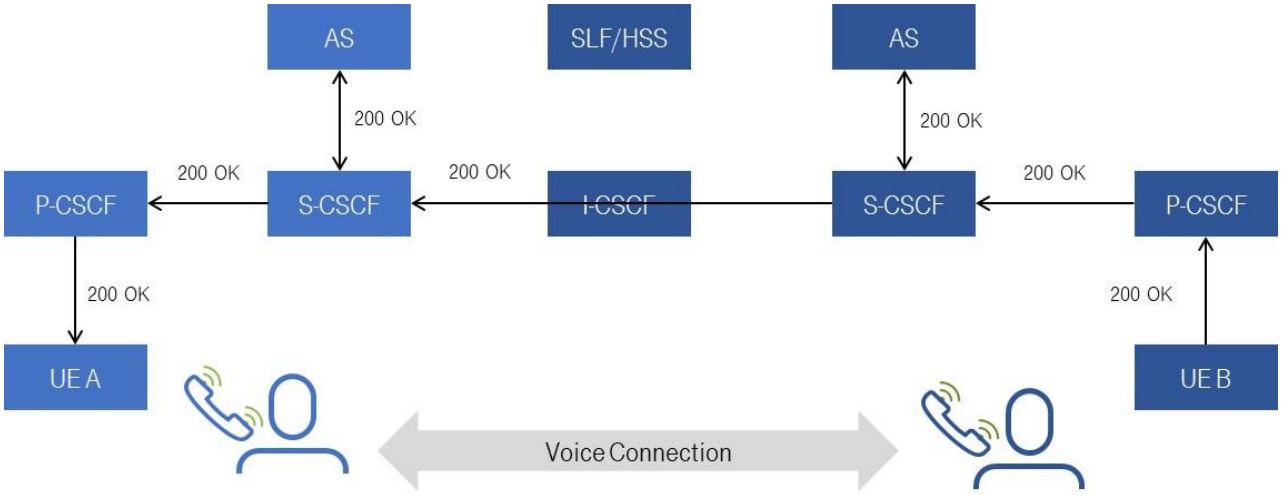
LIR: Location-Info-Request
LIA: Location-Info-Answer

Figure 6: Call Set-Up – SIP Invite



- Device of participant B signals a bell ringing signal to A's terminal device.
- Device from A generates a ringtone and rings, respectively.

Figure 7: Call Set-Up – Ringing



- As soon as participant B has picked up, voice connection (media stream) is established.
- A and B party can start their voice communication.

Figure 8: Call Set-Up – Establishing of a Voice Connection

7 IMS Registration Procedures for 5G-RG

The 5G-RG needs to register on IMS and needs to follow the registration procedures defined in 3GPP and GSMA. Since 5G-RG has also a wireline connectivity the registration procedures need to work also via that access link similarly. Today for fixed IMS slightly different registration mechanisms are in place. For gaining synergies also for the ATSSS use case the registration procedures for IMS via wireless and wireline needs to be identical. The mechanisms are described for clarification regarding IMS on 5G-RG.

7.1 Authentication Procedures for IMS on 5G-RG with IMS AKA

NG.114 defines a profile for voice, video, RCS Messaging and MSRP based Enriched Calling services over IMS, as well as SMS by listing a number of NG-RAN, 5GC, IMS core and UE features and procedures that are considered essential to launch interoperable services. Regarding the 5G-RG and the possibility to register a POTS phone connected to a 5G-RG to the mobile IMS the only required registration procedure is related to the pure voice service in the first step. In a converged IMS only a single security association can be set up using the procedures of IMS-AKA. This also needs to interwork with underlying ATSSS mechanisms. The following section is focusing on IMS authentication and Key Agreement (IMS-AKA) establishing IPSec associations between 5G-RG and P-CSCF. Encryption within IPSec in IMS AKA is optional and depends on the implementation of the operator.

Before the IMS registration can work, the 5G-RG needs to be able to discover the P-CSCF for the IMS APN/DNN. According to NG.114 [23] the P-CSCF discovery mechanism for a registration will depend on the APN/DNN used for that registration. For the 5G-RG IMS POTS use case IMS well-known APN/DNN is used.

The registration mechanism for IMS-AKA is similar to the SIP Digest authentication normally used in the FN-RG use case but requires a specific set of SIP headers and parameters to be used to accomplish the authentication and to establish IPSec associations between 5G-RG and P-CSCF. The reason for using IPSec is the demand that the user connection needs to be encrypted on the wireless radio link. This mechanism is therefore simply reused in the 5G-RG IMS use case for the wireline. The authentication of the 5G-RG takes place in the S-CSCF. An authentication vector is obtained from the HSS containing a challenge for the authentication, the expected response, a value used to authenticate the network to the 5G-RG and the keys that are required to establish a security connection from the 5G-RG to the P-CSCF. After the AKA procedure has been processed the IPSec mechanism will protect all subsequent SIP messages coming from the 5G-RG.

Compared to the IMS-AKA procedure, which is similar to SIP Digest authentication, SIP Digest bases on the usage of username/password and not on a special authentication vector that is used for the authentication and encryption.

During the P-CSCF discovery the P-CSCF IP addresses are provided during the Signaling Bearer Establishment. Typically, two P-CSCF IP addresses are provided. For redundancy reasons i.e., in case of an N+2 redundancy an additional P-CSCF IP address can be provided (in sum three IP addresses or P-CSCFs respectively) optionally. It is up to the operators to decide on their redundancy mechanisms and the number of P-CSCF IP addresses that needs to be provided.

After the P-CSCF discovery the IMS registration process starts. The following process steps are performed and are described in a simplified way.

1. The 5G-RG selects the first IP address and initiates the IMS registration procedure.
   In this process the 5G-RG sends a SIP REGISTER towards the IMS in its home network domain. The REGISTER includes the IP address of the 5G-RG. The REGISTER is routed to the P-CSCF.

2. The P-CSCF stores the 5G-RG contact (IP) address and adds a Route- and Via-Header to the REGISTER before it forwards it to an I-CSCF. According to TS 24.229 section 5.2.2.1 [16] when the P-CSCF receives a REGISTER request from the 5G-RG, the P-CSCF shall insert a Path header field in the request including an entry containing the SIP URI identifying the P-CSCF and an indication that requests routed in this direction of the path (i.e. from the S-CSCF towards the P-CSCF) are expected to be treated as for the 5G-RG-terminating case. Therefore, the included Path-Header-Field is composed using the received Request URI of the REGISTER and a locally configured prefix. It includes the P-CSCF SIP URI to inform the S-CSCF where to route future terminating requests to the user after the 5G-RG is assigned to a dedicated S-CSCF after registration completion.

3. I-CSCF contacts HSS (IMS Database) with an UAR (User Authorization Request, Diameter) to ask for S-CSCF address and capabilities.

4. The HSS returns the required S-CSCF capabilities to the I-CSCF with an UAA (User Authorization Answer, Diameter). Based on the received information and local configuration the I-CSCF selects the S-CSCF.

5. After the S-CSCF selection the I-CSCF forwards the REGISTER to the S-CSCF by inserting the S-CSCF URI and HSS address in a Route-Header.

6. The S-CSCF contacts the HSS with a MAR (Multimedia Authentication Request, Diameter). The HSS itself contacts the AuC (or HSM) via a TCP connection for authentication vector (IMS-AKA) i.e., RAND, AUTN, XRES, CK, IK.

7. HSS sends back the authentication vector to S-CSCF in MAA (Multimedia Authentication Answer, Diameter) message.

8. S-CSCF challenges the 5G-RG. It stores the XRES and replies to the SIP REGISTER request with a 401 Unauthorized response indicating that AKAv1-MD5 is the security mechanism to be used.

9. I-CSCF forwards the 401 Unauthorized – Authentication information to P-CSCF.

10. The P-CSCF further forwards it to the 5G-RG.

11. The 5G-RG 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.

12. The P-CSCF checks the temporary security associations and verifies the security related information received from the 5G-RG. This P-CSCF forwards the SIP REGISTER request to the I-CSCF with the RES included.

13. The I-CSCF uses the UAR message to retrieve the S-CSCF name stored within the HSS.

14. The HSS responds with a UAA message and the related information.

15. After that the I-CSCF forwards to the REGISTER to the relevant S-CSCF including the RES. the S-CSCF checks whether the RES received in the SIP REGISTER and the XRES previously stored

match.

16. The S-CSCF then performs the SAR (Server Assignment Request) procedure to the HSS.

17. It downloads the relevant user profile (SAA - Server Assignment Answer) and registers the 5G-RG. The S-CSCF stores the Path-Header-Field of the P-CSCF and binds this to the contact address of the 5G-RG. This is used for routing to the 5G-RG for future messages.

18. S-CSCF sends a 200 OK response to the I-CSCF.

19. The I-CSCF forwards the 200 OK to the P-CSCF.

20. After the receipt of the 200 OK the P-CSCF changes the temporary set of security associations to a new established set of security associations. It protects the 200 OK with these associations and sends the 200 OK to the 5G-RG. All future messages sent to the 5G-RG will be secured using the security associations.

Additionally, the P-CSCF sends an AAR message to the PCF 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 PCF performs the binding and responds with a AAA message to the P-CSCF.

In case of RCS registration, we will have a separate APN/DNN.

Figure 9 describes the IMS AKA registration graphically.

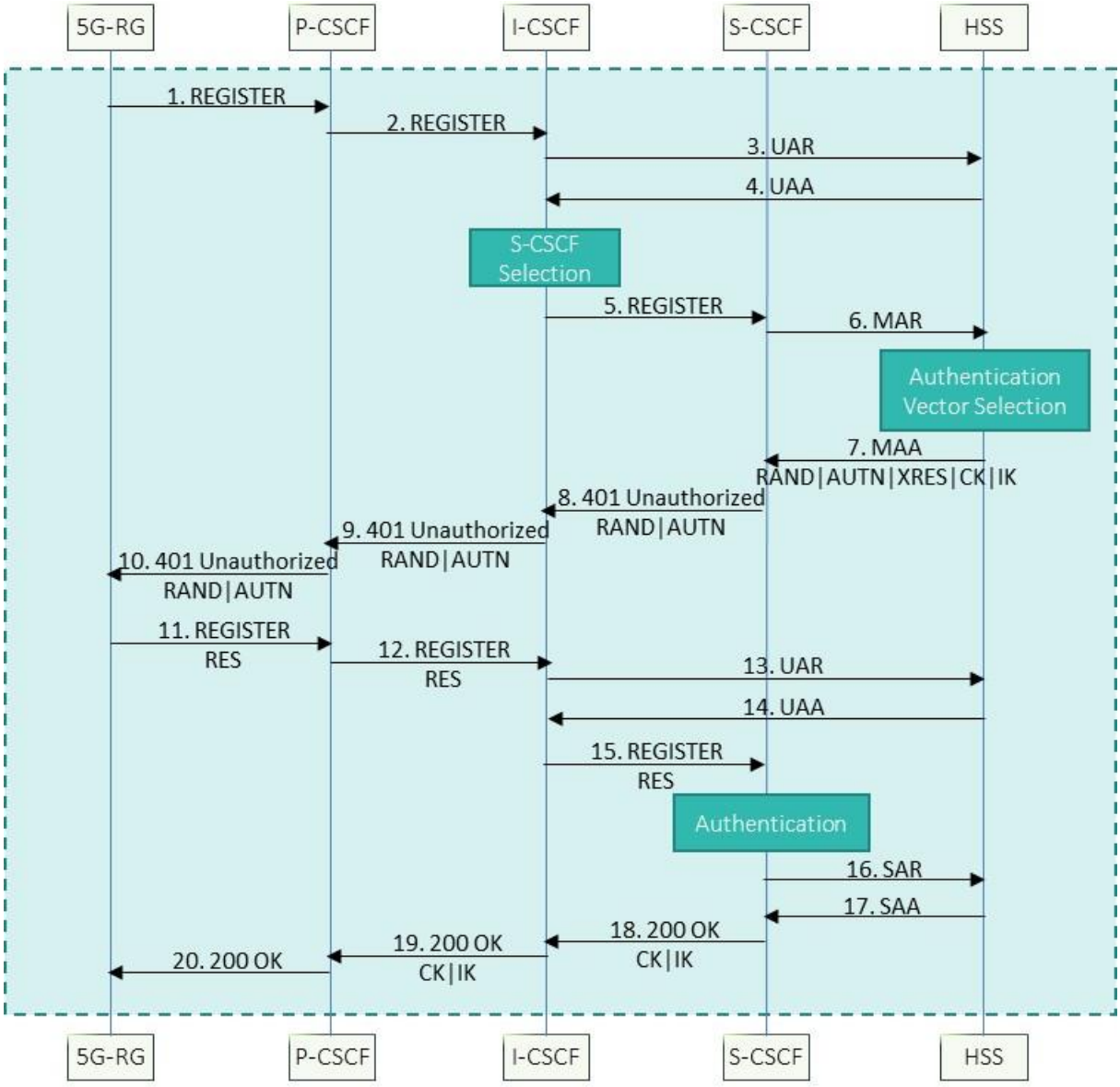


Figure 9: IMS AKA Registration for 5G-RG

7.2 IMS Registration Procedures for 5G-RG with SIP Digest Authentication

The IMS registration mechanism or supported mechanisms for 5G-RG are relevant for the IMS functionality on 5G-RG. NG.114 supports AKA and offers the opportunity for SIP Digest in specific use cases. The proposal here describes the SIP Digest registration procedures. Latter are usually used or are also relevant options for wireline registration of IMS 5G-RGs.

This chapter describes the registration procedures of a 5G-RG at the converged IMS by using SIP Digest Authentication respectively. The single steps of the registration mechanism are described for clarification. In this scenario a Diameter based HSS registration is described. A SIP Digest is a challenge-response mechanism and is username password based. The Session Initiation Protocol (SIP) Digest Access Authentication Scheme [RFC 8760] [31] updates the mechanism by using more secure digest algorithms.

1. The 5G-RG initiates a registration by sending a SIP REGISTER towards the user's home network domain. The REGISTER includes the Public User ID which the user wishes to register. The Request URI is stored in a UICC i.e., ISIM, USIM or configured by IMC (manual configuration in 5G-RG).). The REGISTER contains the public SIP address (SIP Public User Identity), the private address (Private User Identity) of the user and the IP address of the 5G-RG. The REGISTER is routed to the P-CSCF being the outbound proxy for the 5G-RG.

2. The P-CSCF stores the 5G-RG contact IP address and adds a Path header to the REGISTER. It forwards it to a I-CSCF and inserts a Route header. The Route header is composed by the information of the received Request URI of the REGISTER and a locally configured prefix. The Path header contains a P-CSCF-URI to inform the S-CSCF where to route future terminating requests for the user.

3. The I-CSCF sends a UAR (User Authentication Request) basing on the Diameter protocol via the Cx interface to the HSS. This request includes the user's public and private address.

4. The HSS returns the required S-CSCF capabilities to the I-CSCF.

5. Based on the received information and locally configured data the I-CSCF selects the S-CSCF and forwards the REGISTER to the selected S-CSCF. The I-CSCF inserts the S-CSCF URI and HSS address in a Route header. S-CSCF stores the contents of the REGISTER Path header i.e., P-CSCF address used for routing terminating requests and the IP address of the 5G-RG that was received in the REGISTER contact header. It is identified by the S-CSCF that SIP Digest authentication applies for the registration and that the 5G-RG did not send an Authorization Header. The Authentication Realm is configured and for authorization the S-CSCF generates a 'nonce', which is now used as a challenge to the user.

6. The S-CSCF now invokes an Authentication Challenge by returning a 401 Unauthorized towards the 5G-RG. The 'nonce' is included in the WWW-Authenticate header.

7. I-CSCF forwards the message to the P-CSCF.

8. P-CSCF forwards the 401 Unauthorized to the 5G-RG.

9. The 5G-RG generates based on the received information a 'response' and returns the 'response' and the 'nonce' in a new REGISTER request being sent to the P-CSCF.

10. The P-CSCF proxies the REGISTER to select I-CSCF.

11. A Diameter message is sent by the I-CSCF to the HSS via the Cx interface. The UAR contains the private and public address of the user.

12. The HSS returns the S-CSCF URI.

13. After that the REGISTER request is forwarded from the I-CSCF to the S-CSCF.

14. The S-CSCF verifies that the Authorization header is included and extracts the Digest response. It verifies, if the Private ID (from username) matches the Public ID in the SIP request, and if the 'nonce'

is valid for the user. The S-CSCF sends a MAR (Multimedia Authentication Request) to the HSS to receive the SIP digest authentication information.

15. In the HSS the user profile is checked to verify that Digest is used and to find the Digest related credentials. It creates a MAA (Multimedia Authentication Answer) including the Digest-Realm and Digest-H(A1) values (example MD5).

16. The S-CSCF calculates the expected response using the H(A1) value and the ‘nonce’. Subsequently it validates the response from the served user with the calculated expected response. After that it informs the HSS that the user has been successfully authenticated.

17. HSS removes the pending mark for the user and replies with a SAA (Server Assignment Answer) to the S-CSCF.

18. The S-CSCF sends a 200 OK response to the I-CSCF indicating that the registration was successful. The 200 OK contains the ‘nextnonce’ that will be used for authentication of subsequent SIP Requests. Additionally, the Route header containing the S-CSCF URI that is used for routing of subsequent originating SIP requests form the P-CSCF to the S-CSCF is included. The 200 OK includes furthermore a P-Associated-URI header (PAU) containing one or a list of Public User Identities that now have been registered (explicit or implicit registration).

19. The S-CSCF forwards the 200 OK to the P-CSCF.

20. P-CSCF saves the value of the Service-Route header (S-CSCF URI) and the P-Associated-URI header and associates them with the 5G-RG. The P-CSCF forwards the 200 OK response to the 5G-RG.

The Digest registration procedure is depicted in Figure 10.

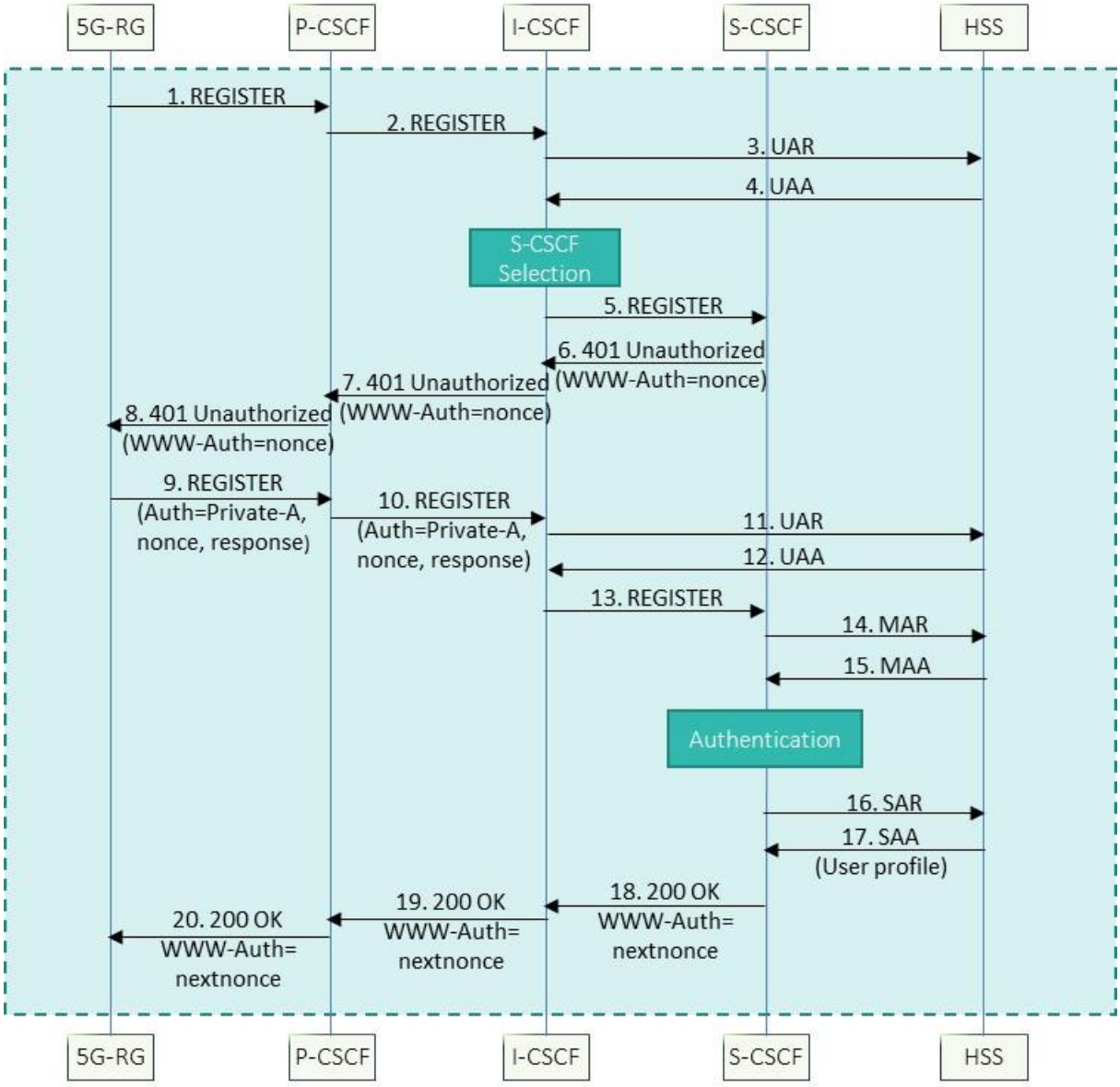


Figure 10: Registration using SIP Digest Authentication

Examples of user address types are described in table Figure 10.

Address Type	Example	Usage
Private User Identity	u12345678@carrier.com	Master identity that is used for authentication and authorization.
SIP Public User Identity	sip: lisa@carrier.com	The public SIP address that is used for addressing the SIP sessions of the user. Note: In case ‘user=phone’ is used the meaning of 'user=phone' is to specify that the user-part of the URI should be interpreted as a telephone number (tel-URI). Example: sip: +4969151001@carrier.com; user=phone
Tel User Identity	tel: +4969151001	The public telephone number of an IMS user (tel-uri). It can be used to address the IMS user.
5G-RG Address/Contact Address	+4969151001@194.25.3.1:5060 lisa@194.25.3.1:5060	IP address that is used to address the 5G-RG where it is registered on IP level. Often dynamic IP addresses are used. It is stored in the P-CSCF & S-CSCF after the Registration.

Table 1: Examples of user address types

[RFC 8760 [31]] “The Session Initiation Protocol (SIP) Digest Access Authentication Scheme” updates [RFC 3261 [25]] by modifying the Digest Access Authentication scheme used by the Session Initiation Protocol (SIP) to add support for more secure digest algorithms, e.g., SHA-256 and SHA-512/256 and to replace the legacy MD5 algorithm. 3GPP [TS 24.229 [16]] also describes the SIP Digest mechanism and handling in IMS. As described in [RFC 8760 [31]] the Session Initiation Protocol [RFC3261 [25]] uses the same mechanism as the Hypertext Transfer Protocol (HTTP) does for authenticating users. This mechanism is called "Digest Access Authentication". As described above, it is a simple challenge-response mechanism that allows a server to challenge a client request and allows a client to provide authentication information in response to that challenge. The version of Digest Access Authentication that [RFC3261 [25]] references is specified in [RFC2617 [24]].

The default hash algorithm for Digest Access Authentication is MD5. However, it has been demonstrated that the MD5 algorithm is not collision resistant and is now considered a bad choice for a hash function (see [RFC6151 [29]] and [TS 24.229 [16]]). The HTTP Digest Access Authentication document [RFC7616 [30]] obsoletes [RFC2617 [24]] and adds stronger algorithms that can be used with the Digest Access Authentication scheme and establishes a registry for these algorithms, known as the "Hash Algorithms for HTTP Digest Authentication" IANA registry, so that algorithms can be added in the future.

[RFC 8760 [31]] updates the Digest Access Authentication scheme used by SIP to support the algorithms listed in the "Hash Algorithms for HTTP Digest Authentication" IANA registry defined by [RFC7616 [30]].

7.3 Implicit Registration

IMS allows one Public User Identity (PUI) to be registered at a time. In case a user has more than one public user identity then the user needs to register every PUI individually. This is an additional message flow effort but has the advantage that each PUI can be registered or de-registered individually. With the concept of “implicit registration” [TS 23.228 [9]] a group of Public User Identities can be registered within a single registration request. When one of the Public User Identities within the IRS (Implicit Registration Set) is registered, all Public User Identities associated with the IRS are registered at the same time. Similarly, when one of the Public User Identities of the IRS is de-registered, all Public User Identities are de-registered at the same time. Public User Identities belonging to an IRS may point to different service profiles. Some of these public user identities may point to the same service profile.

Figure 11 gives an example of Implicit Registration Sets.

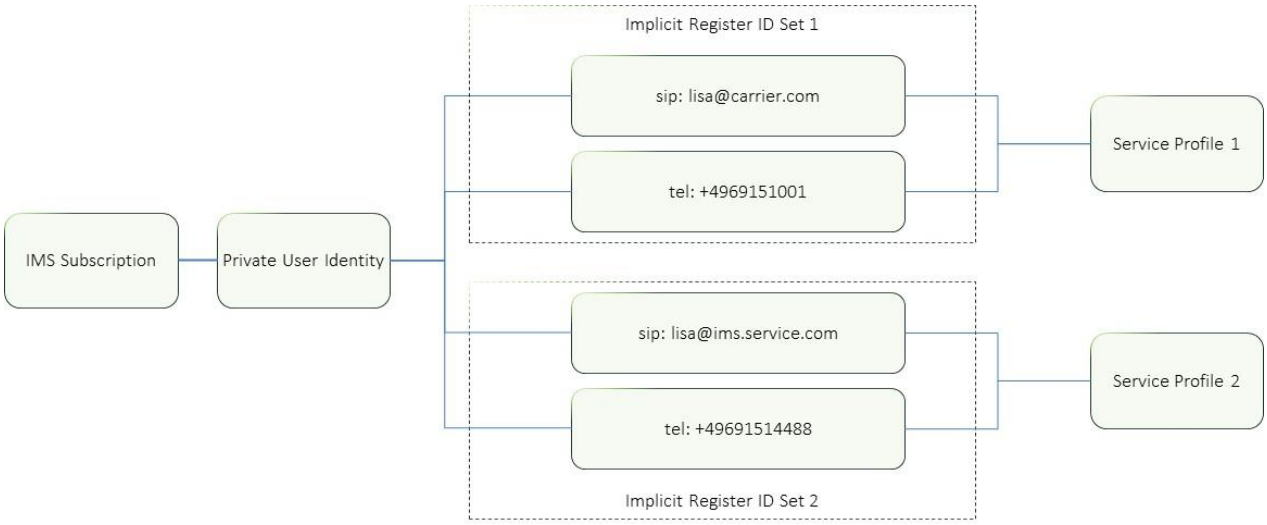


Figure 11: Example of Implicit Registration Set IRS

7.4 Recommended Registration Mechanisms for IMS on 5G-RG

As described in NG.114 [23] AKA Digest or SIP Digest are the preferred registration procedures for 5G VoNR. When projecting this to our case of IMS on 5G-RG these algorithms are also preferred for IMS on 5G-RG. 3GPP defined service based alternatives to the Diameter interfaces Rx, Cx, Dx and Sh. An overview is given in section 7.4.1. However, the protocol used within the network does not impact the procedures at the RG and thus does not impact compliance with this profile.

Registration mechanisms like NBA (NASS (Network Attachement Subsystem) Bundled Authentication) are not recommended because these are not supported by NG.114 [23] and cannot be re-used in the ATSSS use case.

7.4.1 Service Based Architecture and Interface

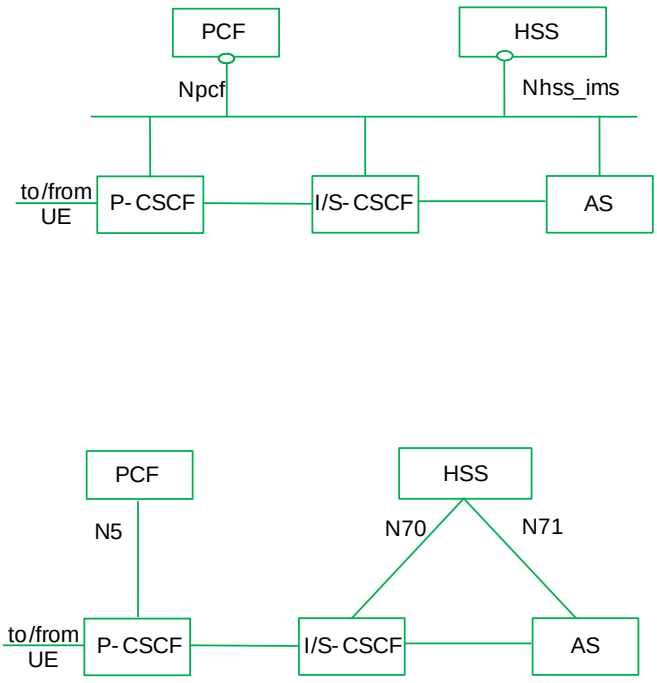


Figure 12: Service Based Architecture for IMS

Service Based Architecture (SBA) & IP Multimedia Network Subsystem (IMS), Figure 12:

- Exposes Network Functions (NFs) accessed via REST based interfaces
- Idea to migrate IMS in 5GC to a stateless architecture
- Characteristics of an SBA is the re-use of web-based protocols i.e., HTTP/JSON and that network functions publishes micro services
- 3GPP TS 23.228 Annex AA [9] shows the architecture to support SBA interactions between IMS entities and relevant reference points
  - Cx interface is replaced by N70 & Sh is replaced by N71
  - PCRF (Policy and Charging Rules Function) is replaced by PCF (Policy Control Function) and N5 instead of Rx interface

7.5 5G RG Initial IMS Registration using IMS-AKA with IPSec via SBI

Previously proposed 5G RG Initial IMS registration solution had diameter Cx interface based HSS interaction with the I/S-CSCF as defined in 3GPP TS 23.228 Section 5.2.2.3 [9] but with 3GPP TS 29.562 [20] now defining I-CSCF & S-CSCF with N70/Nhss SBI interfaces, this proposal is to add/update & align the 5G RG IMS registration flow with the same.

3rd party AS registration and Subscribe/Notify to various event package including reg event is not depicted in this proposed solution.

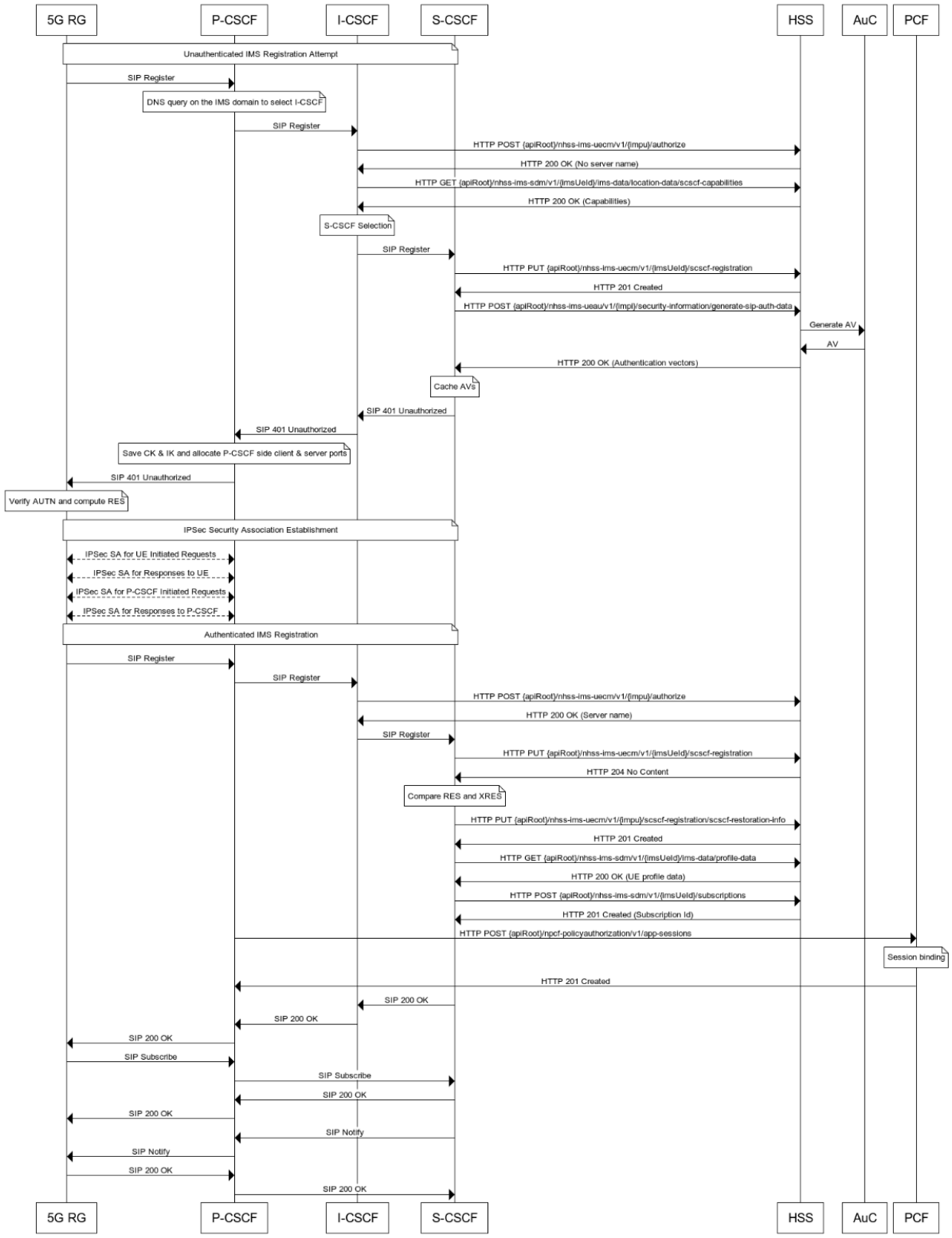


Figure 13: Initial Registration using IMS-AKA with IPSec via SBI Interface

1. 5G RG allocates subscriber side client and server ports and sends an unauthenticated initial SIP REGISTER request message to the unprotected server port (5060) of P-CSCF containing subscriber public & private identity available at the IP address defined in the Contact header. P-CSCF adds a Via header and removes the Route header. Integrity flag is set to false to signify that the subscriber is currently not authenticated. This SIP REGISTER request message is further forwarded to I-CSCF using DNS based routing on the subscriber's IMS domain.

2. Upon receiving the unauthenticated initial SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as "REGISTRATION") to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as "FIRST_REGISTRATION" and CSCF Server Name empty) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then sends a HTTP GET request to retrieve 5G RG's required S-CSCF capabilities with query parameters indicating the supported-features to HSS (as defined in 3GPP TS 29.562 Section 5.3.2.2.3 [20]). HSS responds with HTTP status code "200 OK" with the message body containing the 5G RG's required S-CSCF capabilities (Mandatory Capability List & Optional Capability List). I-CSCF selects the appropriate S-CSCF based on the S-CSCF capabilities required by the 5G RG from a S-CSCF pool and forwards the SIP REGISTER request message to the selected S-CSCF.

4. The S-CSCF sends a HTTP PUT request to HSS to create S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). As there is no previous S-CSCF information stored in HSS hence HSS will store the received S-CSCF registration data and respond with HTTP status code "201 created" containing IMS Registration Type as "INITIAL_REGISTRATION" and list of features supported.

5. The S-CSCF then sends a HTTP POST request to generate-sip-auth-data to the HSS (as defined in 3GPP TS 29.562 Section 5.4.2.2.2 [20]). The payload contains the SIP authentication scheme as "DIGEST-AKAV1-MD5". The HSS requests AuC for generating authentication vectors and AuC responds with the appropriate generated authentication vectors to HSS. The HSS responds with HTTP status code "200 OK" with the message body containing the authentication vector data (RAND, XRES, AUTN, CK, IK). The S-CSCF retains the XRES and creates a SIP 401 Unauthorized message containing the RAND, AUTN, CK, IK (encryption keys to be used by the IPSec on the P-CSCF side) in the WWW-Authenticate header and forwards it to the P-CSCF via I-CSCF. P-CSCF strips CK & IK from WWW-Authenticate header & retains it. P-CSCF allocates the client & server ports and includes it in the Security-Server header and sends the modified 401 Unauthorized authentication challenge message (containing RAND & AUTN) to 5G RG's unprotected client port (5060).

6. Upon receiving the SIP 401 Unauthorized message, 5G RG extracts the RAND & AUTN and verifies AUTN and the computes RES by generating AVs using secret key K (present on USIM/ISIM) with RAND. Then 5G RG authenticates the S-CSCF and calculates the encryption keys for the IPSec channels. 5G RG then creates the IPsec channels and configures the related Security Associations, upon success of which it creates a new authenticated SIP REGISTER request message with authorization header populated with authentication response (RES). 5G RG now forwards the new SIP REGISTER request message to P-CSCF protected server port.

7. Upon receiving the challenged SIP REGISTER request message, P-CSCF verifies the security related information received from the 5G RG. P-CSCF forwards the SIP REGISTER request message to I-CSCF with authorization header indicating integrity protection is enabled. I-CSCF sends a HTTP POST request message to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" containing the serving S-CSCF identity of the user (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]). I-CSCF forwards the SIP REGISTER request message to the S-CSCF received in 200 OK from HSS.

8. S-CSCF compares the RES received from 5G RG with cached XRES on success the S-CSCF sends a HTTP PUT request to HSS to update or create the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). If the resource already exists and the SCSCF registered is the same, the HSS updates the SCSCF Registration resource by replacing it with the received resource information (S-CSCF name, state of the related IMS public identity based on the Registration Type “INITIAL_REGISTRATION” received) and responds with HTTP status code "204 No Content“ or "200 OK".

9. The S-CSCF sends a HTTP PUT request to HSS to update or create S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.6.2 [20]). If the resource does not exist (there is no previous S-CSCF restoration information stored in HSS for that user), HSS stores the received S-CSCF restoration data and responds with HTTP status code "201 created".

10. The S-CSCF sends a HTTP GET request to download the resource representing the 5G RG's user profile in HSS. On success, the HSS responds with HTTP status code "200 OK" with the message body containing the 5G RG's profile data which also includes the Initial Filter Criteria (IFC) (as defined in 3GPP 29.562 Section 5.3.2.2.4 [20]).

11. The S-CSCF sends a HTTP POST request to subscribe for notification of the subscriber data change (as defined in 3GPP TS 29.562 Section 5.3.2.3.2 [20]). On success, the HSS responds with HTTP status code "201 Created" with the message body containing a representation of the created subscription. The Location HTTP header shall contain the URI of the created subscription.

12. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

13. Upon receiving SIP 200 OK response message from I-CSCF, the P-CSCF sends the SIP 200 OK response message to the 5G RG’s protected port.

14. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to subscribe to the status of the IMS Signaling path (as defined in 3GPP TS 29.513 Annex B.5 [21]). The P-CSCF sends an HTTP POST request message to the PCF. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signaling. The PCF confirms the subscription to IMS Signaling path status and replies with an HTTP "201 Created" message back to the P-CSCF.

15. 5G RG then sends a SIP SUBSCRIBE request message to P-CSCF for subscribing to registration (reg) event. P-CSCF sends the SIP SUBSCRIBE request message for reg event to S-CSCF. S-CSCF responds with SIP 200 OK to P-CSCF and then P-CSCF responds to 5G RG with SIP 200 OK.

16. S-CSCF sends a SIP NOTIFY request message to P-CSCF containing the status of each subscriber identity as an XML document in the body of the SIP NOTIFY request message. P-CSCF sends the SIP NOTIFY request message to 5G RG which responds with SIP 200 OK to P-CSCF which further responds to S-CSCF with SIP 200 OK.

Note: SIP 200 OK response message is sent to the UE’s protected client port if the TCP protocol is used and UE’s protected server port if the UDP protocol is used.

7.5.1 IMS Re-Registration via SBI

The following section describes the IMS Re-Registration of a 5G-RG via SBI.

The 3rd party AS Registration and Subscribe/Notify to various event package including reg event is not depicted in this proposed solution.

The following figures depicts the Re-Registration message flow.

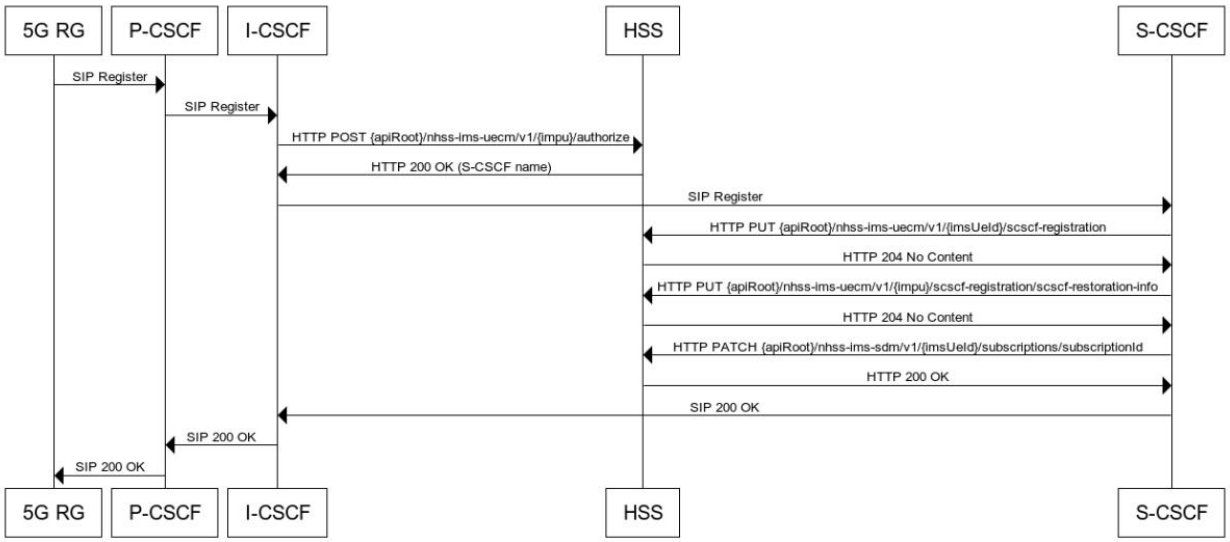


Figure 14: IMS Re-Registration via SBI

1. 5G RG initiates IMS registration refresh by sending an SIP REGISTER request message to P-CSCF which is further forwarded to I-CSCF using DNS based routing.

2. Upon receiving the SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as “REGISTRATION”) to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as “SUBSEQUENT_REGISTRATION” and CSCF Server Name) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then forwards the SIP REGISTER request message to the S-CSCF as given in the previous response.

4. The S-CSCF sends a HTTP PUT request to HSS to update or create the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). If the resource already exists and the SCSCF registered is the same, the HSS updates the SCSCF Registration resource by replacing it with the received resource information (S-CSCF name, state of the related IMS public identity based on the Registration Type “RE_REGISTRATION” received) and responds with HTTP status code "204 No Content“ or "200 OK".

5. The S-CSCF sends a HTTP PUT request to HSS to update or create S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.7.2 [20]). If the resource exist (there is an previous S-

CSCF restoration information stored in HSS for that user), HSS replaces it with the received S-CSCF restoration data and responds with HTTP status code "204 No Content“ or "200 OK".

6. The S-CSCF sends a HTTP PATCH request to the URI previously received during subscription creation (as defined in 3GPP TS 29.562 Section 5.3.2.5.2 [20]). On success, the HSS responds with HTTP status code "200 OK".

7. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

8. Upon receiving SIP 200 OK response message from I-CSCF, the P-CSCF sends the SIP 200 OK response message to the 5G RG.

7.5.2 IMS De-Registration via SBI

The following section describes the IMS De-Registration of a 5G-RG via SBI.

The 3rd party AS De-Registration and Subscribe/Notify to various event package including reg event is not depicted in this proposed solution.

The following figures depicts the De-Registration message flow.

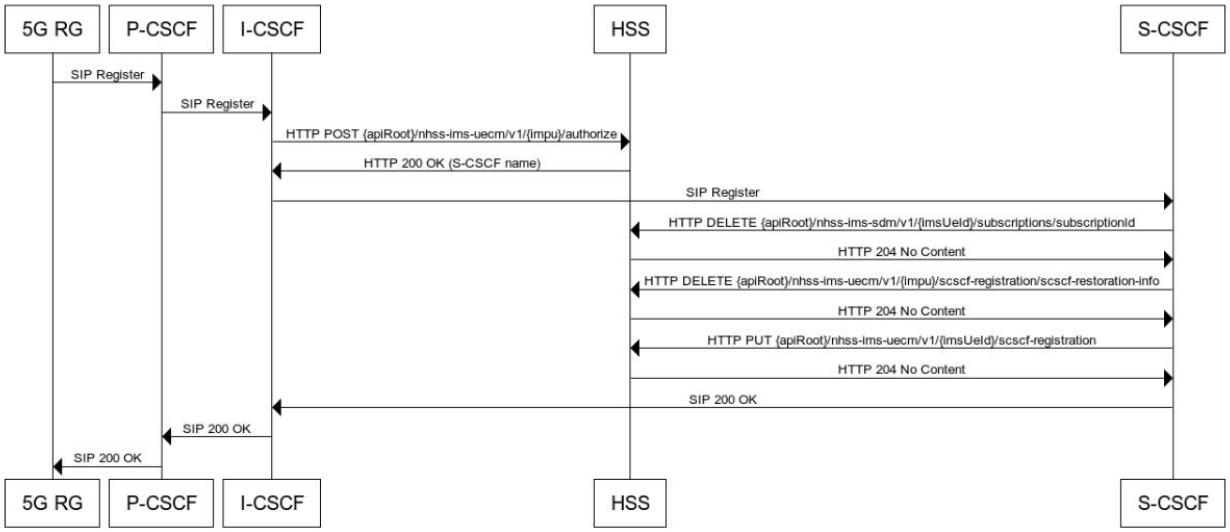


Figure 15: IMS De-Registration via SBI

1. 5G RG initiates IMS deregistration by sending an SIP REGISTER request with expires=0 message to P-CSCF which is further forwarded to I-CSCF using DNS based routing.

2. Upon receiving the SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as “DEREGISTRATION”) to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as

"SUBSEQUENT_REGISTRATION" and CSCF Server Name) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then forwards the SIP REGISTER request message to the S-CSCF as given in the previous response.

4. The S-CSCF sends a HTTP DELETE request to the URI previously received during subscription creation (as defined in 3GPP TS 29.562 Section 5.3.2.4.2 [20]). On success, the HSS responds with HTTP status code "204 No Content ".

5. The S-CSCF sends a HTTP DELETE request to HSS to delete the S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.8.2 [20]). If the resource exist (there is an previous S-CSCF restoration information stored in HSS for that user), HSS deletes it by replacing with the received S-CSCF restoration data and responds with HTTP status code "204 No Content".

6. The S-CSCF sends a HTTP PUT request with the Registration Type set to "USER_DEREGISTRATION" to HSS to delete the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.4.2 [20]). If the resource already exists and the SCSCF registered is the same, and if an IMPI is received as ImsUeId, HSS will deregister all IMPUs associated to that IMPI. If an IMPU is received as ImsUeId, HSS will deregister the IMPU and related IMPUs in the Implicit Registration Set for the related IMPI and responds with HTTP status code "204 No Content".

7. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

8. Upon receiving SIP 200 OK response message from I-CSCF, the P-CSCF sends the SIP 200 OK response message to the 5G RG.

7.5.3 IMS Registration of Telephony Application Server (3rd Party Registration) using SBI and showing PCF interaction

Above shown 5G RG Initial IMS registration solution was aligned with 3GPP TS 29.562 [20] for I-CSCF & S-CSCF with N70/Nhss SBI interfaces for interaction with HSS.

This section adds also the 5G RG IMS registration flow to include 3rd Party Registration on TAS, SIP Subscribe/Notify to Reg event by 5G RG, P-CSCF & TAS and P-CSCF interaction with PCF for signaling path status notification as defined in 3GPP TS 29.513 [21] with N5 SBI interface.

7.5.3.1 5G RG Initial IMS Registration using IMS-AKA with IPSec via SBI including 3rd Party Registration

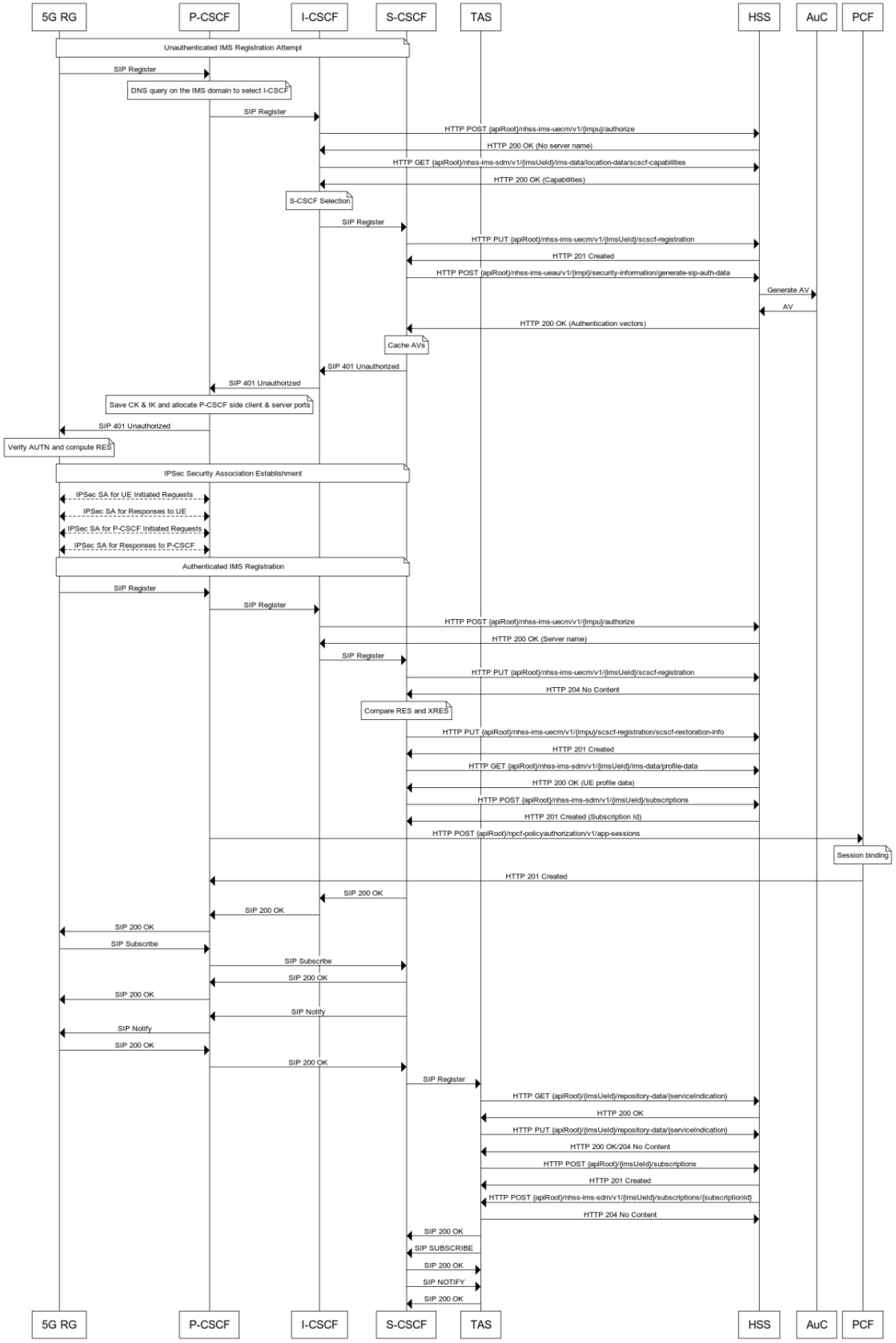


Figure 16: IMS Initial Registration using IMS-AKA with IPSec via SBI

1. 5G RG allocates subscriber side client and server ports and sends an unauthenticated initial SIP REGISTER request message to the unprotected server port (5060) of P-CSCF containing subscriber public & private identity available at the IP address defined in the Contact header. P-CSCF adds a Via header and removes the Route header. Integrity flag is set to false to signify that the subscriber is currently not authenticated. This SIP REGISTER request message is further forwarded to I-CSCF using DNS based routing on the subscriber's IMS domain.

2. Upon receiving the unauthenticated initial SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as "REGISTRATION") to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as "FIRST_REGISTRATION" and CSCF Server Name empty) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then sends a HTTP GET request to retrieve 5G RG's required S-CSCF capabilities with query parameters indicating the supported-features to HSS (as defined in 3GPP TS 29.562 Section 5.3.2.2.3 [20]). HSS responds with HTTP status code "200 OK" with the message body containing the 5G RG's required S-CSCF capabilities (Mandatory Capability List & Optional Capability List). I-CSCF selects the appropriate S-CSCF based on the S-CSCF capabilities required by the 5G RG from a S-CSCF pool and forwards the SIP REGISTER request message to the selected S-CSCF.

4. The S-CSCF sends a HTTP PUT request to HSS to create S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). As there is no previous S-CSCF information stored in HSS hence HSS will store the received S-CSCF registration data and respond with HTTP status code "201 created" containing IMS Registration Type as "INITIAL_REGISTRATION" and list of features supported.

5. The S-CSCF then sends a HTTP POST request to generate-sip-auth-data to the HSS (as defined in 3GPP TS 29.562 Section 5.4.2.2.2 [20]). The payload contains the SIP authentication scheme as "DIGEST-AKAV1-MD5". The HSS requests AuC for generating authentication vectors and AuC responds with the appropriate generated authentication vectors to HSS. The HSS responds with HTTP status code "200 OK" with the message body containing the authentication vector data (RAND, XRES, AUTN, CK, IK). The S-CSCF retains the XRES and creates a SIP 401 Unauthorized message containing the RAND, AUTN, CK, IK (encryption keys to be used by the IPSec on the P-CSCF side) in the WWW-Authenticate header and forwards it to the P-CSCF via I-CSCF. P-CSCF strips CK & IK from WWW-Authenticate header & retains it. P-CSCF allocates the client & server ports and includes it in the Security-Server header and sends the modified 401 Unauthorized authentication challenge message (containing RAND & AUTN) to 5G RG's unprotected client port (5060).

6. Upon receiving the SIP 401 Unauthorized message, 5G RG extracts the RAND & AUTN and verifies AUTN and the computes RES by generating AVs using secret key K (present on USIM/ISIM) with RAND. Then 5G RG authenticates the S-CSCF and calculates the encryption keys for the IPSec channels. 5G RG then creates the IPsec channels and configures the related Security Associations, upon success of which it creates a new authenticated SIP REGISTER request message with authorization header populated with authentication response (RES). 5G RG now forwards the new SIP REGISTER request message to P-CSCF protected server port.

7. Upon receiving the challenged SIP REGISTER request message, P-CSCF verifies the security related information received from the 5G RG. P-CSCF forwards the SIP REGISTER request message to I-CSCF with authorization header indicating integrity protection is enabled. I-CSCF sends a HTTP POST request message to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" containing the serving S-CSCF identity of the user (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]). I-CSCF forwards the SIP REGISTER request message to the S-CSCF received in 200 OK from HSS.

8. S-CSCF compares the RES received from 5G RG with cached XRES on success the S-CSCF sends a HTTP PUT request to HSS to update or create the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). If the resource already exists and the SCSCF registered is the same, the HSS updates the SCSCF Registration resource by replacing it with the received resource information (S-CSCF name, state of the related IMS public identity based on the Registration Type “INITIAL_REGISTRATION” received) and responds with HTTP status code "204 No Content“ or "200 OK".

9. The S-CSCF sends a HTTP PUT request to HSS to update or create S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.6.2 [20]). If the resource does not exist (there is no previous S-CSCF restoration information stored in HSS for that user), HSS stores the received S-CSCF restoration data and responds with HTTP status code "201 created".

10. The S-CSCF sends a HTTP GET request to download the resource representing the 5G RG's user profile in HSS. On success, the HSS responds with HTTP status code "200 OK" with the message body containing the 5G RG's profile data which also includes the Initial Filter Criteria (IFC) (as defined in 3GPP TS 29.562 Section 5.3.2.2.4 [20]).

11. The S-CSCF sends a HTTP POST request to subscribe for notification of the subscriber data change (as defined in 3GPP TS 29.562 Section 5.3.2.3.2 [20]). On success, the HSS responds with HTTP status code "201 Created" with the message body containing a representation of the created subscription. The Location HTTP header shall contain the URI of the created subscription.

12. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

13. Upon receiving SIP 200 OK response message from I-CSCF, the P-CSCF sends the SIP 200 OK response message to the 5G RG’s protected port.

14. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to subscribe to the status of the IMS Signaling path (as defined in 3GPP TS 29.513 Annex B.5 [21]). The P-CSCF sends an HTTP POST request message to the PCF. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signaling. The PCF confirms the subscription to IMS Signaling path status and replies with an HTTP "201 Created" message back to the P-CSCF.

15. 5G RG then sends a SIP SUBSCRIBE request message to P-CSCF for subscribing to registration (reg) event. P-CSCF sends the SIP SUBSCRIBE request message for reg event to S-CSCF. S-CSCF responds with SIP 200 OK to P-CSCF and then P-CSCF responds to 5G RG with SIP 200 OK.

16. S-CSCF sends a SIP NOTIFY request message to P-CSCF containing the status of each subscriber identity as an XML document in the body of the SIP NOTIFY request message. P-CSCF sends the SIP NOTIFY request message to 5G RG which responds with SIP 200 OK to P-CSCF which further responds to S-CSCF with SIP 200 OK.

17. S-CSCF sends a SIP REGISTER request message to TAS containing original SIP REGISTER request message received from 5G RG as an XML document in the body of the SIP REGISTER request message for 3rd Party Registration on TAS.

18. TAS sends a HTTP GET request message (as defined in 3GPP TS 29.562 Section 5.3.2.2.8.1 [20]) containing subscriber identity & service indication to HSS for fetching associated repository data to which HSS responds with HTTP status code “200 OK” to TAS with the message body containing the UE's Repository Data for the requested Service Indication.

19. TAS sends a HTTP PUT request message (as defined in 3GPP TS 29.562 Section 5.3.2.7.2 [20]) for assigning itself as the serving TAS for the given subscriber to the HSS to update the repository data for the given service indication. HSS updates the repository data for the given subscriber identity & service indication and responds with a HTTP status code “200 OK” or “204 No Content” to TAS.

20. TAS sends a HTTP POST request message (as defined in 3GPP TS 29.562 Section 5.3.2.3.2 [20]) to subscribe for notification of data change in the repository data to the HSS. HSS responds with the HTTP status code “201 Created” with Callback Reference URI for the subscription in the Location HTTP header.

21. HSS sends a HTTP POST request message to notify TAS on the data change in the repository data to the TAS (as defined in 3GPP TS 29.562 Section 5.3.2.6.2 [20]). TAS responds with HTTP status code “204 No Content” to HSS.

22. TAS now responds to S-CSCF with SIP 200 OK for successful 3rd party registration on TAS.

23. TAS then sends a SIP SUBSCRIBE request message to S-CSCF for subscribing to registration (reg) event. S-CSCF responds with SIP 200 OK to TAS.

24. S-CSCF sends a SIP NOTIFY request message to TAS containing the status of each subscriber identity as an XML document in the body of the SIP NOTIFY request message. TAS responds with SIP 200 OK to S-CSCF.

Note: SIP 200 OK response message is sent to the UE’s protected client port if the TCP protocol is used and UE’s protected server port if the UDP protocol is used.

7.5.3.2 IMS Re-Registration via SBI including 3rd Party Registration of TAS

The following section describes the IMS Re-Registration of a 5G-RG via SBI as defined in 3GPP TS 29.562 [20].

The following figures depicts the Re-Registration message flow.

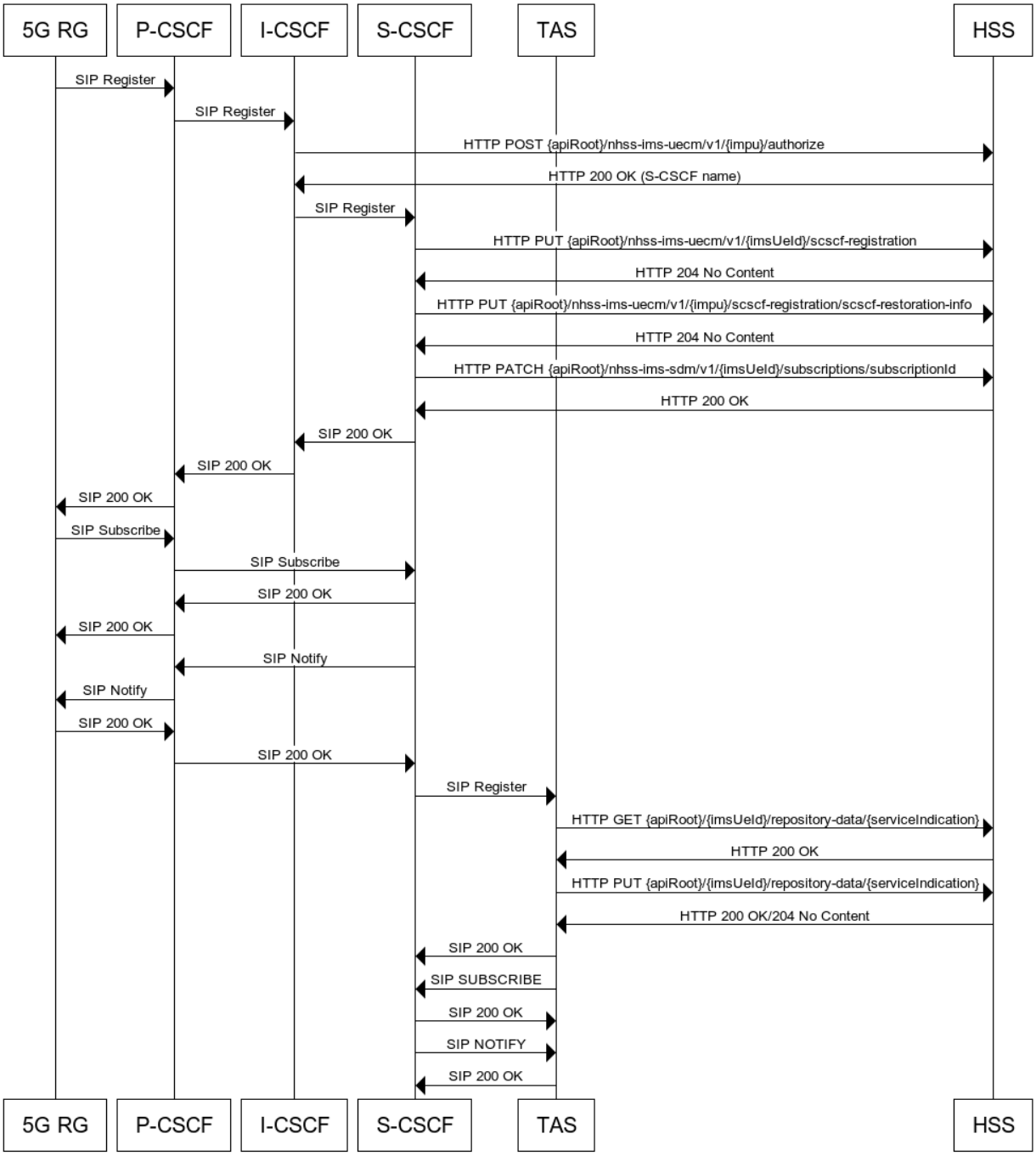


Figure 17: IMS Re-Registration via SBI

1. 5G RG initiates IMS registration refresh by sending an SIP REGISTER request message to P-CSCF on the ports protected by SA, which is further forwarded to I-CSCF using DNS based routing.

2. Upon receiving the SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as “REGISTRATION”) to authorize the 5G RG to register to

HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as “SUBSEQUENT_REGISTRATION” and CSCF Server Name) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then forwards the SIP REGISTER request message to the S-CSCF as given in the previous response.

4. S-CSCF verifies that the integrity-protected parameter of Authorization has an value "yes“, authentication scheme is "Digest” and IMPI is the same as used during initial registration.

5. Then S-CSCF sends a HTTP PUT request to HSS to update or create the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]). If the resource already exists and the SCSCF registered is the same, the HSS updates the SCSCF Registration resource by replacing it with the received resource information (S-CSCF name, state of the related IMS public identity based on the Registration Type “RE_REGISTRATION” received) and responds with HTTP status code "204 No Content“ or "200 OK".

6. The S-CSCF sends a HTTP PUT request to HSS to update or create S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.7.2 [20]). If the resource exist (there is an previous S-CSCF restoration information stored in HSS for that user), HSS replaces it with the received S-CSCF restoration data and responds with HTTP status code "204 No Content“ or "200 OK".

7. The S-CSCF sends a HTTP PATCH request to the URI previously received during subscription creation (as defined in 3GPP TS 29.562 Section 5.3.2.5.2 [20]). On success, the HSS responds with HTTP status code "200 OK".

8. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

9. Upon receiving SIP 200 OK response message from I-CSCF, the P-CSCF sends the SIP 200 OK response message to the 5G RG.

10. 5G RG then sends a SIP SUBSCRIBE request message to P-CSCF for subscribing to registration (reg) event. P-CSCF sends the SIP SUBSCRIBE request message for reg event to S-CSCF. S-CSCF responds with SIP 200 OK to P-CSCF and then P-CSCF responds to 5G RG with SIP 200 OK.

11. S-CSCF sends a SIP NOTIFY request message to P-CSCF containing the status of each subscriber identity as an XML document in the body of the SIP NOTIFY request message. P-CSCF sends the SIP NOTIFY request message to 5G RG which responds with SIP 200 OK to P-CSCF which further responds to S-CSCF with SIP 200 OK.

12. S-CSCF sends a SIP REGISTER request message to TAS containing original SIP REGISTER request message received from 5G RG as an XML document in the body of the SIP REGISTER request message for 3rd Party Registration on TAS.

13. TAS sends a HTTP GET request message (as defined in 3GPP TS 29.562 Section 5.3.2.2.8.1 [20]) containing subscriber identity & service indication to HSS for fetching associated repository data to which HSS responds with HTTP status code “200 OK” to TAS with the message body containing the UE's Repository Data for the requested Service Indication.

14. TAS sends a HTTP PUT request message (as defined in 3GPP TS 29.562 Section 5.3.2.7.2 [20]) for assigning itself as the serving TAS for the given subscriber to the HSS to update the repository data

for the given service indication. HSS updates the repository data for the given subscriber identity & service indication and responds with a HTTP status code “200 OK” or “204 No Content” to TAS.

15. TAS sees that subscriber is already registered and extends the registration with expiry value and responds to S-CSCF with SIP 200 OK for successful 3rd party registration on TAS.
16. TAS then sends a SIP SUBSCRIBE request message to S-CSCF for subscribing to registration (reg) event. S-CSCF responds with SIP 200 OK to TAS.
17. S-CSCF sends a SIP NOTIFY request message to TAS containing the status of each subscriber identity as an XML document in the body of the SIP NOTIFY request message.
18. TAS responds with SIP 200 OK to S-CSCF.

7.5.3.3 IMS De-Registration via SBI including 3rd Party Registration of TAS

The following section describes the IMS De-Registration of a 5G-RG via SBI and the 5G RG IMS De-registration flow as defined 3GPP TS 29.562 [20] & 3GPP TS 29.514 [19].

The following figures depicts the De-Registration message flow.

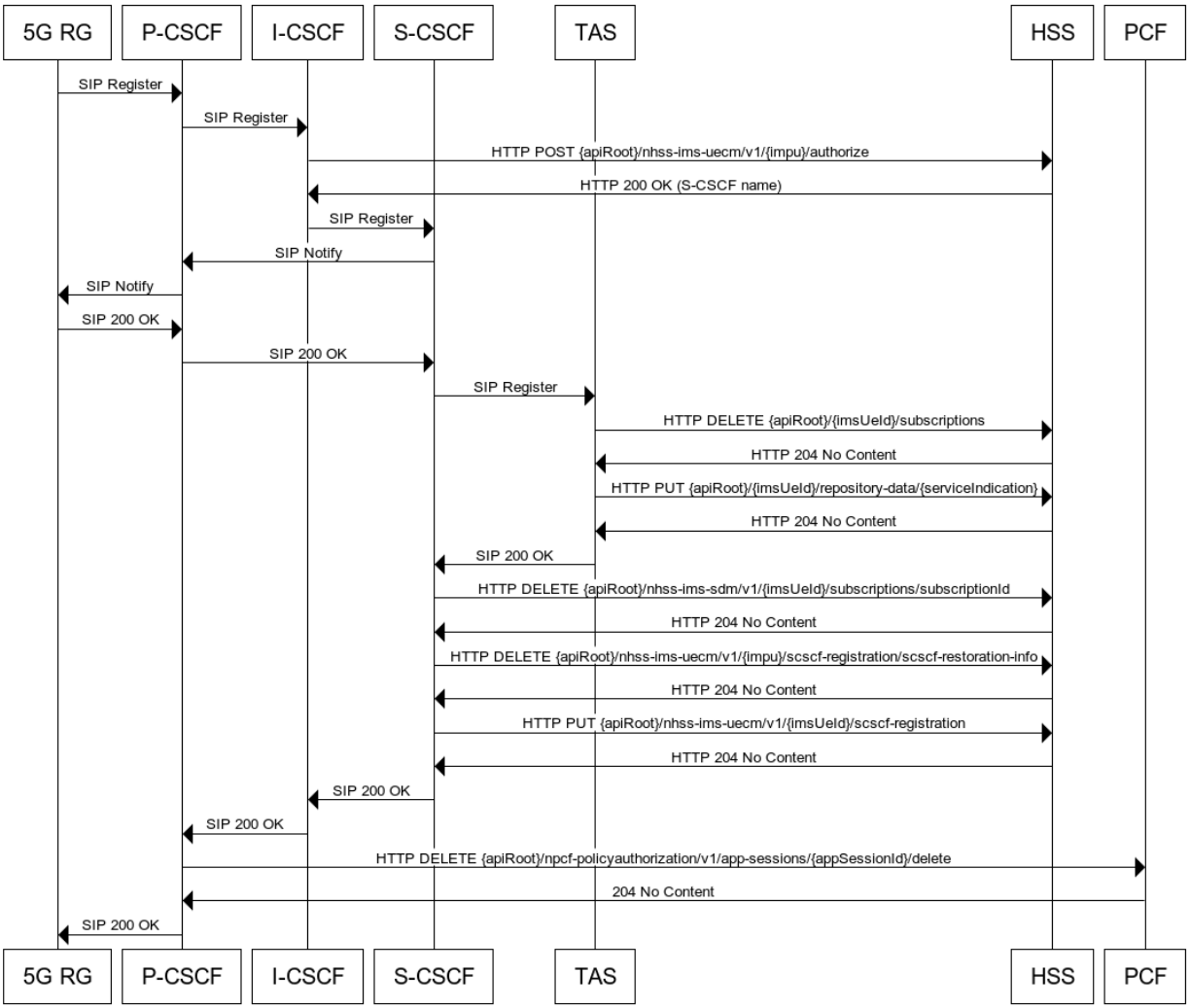


Figure 18: IMS De-Registration via SBI

1. 5G RG initiates IMS deregistration by sending an SIP REGISTER request message with expires=0 and expires tag with 0 in the Contact header to P-CSCF which is further forwarded to I-CSCF.

2. Upon receiving the SIP REGISTER request message, I-CSCF sends a HTTP POST request (containing IMPI and Authorization Type as “DEREGISTRATION”) to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as “SUBSEQUENT_REGISTRATION” and CSCF Server Name) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]).

3. I-CSCF then forwards the SIP REGISTER request message to the S-CSCF as given in the previous response.

4. S-CSCF sends a SIP NOTIFY request message to P-CSCF containing the status (Deactivated) of each subscriber identity as an XML document in the body of the SIP NOTIFY request message. P-CSCF sends the SIP NOTIFY request message to 5G RG which responds with SIP 200 OK to P-CSCF which further responds to S-CSCF with SIP 200 OK.

5. S-CSCF sends a SIP REGISTER request message to TAS with expires=0 for deregistering from TAS.

6. TAS sends a HTTP DELETE request message (as defined in 3GPP TS 29.562 Section 5.3.2.4.2 [20]) to unsubscribe from notification of data change in the repository data to the HSS. HSS responds with the HTTP status code “204 No Content”.

7. TAS sends a HTTP PUT request message (as defined in 3GPP TS 29.562 Section 5.3.2.7.2 [20]) for unassigning itself as the serving TAS for the given subscriber to the HSS to update the repository data for the given service indication. HSS updates the repository data for the given subscriber identity & service indication and responds with a HTTP status code “204 No Content” to TAS.

8. TAS now responds to S-CSCF with SIP 200 OK for successful de-registration on TAS.

9. The S-CSCF sends a HTTP DELETE request to the URI previously received during subscription creation (as defined in 3GPP TS 29.562 Section 5.3.2.4.2 [20]). On success, the HSS responds with HTTP status code “204 No Content”.

10. The S-CSCF sends a HTTP DELETE request to HSS to delete the S-CSCF restoration information (as defined in 3GPP TS 29.562 Section 5.2.2.8.2 [20]). If the resource exists (there is a previous S-CSCF restoration information stored in HSS for that user), HSS deletes it by replacing with the received S-CSCF restoration data and responds with HTTP status code “204 No Content”.

11. The S-CSCF sends a HTTP PUT request with the Registration Type set to “USER_DEREGISTRATION” to HSS to delete the S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.4.2 [20]). If the resource already exists and the SCSCF registered is the same, and if an IMPI is received as ImsUeId, HSS will deregister all IMPUs associated to that IMPI. If an IMPU is received as ImsUeId, HSS will deregister the IMPU and related IMPUs in the Implicit Registration Set for the related IMPI and responds with HTTP status code "204 No Content".

12. S-CSCF sends a SIP 200 OK response message to the P-CSCF via I-CSCF.

13. The P-CSCF requests the deletion of "Individual Application Session Context" resource with the intention to unsubscribe to the status of the IMS Signaling path (as defined in 3GPP TS 29.514 Section 4.2.4.2 [19]). The P-CSCF sends an HTTP DELETE request message to the PCF. The PCF confirms the deletion of subscription to IMS Signaling path status and replies with an HTTP status code “204 No Content” message back to the P-CSCF.

14. The P-CSCF sends the SIP 200 OK response message to the 5G RG.

8 SIP to SIP Call Flow – Detailed Session Establishment

The following sections describes the message flow that are relevant for an IMS SIP session establishment. It gives a more detailed view. In this example the users are in the same domain. In this scenario a SIP-to-SIP voice telephony session is established. It is assumed that A- and B-Party have negotiated the same voice codec for media. The SDP (Session Description Protocol) session is not detailed in this message flow. The terms of originating and terminating call leg are explained.

Figure 19 show the detailed message flow.

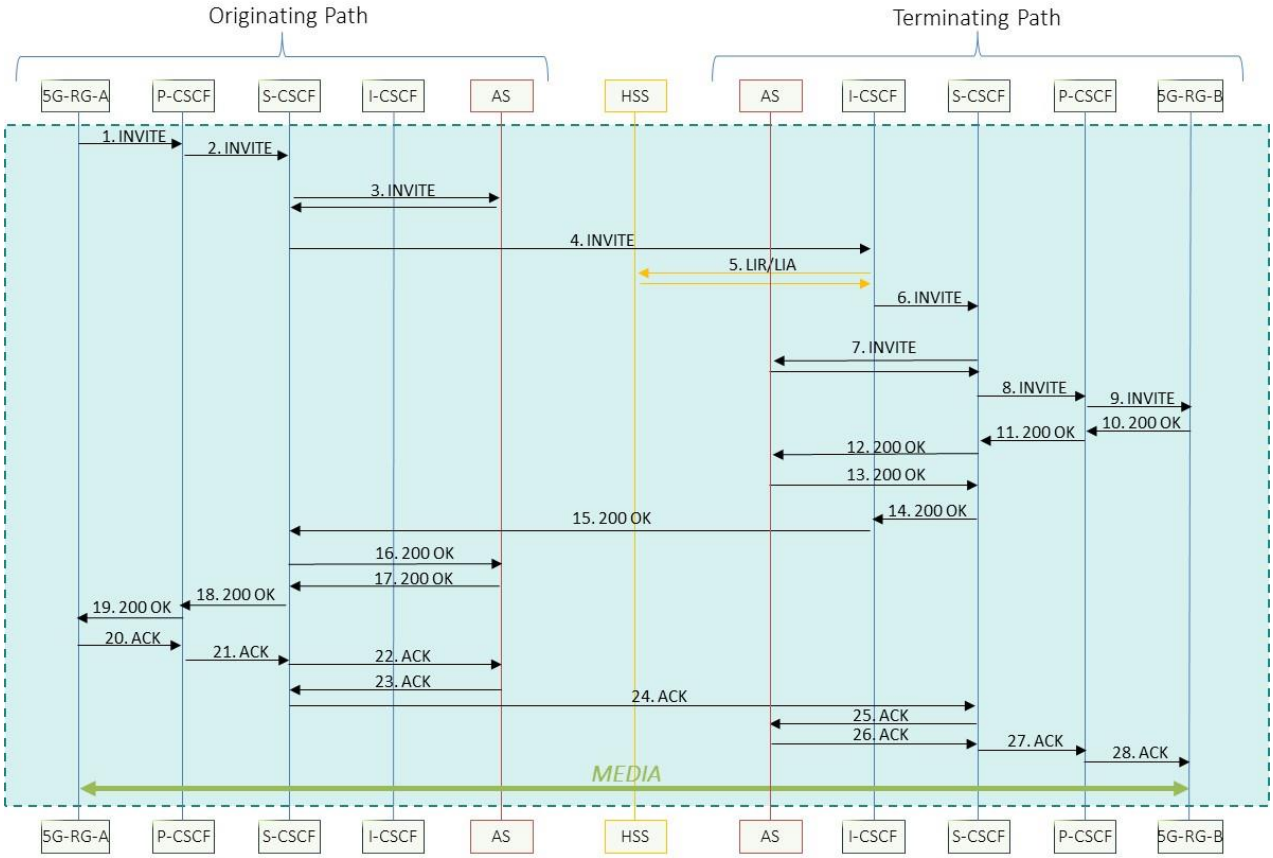


Figure 19: Detailed SIP-to-SIP Signaling Call Flow

1. An initial INVITE is sent from 5G-RG-A to the P-CSCF originating port. The session request is to establish an ‘audio’ session. The Call-ID for this call-leg is included in the INVITE message.

2. P-CSCF proxies the INVITE to the S-CSCF where 5G-RG-A is registered S-CSCF verifies the authentication result and proceeds the call if it is correctly validated.
   The S-CSCF downloads service profiles containing the iFCs pointing at the AS from the HSS for the user during the registration process.

3. After that the INVITE is forwarded to the AS to execute originating services of 5G-RG-A. The INVITE is sent back to the originating S-CSCF.

4. The INVITE is forwarded to the terminating I-CSCF.

5. The terminating I-CSCF queries the HSS with a LIR/LIA (Location Info Request/Location Info Answer) message to get the terminating user’s S-CSCF where 5G-RG-B is registered.

6. The INVITE is sent to the terminating S-CSCF.

7. The INVITE is sent to the terminating AS of 5G-RG-B to execute possible terminating services of 5G-RG-B. Then the INVITE is sent back to the terminating S-CSCF.

8. The S-CSCF sends the INVITE to the terminating user’s P-CSCF.

9. The INVITE is forwarded from the terminating P-CSCF to 5G-RG-B.

10. 5G-RG-B responds with a 200 OK, when the call is answered (the signaling of ringing is not described for simplification reasons). The Via headers from the INVITE are copied into the 200 OK.

11. The terminating P-CSCF checks the Via header in the 200 OK to see to which S-CSCF the response needs to be forwarded.

12. Similarly, the S-CSCF checks the Via header to forward to the appropriate AS.

13. The AS sends a 200 OK to the terminating S-CSCF.

14. The terminating S-CSCF checks the Via header to identify the correct terminating I-CSCF.

15. The terminating I-CSCF checks the Via header to see where to send the response and to identify the originating S-CSCF where the originating INVITE of 5G-RG-A had come.

16. The originating S-CSCF checks the Via header and sends it to the originating AS.

17. The originating AS sends a 200 OK back to the originating S-CSCF.

18. The originating S-CSCF checks the Via header to find the right originating P-CSCF and sends it to it.

19. The originating P-CSCF proxies the message out to 5G-RG-A by checking the Via header.

20. 5G-RG-A responds with an Acknowledgement (ACK) message. The ACK is a final acknowledgement and terminates the INVITE transaction. It is sent by 5G-RG-A (UAC) after receiving a final response (from UAS). The ACK itself is a transaction without a response.

21. The originating P-CSCF routes the ACK using the received Record-Route header field from the 200 OK message. The Record-Route headers are inserted by the IMS components to enforce that future SIP requests within the ongoing session are routed through this component. This ensures that this component remains in the signaling path. In case no Record-Route header was inserted by the IMS

component in the 200 OK the IMS request (here ACK method) is bypassing this component. The Record-Route headers from the 200 OK above are reversed and modified to Route headers in the ACK message thus making sure the next request, here the final ACK, is following the expected path.

22. The originating S-CSCF is checking the Route headers from the ACK and uses topmost route header indicating the right AS and where to route the ACK. According to basic SIP the “own” topmost Route header is removed. The ACK is forwarded to the AS.

23. The AS forwards the ACK to the originating S-CSCF.

24. The originating S-CSCF routes the ACK based on the Route header field to the terminating S-CSCF (I-CSCF has not added itself).

25. The terminating S-CSCF is routing the ACK to the terminating AS by using the information in the Route header.

26. The terminating AS forwards the ACK to the terminating S-CSCF.

27. The terminating S-CSCF routes the ACK to the terminating P-CSCF.

28. Finally, the terminating P-CSCF proxies the message to 5G-RG-B.

Generally, in IMS and SIP, the media stream is negotiated between UE-A and UE-B using the Session Description Protocol (SDP). SDP messages are carried in SIP and are used to negotiate media related information like codecs and addresses to send and receive media. In our example here the media stream is established between 5G-RG-A and 5G-RG-B.

SDP is described in RFC 4566 [28]. It is related to an Offer/Answer model [RFC 3264] [26]. SDP messages are exchanged in SIP Request and Response messages i.e., INVITE, Re-INVITE, 200 OK (INVITE), ACK (INVITE). 183 Session Progress and 180 Ringing can also carry SDP. As indicated above it describes the media related information for the session like IP address, port number or codecs. As SDP has no own transport protocol and uses other protocols like SIP.

Normally, the direct IP address information for media communication between 5G-RG-A and 5G-RG-B are not exchanged. In IMS the RTP [RFC 3550] [27] media messages are routed via a component called IMS-AGW (Access Gateway), see TS 23.228 [9], TS 23.334 [15], TS 23.237 [14], and TS 24.237 [17].

8.1 5G RG IMS to IMS Call via SBI

Previously proposed 5G RG IMS to IMS Call solution had diameter Cx interface based HSS interaction with the I/S-CSCF as defined in 3GPP TS 23.228 [9] but with 3GPP TS 29.562 [20] now defining I-CSCF an S-CSCF with N70/Nhss SBI interfaces. This chapter is to add and align the 5G RG IMS registration flow with the same.

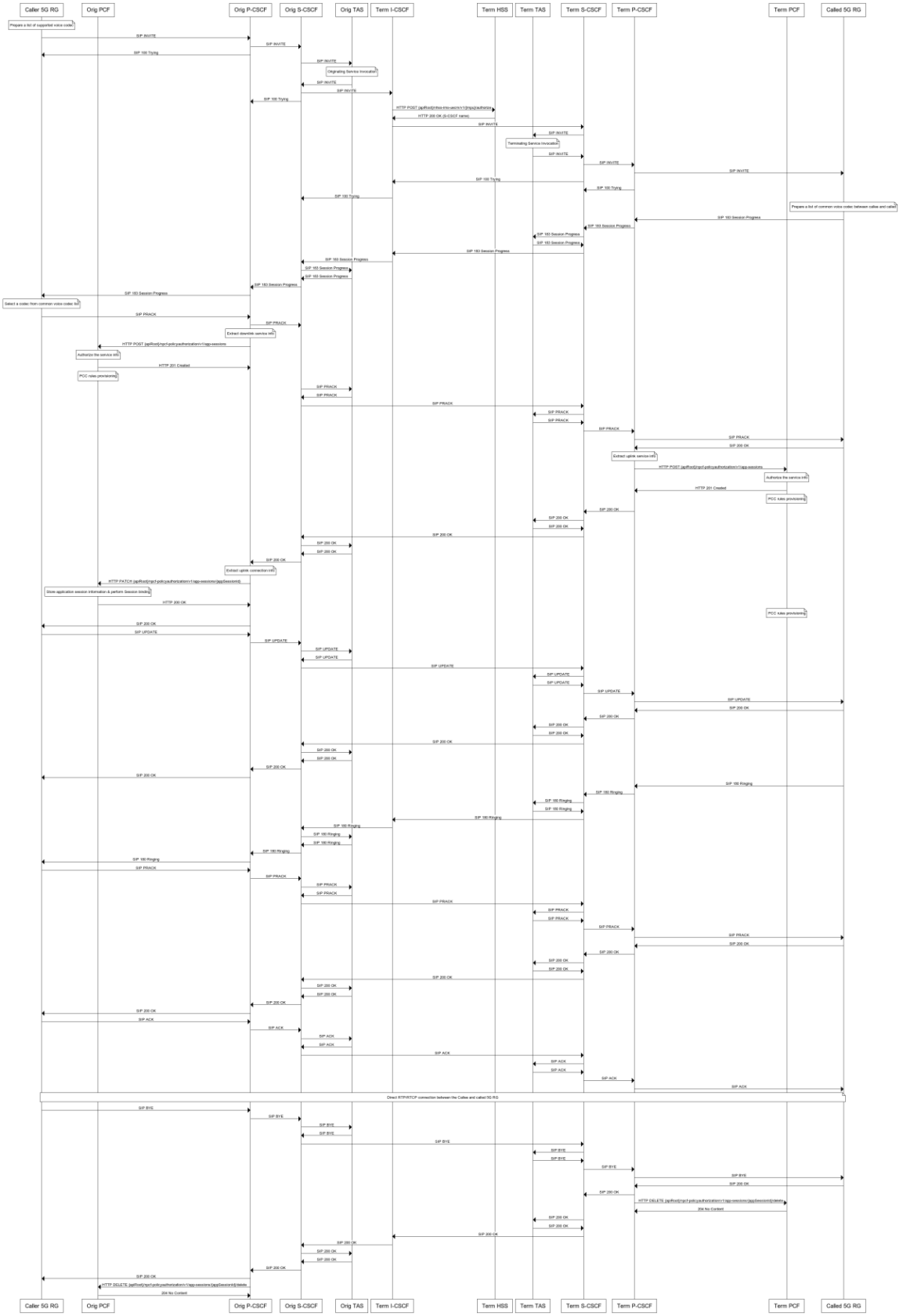


Figure 20: 5G RG IMS to IMS Call via SBI

1. An initial SIP INVITE request message is sent from Calling 5G RG to the Originating P-CSCF. The SDP includes all the Calling 5G RG supported codecs. The session request is to establish an ‘audio’ session. The message contains Route entries for the Calling 5G RG and the Originating S-CSCF address that was extracted from the Service-Route header in the registration SIP 200 OK response message. Security ports setup for IPSec SA establishment are used.

2. The Originating P-CSCF verifies that the preferred public identity specified in the SIP INVITE request message is currently registered. The Originating S-CSCF address for the subscriber was obtained at the time of registration (Service-Route header in the SIP 200 OK response message to the SIP REGISTER request message). The Originating P-CSCF queries the DNS to obtain the IP address of the Originating S-CSCF in the subscriber's home network. The Originating P-CSCF replaces the preferred identity header with the asserted identity header and forwards the message to the Originating S-CSCF in the home network. It adds a Record-Route header with its own address.

3. The Originating P-CSCF just acknowledges the SIP INVITE request message to the Calling 5G RG. The SIP 100 Trying response message indicates that the call setup is in progress.

4. The Originating S-CSCF invokes the Initial Filter Criteria (iFCs) (received from the HSS for the given subscriber during the IMS registration process) pointing at the Originating TAS and forwards the SIP INVITE request message to process originating services. Originating TAS will act as B2BUA and sends back the altered (due to active supplementary services) SIP INVITE request message to Originating S-CSCF with a new Call ID.

5. The Originating S-CSCF queries the DNS to obtain the IP address of the Originating I-CSCF in the called subscriber's home network.

6. The Originating S-CSCF removes the Route header and routes the SIP INVITE request message to the Terminating I-CSCF IP address obtained from the DNS query. Note that the Originating S-CSCF has added the telephone URL to the P-Asserted-Identity. The Via and Record-Route headers are also updated with self-address. The Originating S-CSCF acknowledges the SIP INVITE request message that was received from Originating P-CSCF.

7. Terminating I-CSCF queries the terminating HSS to obtain the Terminating S-CSCF serving the Called 5G RG.

8. Terminating I-CSCF sends a HTTP POST request to authorize and retrieve the Terminating S-CSCF server name. HSS responds with HTTP status code “200 OK” and provides Terminating I-CSCF with the identity of the serving Terminating S-CSCF.

9. As part of the message processing, a route entry is added for the Terminating S-CSCF. A new Via header is added to record that the message traversed this Terminating I-CSCF. The message is forwarded to the first route header (in this case, the Terminating S-CSCF).

10. The Terminating S-CSCF invokes the iFC’s (received from the HSS for the given subscriber during the registration process) pointing at the Terminating TAS and forwards the SIP INVITE request message to process terminating services. Terminating TAS acts as B2BUA and sends back the SIP INVITE request message to Terminating S-CSCF. Terminating S-CSCF maps the public URI to the Called 5G RG registered IP address and port number.

11. The public URI in the SIP INVITE request message is replaced with the Called 5G RG registered IP address and port number. The message is routed to the Terminating P-CSCF IP address that was recorded at the time of registration. The Via and Record-Route headers are updated.

12. The Terminating P-CSCF updates the Via and Route-Record headers and forwards the request to the Called 5G RG. Note that the secure port is included in the Via address.

13. The Called 5G RG examines the SDP list of available codecs. It prunes the list by excluding codecs that are not supported by the Called 5G RG. This list will be included in the SIP 183 Session Progress response message sent to the Calling 5G RG.

14. The Called 5G RG replies indicating that the session is in progress. The contact address is set its own IP address. The Via and the Record-Route headers are copied from the received SIP INVITE request message.

15. The Terminating P-CSCF removes its own Via header entry and addresses the message to the top via header (Terminating S-CSCF in this case). The Terminating P-CSCF also removes the secure port from the Record-Route.

16. SIP 183 Session Progress response message just retraces the path of the original SIP INVITE request message. Each function removes its own entry from the via header and forwards the message to the Via entry at the top. The Record-Route header is not touched.

17. Just like other nodes, the Originating P-CSCF removes its own entry from the Via header. The Originating P-CSCF also updates the Record-Route header to include the protected port number in its entry. This forces the Calling 5G RG to send all responses using the protected IPSec SA.

18. The Calling 5G RG examines the received common codec list and selects an codec to activate.

19. Now that the codec to be used has been selected, the PDP context activation is initiated for allocating resources for meeting the Quality of Service (QoS) requirements for the codec. The Originating P-CSCF requests the Originating PCF in order to request the authorization for the bearer usage for the Originating P-CSCF session. Subscription to Service Data Flow Deactivation is included in the request.

20. The Calling 5G RG now sends a SIP PRACK message to inform the called subscriber about the selected Codec. The message also indicates that currently the resources needed for meeting the quality-of-service requirements of the session are not available.

21. The Called 5G RG acknowledges the PRACK by sending a SIP 200 OK response message to Calling 5G RG. The message also indicates that quality of service for the session is not met for the Called 5G RG.

22. The final codec at the called side is decided. So, initiate the PDP context activation to allocate resources for meeting the QoS of the terminating leg of the call. The Calling PDP context activation has been completed. The Terminating P-CSCF requests the Terminating PCF in order to request the authorization for the bearer usage for the Terminating P-CSCF session. Subscription to Service Data Flow Deactivation is included in the request.

23. Since the Calling 5G RG PDP context has been activated, notify the Called 5G RG that the Calling 5G RG can now meet the quality of service in the send and receive direction by sending a SIP UPDATE message. Note that the Local QoS is still set to none as the Called 5G RG PDP context activation has not been completed.

24. The Called 5G RG PDP context activation has been completed. At this point, the Calling 5G RG and the Called 5G RG PDP contexts are both active. The QoS for the call can now be met.

25. Now all the resources for the call are in place. Ring the Called 5G RG subscriber to notify the user about the incoming call.

26. Inform the Calling 5G RG that the Called 5G RG is being rung. This serves as an implicit indication to the Calling 5G RG that the QoS at the Called 5G RG side has also been met.

27. The Calling 5G RG acknowledges the ringing message.

28. The Called 5G RG subscriber answers the call.

29. Notify the Calling 5G RG that that the call has been answered.

30. The Calling 5G RG acknowledges the SIP 200 OK response message. The call is now ready to enter conversation mode.

31. After finishing the conversation Calling 5G RG ends the call by sending a SIP BYE request message to Called 5G RG using the previously traversed path.

32. Called 5G RG sends a SIP 200 OK response message to Terminating P-CSCF.

33. Terminating P-CSCF then tears down the PDP context by sending HTTP DELETE request message to Terminating PCF.

34. Terminating P-CSCF sends the SIP 200 OK response message to Originating P-CSCF using the previously traversed path.

35. Originating P-CSCF then tears down the PDP context by sending HTTP DELETE request message to Originating PCF.

36. Originating P-CSCF forwards the SIP 200 OK response message to Calling 5G RG.

37. Calling 5G RG tears down the call.

8.2 Mobile termination unregistered subscriber services related to unregistered state and SBI

This call flow is also known as mobile termination unregistered subscriber, services related to unregistered state as per 3GPP TS 24.228 section 7.4.9.3 [22].

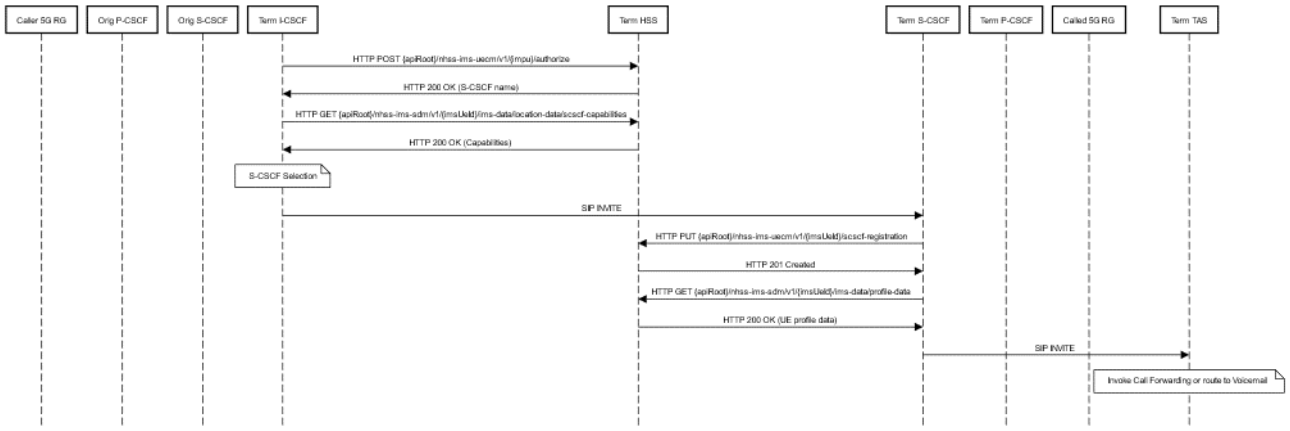


Figure 21 Mobile Termination for Unregistered Subscriber via SBI

1. An initial SIP INVITE request message is sent from Calling 5G RG to the Terminating I-CSCF via Originating P-CSCF and Originating S-CSCF.

2. Terminating I-CSCF sends a HTTP POST request message (containing IMPI and Authorization Type as “REGISTRATION”) to authorize the 5G RG to register to HSS. HSS responds with HTTP status code "200 OK" (containing Authorization Result as “FIRST_REGISTRATION” and CSCF Server Name empty) (as defined in 3GPP TS 29.562 Section 5.2.2.5.2 [20]) as the Called 5G RG is not registered in terminating IMS domain.

3. Terminating I-CSCF then sends a HTTP GET request message to retrieve Called 5G RG’s required S-CSCF capabilities with query parameters indicating the supported-features to Terminating HSS (as defined in 3GPP TS 29.562 Section 5.3.2.2.3 [20]). Terminating HSS responds with HTTP status code "200 OK" with the message body containing the Called 5G RG's required S-CSCF capabilities (Mandatory Capability List & Optional Capability List). Terminating I-CSCF selects the appropriate Terminating S-CSCF based on the S-CSCF capabilities required by the Called 5G RG from a Terminating S-CSCF pool and forwards the SIP INVITE request message to the selected S-CSCF.

4. Terminating S-CSCF sends a HTTP PUT request message to HSS to create S-CSCF registration information (as defined in 3GPP TS 29.562 Section 5.2.2.2.2 [20]) with IMS Registration Type as “UNREGISTERED_USER”. As there is no previous S-CSCF information stored in the Terminating HSS hence Terminating HSS will store the received S-CSCF registration data and respond with HTTP status code "201 created" with list of features supported.

5. Terminating S-CSCF sends a HTTP GET request message to download the resource representing the Called 5G RG's user profile in Terminating HSS. On success, the Terminating HSS responds

with HTTP status code "200 OK" with the message body containing the Called 5G RG's profile data which also includes the Initial Filter Criteria (IFC) (as defined in 3GPP TS 29.562 Section 5.3.2.2.4 [20]).

6. Terminating S-CSCF forwards the SIP INVITE request message to the Terminating TAS for invoking terminating services for unregistered subscribers like Call Forwarding or routing to Voicemail.

9 Voice Codecs

9.1 5G-RG recommended Voice Codecs

The wireless and wireline voice world are using different voice codecs. Some of the mobile voice codecs are rate adaptive and offering a high voice quality. The main standard codec in the PSTN is or was G.711 (a-law / µ-law). Therefore, this codec is supported in the fixed world and is used for features like classical fax.

In principle the 5G-RG device can handle various codecs or any voice codec, respectively, in case it is implemented on the 5G-RG. In case A- and B-party are using different codecs the media stream can be transcoded. The latter is provided by a transcoder in the IMS platform. Transcoding usually degrades the voice quality. Some of the codecs are royalty free, others require a license.

A typical mobile device codecs is the Adaptive Multi-Rate (AMR) narrow band codec including all codec modes via GSM and UMTS. The UE can support IMS voice with Adaptive Multi-Rate Wide Band (AMR-WB) codec including all codec modes as described in IR.92 section 3.2.1 [35], too.

This document gives a recommendation of a codec-set for IMS on 5G-RG making the 5G-RG compatible with the wireless and wireline voice implementations. This codec set considers both, potential fallback scenarios for wireless communication and legacy communication to POTS.

Recommended Codecs are:

- AMR (mobile)
- AMR-WB (mobile)
- EVS (mobile)
- G.711 a-law and µ-law (wireline)
- G.722 (wireline)

10 Emergency Services

10.1 Emergency call type

10.1.1 5G-RG detectable emergency call

When an end user dials a number related to an emergency, or similar regulated number, the 5G-RG shall check if this number is identified as a valid emergency number.

The following nominal cases are identified by the 5G-RG as valid emergency scenarios:

- Red button usage
- Emergency Numbers as defined in section 10 of [3GPP TS 22.101 [2]]
- Standard emergency numbers dialled by the user (112 and 911)
- Any emergency call number stored on a SIM/USIM (only possible if SIM/USIM present)
- 000, 08, 110, 999, 118 and 119 when a SIM/USIM is not present (these numbers are stored in the 5G-RG).
- Additional emergency numbers that may have been downloaded by the serving network when the SIM/USIM is present.

If the 5G-RG has identified an emergency number (as defined above), the 5G-RG initiates an emergency call setup procedure, enabling high priority in case of network congestion.

The local emergency call signaling plane will be prioritized by AMF upon initial emergency attach whereas media plane will be prioritized by P-CSCF through PCF to SMF by applying QoS on UPF for the said PDU session.

In case of network congestion 5G core will preempt the then non active registration and even normal calls for allowing emergency attach and call.

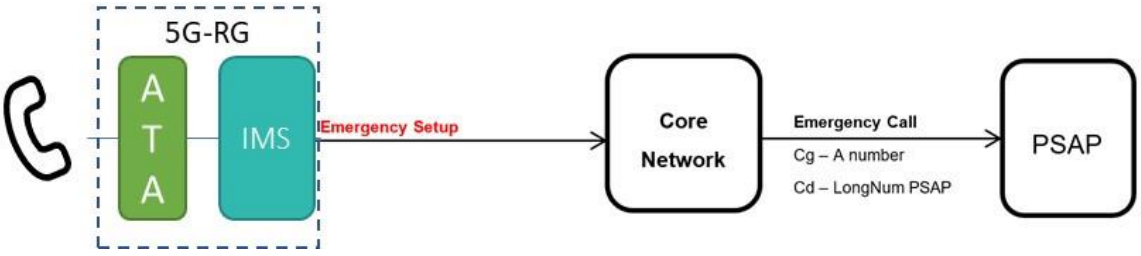


Figure 22: Emergency Call Setup

10.1.2 Non 5G-RG detectable emergency call

If telecommunication operators need to support “Local Emergency number” to comply with their legislation and these numbers are not made 5G-RG detectable as described in section 10.1.1, then the 5G-RG is not able to identify the emergency number dialed by the end user. The 5G-RG does not setup an emergency call but a normal call.

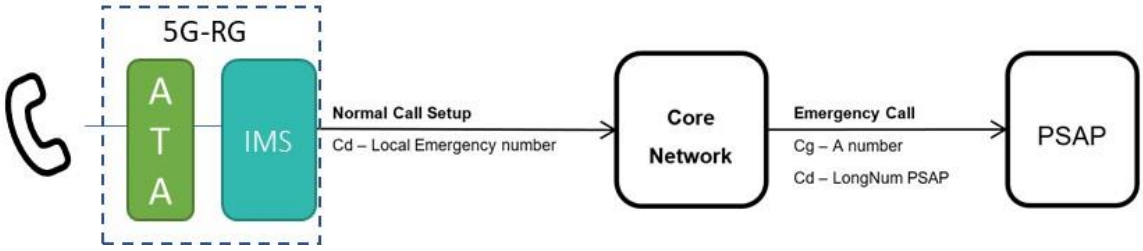


Figure 23: Normal Call Setup for Local Emergency Number

The local emergency call will not be prioritized on the way to the IMS Core Network, and could be dropped in case of network congestion.

Prioritization will take place once IMS (P-CSCF) recognized the emergency call.

The IMS core network identifies an emergency call, translates the dialed short number and routes the call to the right PSAP (Public Safety Answering Point). As such, for an identified emergency number, the call will be free of charge for the end user.

The call signaling is prioritized in the IMS core only but for media plane, it is prioritized in P-CSCF and is indicated to SMF through PCF to apply the right QoS and prioritization on UPF for the emergency PDU session on the way to the PSAP.

10.1.3 General Emergency Call Requirements

In this section general implementation options regarding emergency call requirements are described. These features are optional and not pure technic related:

- Emergency call can be established by using UE (POTS phone) “red button”, without the need to dial a dedicated number in order to minimize miss-connection in roaming case (if supported).
- Emergency call shall be free of charge for the user.

- Emergency calls shall be routed to the emergency services in accordance with national regulations where the subscriber is located.
- Emergency local numbers shall be provisioned on the 5G-RG in the SIM/eSIM
    - If the number is not provisioned, then the network needs to provision the emergency local number during the initial attach.

10.2 Emergency Services

The 5G-RG and the network shall support the IMS emergency services as specified in 3GPP TS 24.229 [8] and Annex H of 3GPP TS 23.167 [13]. In the case of the 5G-RG, this requirement is also applicable where the 5G-RG is in a limited service state. Limited service state refers to the availability of a specific service in the network and is defined in section 3.5 of 3GPP TS 23.122 [12].

5G-RGs in limited service state can perform an IMS emergency call without emergency registration. This is also applicable to 5G-RGs with reduced/limited voice capabilities.

Note: In corner cases the 5G-RG can attach to another operator's RAN.

The network is recommended to support an IMS emergency call from a 5G-RG in limited service state dependent on local policy and regulations.

The 5G-RG supports the Emergency Services natively over 5GS.

The 5G-RG supports the emerg-reg timer defined in table 7.8.1 of 3GPP TS 24.229 [16] and the related procedure defined in section 5.1.6.1 of 3GPP TS 24.229 [16]. The operator can configure the 5G-RG with the emerg-reg timer parameter as specified in Annex C.3 [23].

Fallback to preferred access and potential handover procedures from wireline to wireless and vice versa will not be covered in the initial release of this document.

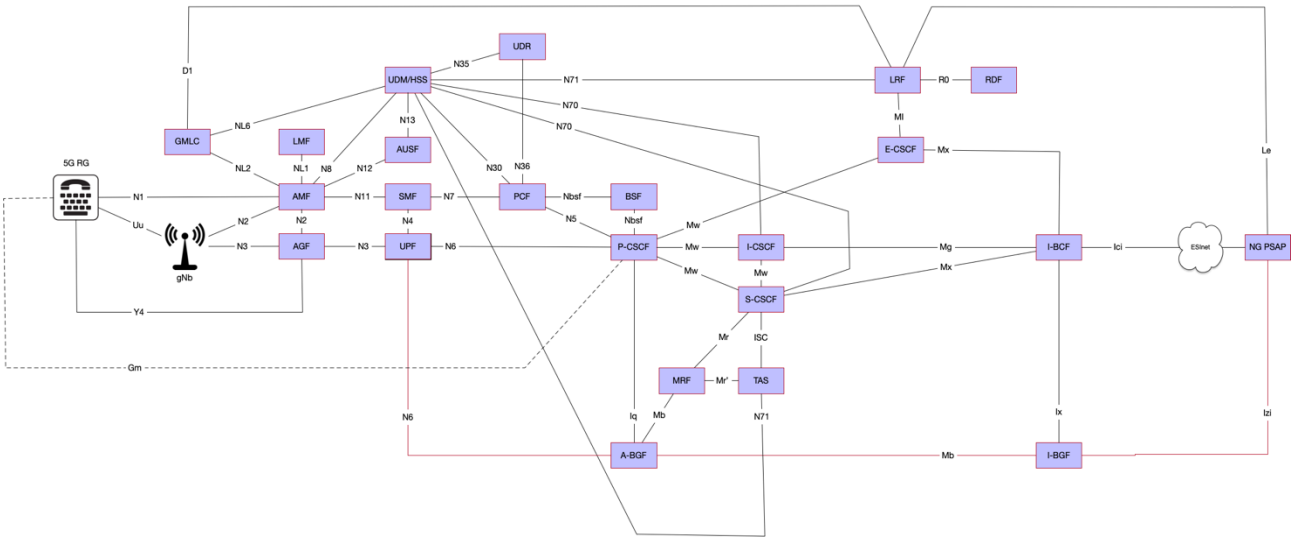
The default behavior of the 5G RG for emergency call when both wired and wireless connectivity are available is for further study (fallback procedure).

The behavior of emergency call handovers between wired and wireless connectivity is for further study and for clarification of the handover procedure.

10.3 Emergency Service Network Architecture

3GPP TS 23.167 [13] is the relevant standard and reference for creating network architecture & call flows for emergency services to be utilized by 5G-RG.

General:



Via ESInet:

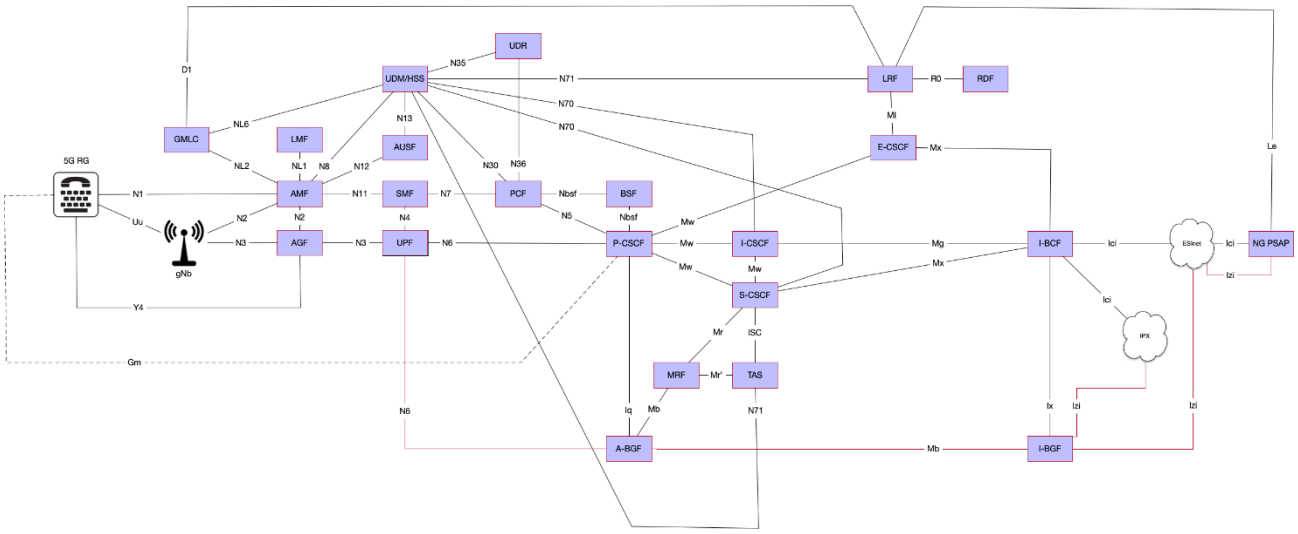


Figure 24: Emergency Service Network Architecture

Note: Legacy PSAP is not shown in the above architecture.

Note: LS (Location Server) in the above architecture will be GMLC.

Note: ESInet is only applicable for North-American operators, [ATIS-0500032 Standard for Implementation of an IMS-based NG9 1 1 Service Architecture]

Note: 5G RG will send the Cell ID in the P-ANI Header (P-Access Network Information)

Emergency Call Session Control Function (E-CSCF)

The Emergency Call Session Control Function is defined in 3GPP TS 23.167 [13].

The E-CSCF receives the emergency session establishment request from the Proxy Call Session Control Function (P-CSCF), queries the LRF/RDF for routing information, and forwards the call request toward the appropriate PSAP per the routing information. After initial call routing to the appropriate PSAP, the E-CSCF may or may not remain in the call path per implementation.

Location Retrieval Function (LRF)

The Location Retrieval Function (LRF) is defined in 3GPP TS 23.167 [13].

The LRF is queried by the E-CSCF and may obtain location information from the LS in the Originating Service Provider Network, if it is not provided in the call request (i.e., the location information is provided by reference and not by value). Either the location obtained from the LS or the location included in the

emergency call request (i.e., LbyV) is used to query the RDF. The LRF obtains routing information for an emergency session from the Routing Determination Function (RDF). It returns the routing information to the E-CSCF.

Routing Determination Function (RDF)

The Routing Determination Function (RDF) is defined in 3GPP TS 23.167 [13].

The RDF provides routing information for an emergency session based upon the location information in a request from the LRF. This routing information will designate a legacy PSAP or a NENA i3 PSAP.

Location Server (LS)

The Location Server (LS) is defined in 3GPP TS 23.167 [13].

The LS resides within the Originating Service Provider network. If the emergency call request does not have the location information (by-value) contained within it, the LRF or NENA i3 PSAP may query (i.e., send a dereference request to) the LS in the Originating Service Provider network to obtain it. If the Originating Service Provider network is an IMS-based network, the LS will be queried via an LRF in the Originating Service Provider network.

Interconnection Border Control Function (I-BCF)

The Interconnection Border Control Function (I-BCF) is defined in 3GPP TS 23.228 [9] and in 3GPP TS 23.167 [13].

In the context of emergency (9-1-1) originations, an egress I-BCF in an IMS-based NG9-1-1 Emergency Services Network will receive emergency calls from an E-CSCF in an IMS-based NG9-1-1 Emergency Services Network and forward them to a PSAP for further processing. In the context of callback calls, an egress I-BCF will receive callback calls from the PSAP and forward them to I-CSCF.

10.4 Reference Protocols

E-CSCF to LRF Reference Point (Ml)

The Ml interface is defined in 3GPP TS 23.167 [13] and expanded upon in Clauses 5.11 and 5.12 of 3GPP TS 24.229 [16]. The LRF operates as a SIP redirecting server to the E-CSCF. The E-CSCF sends a SIP INVITE to the LRF passing sufficient information in the headers and/or body to allow the LRF to acquire location if necessary and determine routing (via the RDF). The LRF responds with a SIP 300 Multiple Choices response containing routing information.

LRF to RDF Reference Point (R0)

The R0 Reference point is used by the LRF to obtain routing URIs from the RDF. The protocol between the LRF and the RDF is the Location to Service Translation Protocol (LoST). Using this protocol, the location and the service URN are sent to the RDF and a routing URI is returned. The LoST messages of findService and findServiceResponse are used. It is assumed that the RDF returns a SIP URI in all cases, regardless of the destination (i.e., legacy or NENA i3 PSAP).

LRF to LS Reference Point (D1)

The D1 Reference Point is specific to location acquisition for call routing where the emergency call request contains a location reference and the LRF has to query the Originating Service Provider network. The protocol used on the D1 Reference Point is the Dereferencing Protocol using HTTP Enabled Location Protocol (HELD). The messages of locationRequest and locationResponse are used.

Egress I-BCF to NENA i3 PSAP (ici)

The ici Reference Point is used by the I-BCF to deliver emergency sessions requests toward the NENA i3 PSAP. This Reference Point uses the SIP protocol.

10.5 Emergency Call Flow

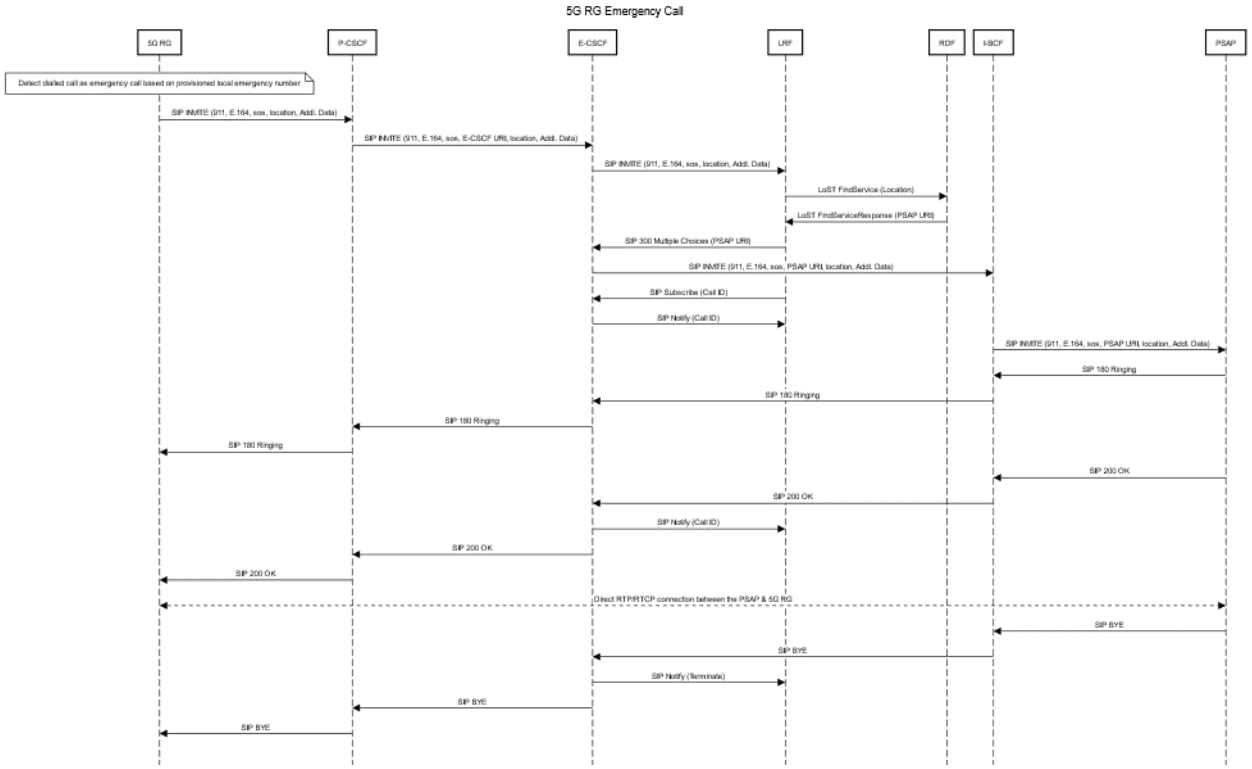


Figure 25: Emergency Call Flow

1. The user dials local emergency number.

2. The 5G RG detects the dialed number as emergency call based on the provisioned local emergency number.

3. The 5G RG constructs a SIP INVITE message containing “911” (expressed as a URI) in the To header, the sos service URN in the Request-URI, the E.164 number in the From and forwards the SIP INVITE to the P-CSCF.

4. The P-CSCF forwards the SIP INVITE message to the pre-configured E-CSCF.

5. The E-CSCF forwards the SIP INVITE to the LRF.

6. The LRF queries the RDF with the location and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

7. The RDF returns a Route (PSAP) URI.

8. The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

9. The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, and forwards it to the I-BCF. The SIP INVITE message contains “911” (expressed as a URI) in the To header, the PSAP URI in the Route header, the sos service URN in the Request-URI, the E.164 number in the From and P-Asserted-Identity headers, and a message body that contains the LbyV, Additional Data (by value) and the SDP. The SIP INVITE also contains a pointer to the LbyV in the Geolocation header, a Geolocation-Routing header set to “yes”, and a pointer(s) to the Additional Data in the Call-Info header(s).

10. (Optional) The LRF may subscribe to the state of the call.

11. (Conditional on Step 10) The E-CSCF sends an initial notification of the state.

12. The I-BCF forwards the SIP INVITE to the NENA i3 PSAP.

13. An indication that the call taker is being alerted is returned by the NENA i3 PSAP to the (egress) I-BCF (using a SIP 180 RINGING message).

14. The (egress) I-BCF passes the SIP 180 RINGING message to the E-CSCF.

15. The E-CSCF passes the SIP 180 RINGING message to the P-CSCF.

16. The P-CSCF passes the SIP 180 RINGING message to the 5G RG.

17. When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) I-BCF.

18. The (egress) I-BCF passes the SIP 200 OK message to the E-CSCF.

19. (Conditional on Step 10) The E-CSCF sends a notification to the LRF updating the call state.

20. The E-CSCF passes the SIP 200 OK message to the P-CSCF.

21. The P-CSCF passes the SIP 200 OK message to the 5G RG.

22. At this point a two-way connection is established between the 5G RG and the PSAP.

23. At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) I-BCF.

24. The SIP BYE is passed from the (egress) I-BCF to the E-CSCF.

25. (Conditional on Step 10) The E-CSCF then notifies the LRF that the call has terminated, provided the E-CSCF added itself to the Record-Route.

26. The E-CSCF passes the SIP BYE message to the P-CSCF.

27. The P-CSCF passes the SIP BYE message to the 5G RG.

10.6 AML Option

10.6.1 Definition

AML	AML (Advanced Mobile Location) is a supplemental service that makes handset location available to emergency services when an emergency call is placed. The user's location is sent directly to a Public Safety Answering Point or emergency call centre. GPS coordinates are sent using HTTPS. AML was standardised by the European Telecommunications Standards Institute (ETSI) Emergency Telecommunications Subcommittee (EMTEL)

Note: In case the AML Option is used, then the 5G-RG shall have the capability to identify its location based on (internal) GPS.

The usage and the availability of AML is for further study, see also [32], [33] and [34].

End of Broadband Forum Technical Report TR-493