**3GPP TSG-SA WG2 Meeting #165 S2-2410189**

**Hyderabad, India, Oct 14 - 18, 2024**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **23.228** | **CR** | **1478** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Support of third party user identity information in IMS |
|  |  |
| ***Source to WG:*** | Nokia, Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | NG\_RTC\_Ph2 |  | ***Date:*** | 2024-10-04 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | KI#4 on "Extensible IMS framework to support authorization and authentication of third-party identities in IMS sessions" was concluded during study phase Conclusion principles can be found in clause 8.4 of TR 23.700-77. This CR implements the conclusions principles in the specification. |
|  |  |
| ***Summary of change:*** | Conclusion principles from TR 23.700-77 are implemented in TS 23.228. Especially a new Annex is introdcued showing the overall architecture and descriping the impacts to functional entities. Provisioning of RCD information is not supported in this release of the specification due to missing agreement on the overall concept. |
|  |  |
| ***Consequences if not approved:*** | KI#4 conclusions from TR 23.700-77 are not implemented in normative phase. |
|  |  |
| ***Clauses affected:*** | 2, 3.1, 3.3, 4.6.3, 4.14, 4.16.3, Annex XX (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

>>>>START OF CHANGES <<<<

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 23.002: "Network Architecture".

[2] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[3] CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterisation of services supported by an ISDN".

[4] ITU Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] Void.

[7] 3GPP TS 23.221: "Architectural Requirements".

[8] 3GPP TS 22.228: "Service requirements for the IP multimedia core network subsystem".

[9] 3GPP TS 23.207: "End-to-end QoS concept and architecture".

[10] Void.

[10a] 3GPP TS 24.229: "IP Multimedia Call Control based on SIP and SDP; Stage 3".

[11] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[11a] 3GPP TS 29.207: "Policy control over Go interface".

[12] IETF RFC 3261: "SIP: Session Initiation Protocol".

[13] IETF RFC 3986: "Uniform Resource Identifiers (URI): Generic Syntax".

[14] IETF RFC 4282: "The Network Access Identifier".

[15] IETF RFC 3966: "The tel URI for Telephone Numbers".

[16] IETF RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[16a] IETF RFC 4941: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[17] ITU Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

[18] ITU Recommendation H.248: "Gateway control protocol".

[19] 3GPP TS 33.203: "Access Security for IP-based services".

[20] 3GPP TS 33.210: "Network Domain Security: IP network layer security".

[21] Void.

[22] 3GPP TR 22.941: "IP Based Multimedia Services Framework".

[23] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[24] 3GPP TS 23.003: "Technical Specification Group Core Network; Numbering, addressing and identification".

[25] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[26] 3GPP TS 32.260: "Telecommunication Management; Charging Management; IP Multimedia Subsystem (IMS) charging".

[27] 3GPP TS 22.071: "Technical Specification Group Services and System Aspects, Location Services (LCS); Service description, Stage 1".

[28] 3GPP TS 23.271: "Technical Specification Group Services and System Aspects, Functional stage 2 description of LCS".

[29] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2".

[29a] 3GPP TS 22.340: "IMS Messaging; Stage 1".

[30] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[31] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2".

[32] 3GPP TS 22.250: "IP Multimedia Subsystem (IMS) group management"; Stage 1".

[33] IETF RFC 2766: "Network Address Translation-Protocol Translation (NAT-PT)".

[34] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".

[35] Void.

[36] 3GPP TS 23.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service".

[37] Void.

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

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

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

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

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

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

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

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

[46] IETF RFC 5766: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[47] IETF RFC 5389: "Session Traversal Utilities for NAT (STUN)".

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

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

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

[51] IETF RFC 4787: "Network Address Translation (NAT) Behavioural Requirements for Unicast UDP".

[52] 3GPP TS 23.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2".

[53] 3GPP TS 22.173: "IMS Multimedia Telephony Service and supplementary services; Stage 1".

[54] 3GPP TS 23.203: "Policy and Charging Control architecture".

[55] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[56] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access".

[57] IETF RFC 4769: "IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information".

[58] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[59] 3GPP TS 29.333: "Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp Interface; Stage 3".

[60] 3GPP2 X.S0011: "cdma2000 Wireless IP Network Standard".

[61] 3GPP2 C.S0001-D: "Introduction to cdma2000 Spread Spectrum Systems - Revision D".

[62] 3GPP2 C.S0024-A: "cdma2000 High Rate Packet Data Air Interface Standard, April 2004".

[63] 3GPP2 C.S0084-000: "Overview for Ultra Mobile Broadband (UMB) Air Interface Specification".

[64] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".

[65] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

[66] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services".

[67] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity".

[68] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[69] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[70] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[71] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[72] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol".

[73] 3GPP TS 23.333: "Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp interface: Procedures Descriptions".

[74] 3GPP TS 23.334: " IMS Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures Descriptions".

[75] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[76] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[77] 3GPP TS 22.153: "Multimedia priority service".

[78] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[79] 3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh Interface; Signalling flows and message contents".

[80] 3GPP TS 23.380: "IP Multimedia Subsystem (IMS); IMS Restoration Procedures".

[81] 3GPP TS 24.525: "Business trunking; Architecture and functional description".

[82] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[83] 3GPP TS 33.328: "IP Multimedia (IM) Subsystem media plane security".

[84] IETF RFC 8825: "Overview: Real Time Protocols for Brower-based Applications".

[85] W3C: "WebRTC 1.0: Real-time Communication Between Browsers", W3C Recommendation, 26 January 2021, https://www.w3.org/TR/2021/REC-webrtc-20210126/.

[86] W3C: "Cross-Origin Resource Sharing", W3C Proposed Recommendation, 05 December 2013, http://www.w3.org/TR/2013/PR-cors-20131205/.

[87] ITU-T Recommendation T.140: "Protocol for multimedia application text conversation".

[88] IETF RFC 6455: "The WebSocket Protocol".

[89] IETF RFC 7118: "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)".

[90] IETF RFC 4571: "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport".

[91] 3GPP TS 24.610: "Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem".

[92] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[93] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[94] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[95] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[96] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[97] 3GPP TS 23.632: "User data interworking, coexistence and migration; Stage 2".

[98] 3GPP TS 29.563: "5G System (5GS); Home Subscriber Server (HSS) services for interworking with Unified Data Management (UDM); Stage 3".

[99] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[100] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[101] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

[102] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

[103] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[104] 3GPP TS 26.264: "IMS-based AR Real-Time Communication".

[105] 3GPP TS 24.186: "IMS Data Channel applications; Protocol specification".

[106] IETF RTC 4028: "Session Timers in the Session Initiation Protocol (SIP)".

[xx] IETFdraft-ietf-sipcore-callinfo-rcd-12: "SIP Call-Info Parameters for Rich Call Data".

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

[yy] IETFdraft-ietf-stir-passport-rcd-26: "PASSporT Extension for Rich Call Data".

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

>>>>NEXT CHANGE <<<<

## 3.1 Definitions

Refer to TS 23.002 [1] for the definitions of some terms used in this document.

For the purposes of the present document the terms and definitions given in TR 21.905 [68] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [68].

For the purposes of the present document, the following terms and definitions given in TS 23.003 [24] apply:

**- Distinct Public Service Identity**

**- Public User Identity**

**- Wildcarded Public User Identity**

**- Wildcarded Service User Identity**

**Alias Public User Identities:** A set of Public User Identities that belong to the same alias group as specified in TS 29.228 [30].

**ALG:** Application Level Gateway (ALG) is an application specific functional entity that allows communication between disparate address realm or IP versions, e.g. an IPv6 node to communicate with an IPv4 node and vice versa, when certain applications carry network addresses in the payloads like SIP/SDP. NA(P)T-PT or NA(P)T is application unaware whereas ALGs are application specific translation entities that allow a host running an application to communicate transparently with another host running the same application but in a different IP version or IP address realm. See IETF RFC 2663 [34] for more details.

 For IMS, an IMS ALG provides the necessary application function for SIP/SDP protocols in order to communicate between different address realms or IP versions, e.g. IPv6 and IPv4 SIP applications.

**Application data channel:** A data channel within an IMS session used to transfer data of data channel applications between UEs or between the UE and the network.

**AR Application Server:** An application server used to control the service logic related to AR communication via IMS data channel.

**Bootstrap data channel:** A data channel established within an IMS session between the UE and the network, to transfer a graphical user interface that can include a list of data channel applications.

**Business trunking:** as defined in TS 24.525 [81].

**Data channel application:** A HTML page including JavaScript(s) and optionally image(s) and style sheet(s). It is downloaded from the network to the UE through the bootstrap data channel.

**DC Application Server:** An application server that interacts with the DCSF and the DC media function for data channel traffic handling.

**Distinct Public User Identity:** used in relation to wildcarded Public User/Service Identities to denote an explicitly provisioned Public User/Service Identity. See more details in TS 23.003 [24].

**Entry point:** In the case that border control concepts are to be applied in an IM CN subsystem, then these are to be provided by capabilities within the IBCF, and the IBCF acts as an entry point for this network (instead of the I‑CSCF). In this case the IBCF and the I‑CSCF can be co-located as a single physical node. If border control concepts are not applied, then the I-CSCF is considered as an entry point of a network. If the P‑CSCF is in the home network, then the I‑CSCF is considered as an entry point for this document.

**Exit point:** If operator preference requires the application of border control concepts then these are to be provided by capabilities within the IBCF, and requests sent towards another network are routed via a local network exit point (IBCF), which will then forward the request to the other network (discovering the entry point if necessary).

**Geographical Identifier:** A Geographical Identifier identifies a geographical area within a country or territory. See more details in clause E.8.

**Geo-local service number:** A local service number that is used to access a service in the roamed network (a local service where the subscriber is located).

**Home local service number:** A local service number is used to access a service that is located in the home network of the user.

**HSS Group ID:** This refers to one or more SBI capable HSS instances managing a specific set of IMPIs/IMPUs.

**IMC:** IMS Credentials as defined in TR 21.905 [68].

**IMS application reference:** An IMS application reference is the means by which an IMS communication service identifies an IMS application.

**IMS application:** An IMS application is an application that uses an IMS communication service(s) in order to provide a specific service to the end-user. An IMS application utilises the IMS communication service(s) as they are specified without extending the definition of the IMS communication service(s).

**IMS communication service identifier:** An IMS communication service identifier uniquely identifies the IMS communication service associated with the particular IMS request.

**IMS communication service:** An IMS communication service is a type of communication defined by a service definition that specifies the rules and procedures and allowed medias for a specific type of communication and that utilises the IMS enablers.

**IMS enabler:** An IMS enabler is a set of IMS procedures that fulfils specific function. An IMS enabler may be used in conjunction with other IMS enablers in order to provide an IMS communication service.

**Instance identifier:** An identifier, that uniquely identifies a specific UE amongst all other UEs registered with the same Public User Identity.

**Inter-IMS Network to Network Interface:** The interface which is used to interconnect two IM CN subsystem networks. This interface is not constrained to a single protocol.

**IP Flow:** Unidirectional flow of IP packets with the following properties:

- same destination IP address and port number;

- same source IP address and port number;

- same transport protocol (port numbers are only applicable if used by the transport protocol).

**IP-Connectivity Access Network:** refers to the collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities. An example of an "IP-Connectivity Access Network" is GPRS.

**IP SM GW (IP short message gateway):** An IP SM GW is an AS providing the support of Short Message Service of the IMS domain. See more details in TS 23.204 [56].

**Local Service Number:** A local service number is a telephone number in non-international format. A local service number is used to access a service that may be located in the home network of the user (home local service number) or the roamed network of the user (geo-local service number).

**Media Flow:** One or more IP flows carrying a single media instance, e.g. an audio stream or a video stream. In the context of this specification the term Media Flow is used instead of IP Flow regardless of whether the actual IP packet corresponds to media plane information (e.g. audio RTP flow) or control signalling (e.g. RTCP or SIP Signalling).

**MPS:** Based on TS 22.153 [77]. Multimedia Priority Service allows authorized users to obtain and maintain radio and network resources with priority, also during national security or emergency situations when PLMN congestion may occur.

**MPS session:** A session (e.g. voice, video, data session) for which priority treatment is applied for allocating and maintaining radio and network resources.

**MPS for Messaging:** Within the scope of this specification, IMS Immediate Messaging and IMS Session-based Messaging delivered with MPS priority.

**MPS-subscribed UE:** A UE having a USIM with MPS subscription.

NAT-PT/NAPT-PT: NAT-PT uses a pool of globally unique IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across the IP version boundaries. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing between the two IP domains without requiring any changes to end points, like the UE. NAT-PT needs to track the sessions it supports and mandates that inbound and outbound data for a specific session traverse the same NAT-PT router.

 NAPT-PT provides additional translation of transport identifier (e.g. TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of IPv6 hosts to be multiplexed into the transport identifiers of a single assigned IPv4 address. See IETF RFC 2766 [33] for more details.

**Network Address Translation (NA(P)T):** method by which IP addresses are mapped from one group to another, transparently to end users. Network Address Port Translation, or NA(P)T is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. See RFC 3022 [65] for further details.

**Outbound:** Managing Client Initiated Connections in the Session Initiation Protocol (Outbound) defines behaviours for User Agents, registrars and proxy servers that allow requests to be delivered on existing connections established by the User Agent. See RFC 5626 [48] for further details.

**Preferred Circuit Carrier Access:** An IMS service that allows a specific long distance circuit carrier to be selected for a long distance call.

**Preferred Circuit Carrier Selection:** An IMS service that allows the subscriber to select a long distance circuit carrier per call when dialling a call origination.

**Rich Call Data (RCD) server:** It refers to a server in a third party network storing IMS subscriber specific RCD information.

**Rich Call Data (RCD) server address:** It refers to the address of an RCD server.

**Rich Call Data (RCD) information:** It refers to a collection of properties associated with an IMS subscriber. Such properties can be caller name, Email address, telephone number, job title and characteristics of an organization. Details of the properties in the context of RCD can be found in draft-ietf-sipcore-callinfo-rcd-12 [xx].

**Rich Call Data (RCD) URL:** It refers to the URL from where RCD information of a specific IMS subscriber stored at an RCD server can be retrieved from.

**Service User:** According to TS 22.153 [77].

**Stand-alone Non-Public Network:** A non-public network not relying on network functions provided by a PLMN.

**STUN:** Simple Traversal of UDP Through NAT (STUN), provides a toolkit of functions. These functions allow entities behind a NAT to learn the address bindings allocated by the NAT, to keep those bindings open, and communicate with other STUN-aware devices to validate connectivity. See RFC 5389 [47] for further details.

**STUN Keep-alive:** Is a usage of STUN, to keep NAT bindings open.

**STUN Relay:** Is a usage of STUN, that allows a client to request an address on the STUN server itself, so that the STUN server acts as a relay. See IETF RFC 5766 [46] for further details.

**Subscriber:** A Subscriber is an entity (comprising one or more users) that is engaged in a Subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of user authorized to enjoy these services, and also to set the limits relative to the use that users make of these services.

**Transport address:** A unique identifier of transport-layer address, i.e. a combination of a network address, protocol identifier and port number. For example an IP address and a UDP port.

**Standalone IMS Data Channel Session:** An IMS session with only data channel media component(s) defined in TS 26.114 [76] without accompanying audio/video/messaging media.

>>>>NEXT CHANGE <<<<

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [68] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [68].

5GS 5G System

API Application Program Interface

APN Access Point Name

AS Application Server

A2P Application to Person

BCSM Basic Call State Model

BG Border Gateway

BGCF Breakout Gateway Control Function

BS Bearer Service

CAMEL Customised Application Mobile Enhanced Logic

CAP Camel Application Part

CDR Charging Data Record

CN Core Network

CS Circuit Switched

CSCF Call Session Control Function

CSE CAMEL Service Environment

DC Data Channel

DCAR Data Channel Application Repository

DCMTSI Data Channel Multimedia Telephony Service for IMS

DCSF Data Channel Signalling Function

DHCP Dynamic Host Configuration Protocol

DNN Data Network Name

DNS Domain Name System

ECN Explicit Congestion Notification

ENUM E.164 Number Mapping

GGSN Gateway GPRS Support Node

GLMS Group and List Management Server

GMLC Gateway Mobile Location Centre

GRUU Globally Routable User Agent URI

GUP Generic User Profile

HSS Home Subscriber Server

IBCF Interconnection Border Control Function

I‑CSCF Interrogating‑CSCF

IETF Internet Engineering Task Force

IM IP Multimedia

IMC IMS Credentials

IMS IP Multimedia Core Network Subsystem

IMS ALG IMS Application Level Gateway

IMSI International Mobile Subscriber Identifier

IN Intelligent Network

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IP‑CAN IP-Connectivity Access Network

IP‑SM‑GW IP Short Message Gateway

ISDN Integrated Services Digital Network

ISIM IMS SIM

ISP Internet Service Provider

ISUP ISDN User Part

IWF Interworking Function

NP Number portability

MAP Mobile Application Part

MGCF Media Gateway Control Function

MGF Media Gateway Function

MRB Media Resource Broker

MRFC Multimedia Resource Function Controller

MRFP Multimedia Resource Function Processor

NAI Network Access Identifier

NAPT Network Address Port Translation

NAT Network Address Translation

NA(P)T-PT Network Address (Port-Multiplexing) Translation-Protocol Translation

II-NNI Inter-IMS Network to Network Interface

OSA Open Services Architecture

P2A Person to Application

P2P Person to Person

P‑CSCF Proxy‑CSCF

PCC Policy and Charging Control

PCEF Policy and Charging Enforcement Function

PCRF Policy and Charging Rules Function

PDN Packet Data Network

PDP Packet Data Protocol e.g. IP

P‑GRUU Public Globally Routable User Agent URI

PLMN Public Land Mobile Network

PSI Public Service Identity

PSTN Public Switched Telephone Network

QoS Quality of Service

RAB Radio Access Bearer

RCD Rich Call Data

RFC Request for Comments

SCS Service Capability Server

S‑CSCF Serving‑CSCF

SDP Session Description Protocol

SGSN Serving GPRS Support Node

SLF Subscription Locator Function

SNPN Stand-alone Non-Public Network

SSF Service Switching Function

SS7 Signalling System 7

SIM Subscriber Identity Module

SIP Session Initiation Protocol

S‑GW Signalling Gateway

TAS Telephony Application Server

T‑GRUU Temporary Globally Routable User Agent URI

THIG Topology Hiding Inter-network Gateway

TrGW Transition Gateway

UE User Equipment

UMTS Universal Mobile Telecommunications System

URL Universal Resource Locator

USIM UMTS SIM

>>>>NEXT CHANGE <<<<

### 4.6.3 Serving‑CSCF

The Serving‑CSCF (S‑CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S‑CSCFs may have different functionalities. The functions performed by the S‑CSCF during a session are:

For Registration:

- May behave as a Registrar as defined in IETF RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (e.g. HSS).

- When a registration request includes an Instance ID with the contact being registered and indicates support for GRUU, the S‑CSCF shall assign a unique P‑GRUU and a new and unique T‑GRUU to the combination of Public User Identity and Instance ID.

- If a registration request indicates support for GRUU, the S‑CSCF shall return the GRUU set assigned to each currently registered Instance ID.

- The S‑CSCF shall notify subscribers about registration changes, including the GRUU sets assigned to registered instances.

- During registration process, the S-CSCF shall provide policy information, if available, for a Public User Identity from the HSS to the P-CSCF and/or UE.

NOTE 1: For example, the policy information includes MPS IMS Subscription status and policy applicable to enterprise network subscribers.

For Session-related and session-unrelated flows:

- Session control for the registered endpoint's sessions. It shall reject IMS communication to/from Public User Identity(s) that are barred for IMS communications after completion of registration, as described in clause 5.2.1.

- May behave as a Proxy Server as defined in IETF RFC 3261 [12] or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.

- May behave as a User Agent as defined in IETF RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.

- Based on the determined served user, handle interaction with Services Platforms for the support of Services

- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)

- For an originating endpoint (i.e. the originating user/UE, or originating AS)

- Obtain from a database the Address of the entry point for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and forward the SIP request or response to that entry point.

 If a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity encapsulated in the P‑GRUU or associated with the T‑GRUU belongs to the same service profile.

- When the destination name of the destination user (e.g. dialled phone number or SIP URI), and the originating user is a customer of the same network operator, forward the SIP request or response to an I‑CSCF within the operator's network.

- Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

- Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.

- Ensure the originating end point is subscribed to the determined IMS communication service.

- Ensure that the content of the SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the originating endpoint matches the determined IMS communication service definition, based on originating user's subscription.

- When the INVITE message includes an MPS code or an MPS input string, forward the INVITE, including the Service User's priority level if available.

- When an MPS user is authorized by an AS for priority service, include the Service User's priority level received from the AS in the INVITE and forward the INVITE.

NOTE 2: The mechanism to provide authorisation by an AS for priority service is out of scope of this specification.

- Attestation of the identity of the originating subscriber if configured through operator policies. Optionally the S-CSCF can invoke an AS for attestation of the identity of originating subscriber, if configured through operator policies.

- Optionally the S-CSCF can invoke an AS for attestation of the RCD information or RCD URL of originating subscriber, if configured through operator policies as per Annex XX.

NOTE 3: Only one network element performs attestation for an originating subscriber in the originating network.

- Assertion of authorization for the Resource-Priority information for an IMS priority session if configured through operator policies. Optionally, the S-CSCF can invoke an AS for assertion and signing of the authorization for the Resource-Priority information for the IMS priority session, if configured through operator policies.

- If the request is an originating request from an Application Server:

- Verify that the request coming from the AS is an originating request, determine the served user and apply procedures accordingly (e.g. invoke interaction with Service Platforms for originating services, etc.).

- Process and proceed with the request even if the served user on whose behalf the AS had generated the request is unregistered. If the served user is unregistered, the S‑CSCF shall execute any unregistered origination service logic on behalf of the served user before forwarding requests from an AS.

- Process and proceed with other requests to and from the served user on whose behalf the AS had generated the request.

- Reflect in the charging information that an AS has initiated the session on behalf of a served user.

- For a destination endpoint (i.e. the terminating user/UE)

- Forward the SIP request or response to a P‑CSCF.

- Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, if the user is to receive the incoming session via the CS domain.

- Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.

- Ensure the terminating end point is subscribed to the determined IMS communication service.

- Ensure that the content of SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the destination end point matches the determined IMS communication service definition, based on terminating user's subscription.

- If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in IETF RFC 3312 [41].

- In addition, and if configured through operator policies, the S-CSCF may perform signature verification of the RCD information or RCD URL of the originating subscriber for terminating requests, if a signature is included as per Annex XX.

- Optionally for a redirected session, if configured through operator policies, performs attestation of the identity of the diverting subscriber initiating the diversion.

- Proxies a terminating request to an AS associated with the terminating user for signature verification if signature verification is required.

NOTE 4: The S-CSCF would normally proxy any terminating request to an AS via ISC for additional processing.

- For an originating request with a Request URI containing the SIP representation of an E.164 number, and configured per operator policy:

- the S‑CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI using the procedures specified in clause 4.3.5. As stated in clause 4.3.5, if the E.164 address translation fails, the request may be forwarded to a BGCF to allow routing to the PSTN and if the translation succeeds, the Request URI is updated and the request is routed based on the SIP URI that was obtained.

NOTE 5: When requests are sent towards another domain they may, if required, be routed via a local network exit point (IBCF), which will then forward the request to the entry point of the other domain. More details on this can be found in clause 4.14 and Annex I.

Based on local configuration, the S‑CSCF may be provisioned as the contact point within an operator's network for transit IMS scenarios and may perform transit routing functions (see clause 5.19).

Charging and resource utilisation:

- Generation of CDRs

>>>>NEXT CHANGE <<<<

## 4.14 Border Control concepts

Based on operator preference, border control functions may be applied between two IM CN subsystem networks or between an IM CN subsystem network and other SIP based multimedia network. These functions are provided by the IBCF and include:

- Controlling transport plane functions;

- Supporting functions to allow establishing communication between disparate address realms' SIP applications;

- Supporting functions to allow establishing communication between IM CN subsystems using different media codecs based on the interworking agreement and session information;

- Providing network configuration hiding to restrict the following information from being passed outside of an operator's network: exact number of S‑CSCFs, capabilities of S‑CSCFs, or capacity of the network, etc;

NOTE 1: Network configuration hiding was not intended to be invoked in IMS roaming scenarios when the P‑CSCF and IBCF are both located in the visited network as information available in certain SIP headers may be used by the home network for further processing of signalling messages.

- Screening SIP signalling information based on source/destination and operator policy (e.g. remove information that is of local significance to an operator) and optionally, for an IBCF located in the home network, policing the IMS Communication Service ID;

- Generation of CDRs;

- Invoking an IWF when interworking between different SIP profiles or different protocols (e.g. SIP and H.323) is necessary; in this case the IWF acts as an entry point for the IMS network;

NOTE 2: IWF and IBCF may be co-located. The IWF is not specified within this release of the specification.

- Selecting the appropriate signalling interconnect.

- Indicating whether an incoming SIP request is to be handled as an originating request by subsequent nodes in the IMS network.

- For an originating session leaving an IBCF, the IBCF of the originating network, if configured through operator policies, invokes an AS for the signing of attestation and identity information, if available in the incoming request. The IBCF includes the signed information in the outgoing request.

- For an originating session leaving an IBCF, the IBCF of the originating network, if configured through operator policies, invokes an AS for the signing of RCD information or RCD URL, if available in the incoming request. The IBCF includes the signed information in the outgoing request as per Annex XX.

- For an originating session leaving an IBCF, the IBCF of the originating network, if configured through operator policies, invokes an AS for the signing of Resource-Priority related information, if available in the incoming request. The IBCF includes the signed Resource-Priority related information in the outgoing request.

- For a terminating session entering the IBCF without identity attestation information, the IBCF adds, if configured through policies, gateway attestation information based on the network from which the request was received.

- For a terminating session entering the IBCF with signed identity attestation information, the IBCF, if configured through policies, invokes an AS for signature verification.

- For a terminating session entering the IBCF with signed RCD information or signed RCD URL, the IBCF, if configured through policies, invokes an AS for signature verification as per Annex XX.

- For a terminating session entering the IBCF with signed Resource-Priority information, the IBCF, if configured through policies, invokes an AS for signature verification.

If border control concepts are to be applied in an IMS network, the IBCF acts as an entry point for this network (instead of the I‑CSCF), and also acts as an exit point for this network.

NOTE 3: In this case the IBCF and I‑CSCF may be co-located as a single physical node.

Based on local configuration, the IBCF may perform transit routing functions (see clause 5.19).

More detailed description of these functions is provided in Annex I.

>>>>NEXT CHANGE <<<<

### 4.16.3 Session setup principles

When establishment of UE initiated IP‑CAN bearer(s) for the media is required it is recommended to reserve IP‑CAN bearer(s) at the reception of the SDP answer. If the UE has been made aware of the operator policies with regards to allowed media for the multimedia telephony service, then the UE may reserve IP‑CAN bearer(s) at the sending of the SIP INVITE request. For multimedia telephony, the UE should only mark resource reservation as required for voice and video.

When there are no requirements for resource reservation or when required resources are available on the originating side, the P‑CSCF on the terminating side may send available session information to the PCRF/PCF at the reception of the SDP offer, as in such cases the UE can attempt resource reservation before sending the SDP answer.

If configured through policies, the telephony AS, or any other AS, may perform for originating requests attestation of the identity of the originating subscriber.

If configured through policies, the telephony AS, or any other AS, may perform for originating requests attestation of the RCD information or RCD URL of the originating subscriber as per Annex XX.

If configured through policies, the telephony AS, or any other AS, may perform for originating IMS priority sessions, assertion of authorization for the Resource-Priority information.

If configured through operator policies, the telephony AS may perform for diverted sessions attestation of the identity of the diverting subscriber initiating the diversion,

In addition, and if configured through policies, the telephony AS, or any other AS, may perform for terminating requests signature verifications, if one or more signatures is included.

In addition, and if configured through policies, the telephony AS, or any other AS, may perform signature verification of the RCD information or RCD URL of the originating subscriber for terminating requests, if a signature is included as per Annex XX.

NOTE: Only one network element performs attestation for an originating subscriber in the originating network.

>>>>NEXT CHANGE <<<<

Annex XX (normative):
Support for authorization, signing, and verification of third party user identity information in IMS

# XX.1 General

This annex describes support for authorization, signing, and verification of third party user identity information in IMS. A third party user in this context is a user belonging to a third party network which can be e.g., an Enterprise or private network.

The format of third party user identity information used in IMS follows the definitions in draft-ietf-sipcore-callinfo-rcd-12 [xx]. This allows to associate third party user identity information in IMS with Rich Call Data (RCD) information. An RCD server in the third party network or optionally the HSS may store third party user identity information. The IMS network can retrieve the third party user identity information from the RCD server during IMS session establishment and include this information in the outgoing SIP INVITE request.

Based on operator policies, third party user identity information can be signed by the originating IMS network and verified by the terminating IMS network. The process of signing and verifying third party user identity information follows draft-ietf-stir-passport-rcd-26 [yy]. The AS for signing and the AS for verification need to be able to sign and verify following information elements: RCD information and RCD URL.

# XX.2 Architecture and functions

## XX.2.1 Architecture

Figure XX.2.1-1 shows the overall system architecture to support authorization, authentication, and verification of third party user identity information in IMS.



Figure XX.2.1-1: System architecture to support authorization, authentication, and verification of third party user identity information in IMS

## XX.2.2 Functional entities

### XX.2.2.1 HSS

HSS stores either one RCD server address or one RCD URL per IMPU or wildcarded IMPU, or it may store a limited set of user specific properties (e.g., caller name, company name, job title, and Email address), whose format shall be compliant with draft-ietf-sipcore-callinfo-rcd-12 [xx], in the HSS repository data. Optionally, the RCD information, the RCD server address or the RCD URL may be provisioned per IMPU or wildcarded IMPU in the HSS repository data. HSS may store authorization information to allow use of third party user identity information.

NOTE 1: RCD information, RCD server address, RCD URL and RCD authorization information are stored as part of the IMS AS repository data (e.g., in the MMTel repository data).

NOTE 2: The provisioning of the RCD information, the RCD server address or the RCD URL via NEF is not supported in this release of the specification.

### XX.2.2.2 IMS AS

Originating IMS AS authorizes the calling party (IP-PBX or UE) to use third party user identity information based on the user profile retrieved from the HSS.

Originating IMS AS retrieves the RCD URL, RCD address or RCD information from the HSS. IMS AS can use the RCD server address or RCD URL to fetch the RCD information from the RCD server. Based on operator policies, IMS AS can invoke signing of the RCD information or the RCD URL.

NOTE: The interface between IMS AS and RCD server is out of scope of 3GPP.

Terminating IMS AS forwards the RCD URL or RCD information to the terminating UE after successful signature verification.

### XX.2.2.3 UE and IP-PBX

Based on agreements and trust relationship between the third party network and the IMS network, the third party network can provide RCD information or RCD URL in outgoing initial SIP INVITE requests. The IMS network, based on operator policy, may sign the provided RCD information or RCD URL.

The terminating UE may present third party user identity information of the calling-party to the called party, either received from RCD information in the SIP INVITE request or fetched from the RCD server based on the received RCD URL.

### XX.2.2.4 IBCF

The IBCF, based on operator policies, can invoke signing and verification of the RCD information or the RCD URL received in SIP signalling.

### XX.2.2.5 S-CSCF

For calls inside an IMS network, and based on operator policies, the S-CSCF can invoke signing and verification of the RCD information or the RCD URL received in SIP signalling.

# XX.3 Procedural description

Based on the user profile retrieved from HSS, IMS AS authorizes the usage of third party user identity information in a SIP INVITE request that originated from a UE or IP-PBX.

If originating UE or IP-PBX is authorized to use third party user identity information in the SIP INVITE request, and based on operator policies, S-CSCF, IMS AS or IBCF invoke signing of the provided third party user identity information with a signing AS.

The originating IMS AS can retrieve RCD server address, RCD URL, or RCD information from the HSS, based on the originating IMPU or wildcarded IMPU.

If the IMS AS has retrieved an RCD URL, the IMS AS, based on configuration, may retrieve the RCD information from the RCD server using the RCD URL. The IMS AS includes either the RCD URL or, if retrieved from the RCD server, the RCD information in the outgoing SIP INVITE request.

If the IMS AS has retrieved an RCD server address, the IMS AS provides the originating IMPU or wildcarded IMPU to the RCD server, to retrieve the RCD information. The IMS AS includes the retrieved RCD information in the outgoing SIP INVITE request.

Based on operator policies, the S-CSCF, IMS AS or IBCF in the originating IMS network will invoke signing of the RCD information or RCD URL included in the outgoing SIP INVITE request with a signing AS.

Based on operator policies, the S-CSCF, IMS AS or IBCF in the terminating IMS network will invoke signature verification of the RCD information or RCD URL included in the incoming SIP INVITE request with a verification AS.

The terminating UE may present third party user identity information of the calling-party to the called party, either from RCD information in SIP INVITE or from the RCD server based on the received RCD URL.

>>>>END OF CHANGES<<<<