NG.134 IMS Data Channel
Version 3.0
12 June 2024

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2024 GSM Association

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Contents

1 Introduction

Multimedia Telephony Service for IMS (MTSI) is a standardized IMS telephony service using the IMS capabilities to establish multimedia communications between terminals within and in-between operator networks. The terminals connect to the IMS using either a fixed access network, a WLAN access, or a 3GPP access network. The present document specifies a data channel extension to GSMA defined Voice and Video over IMS (VoIMS).

1.1 Overview

The IP Multimedia Subsystem (IMS) Profile for IMS data channel, documented in this Permanent Reference Document (PRD), defines a minimum mandatory set of features which are defined in 3GPP, IETF, GSMA specifications and W3C recommendations that a User Equipment (UE) and network are required to implement in order to guarantee interoperable, high quality end to end IMS-based communication services for IMS data channel over any IP access (e.g. WLAN access, 3GPP access) . The content of this document includes the following aspects:

1. Basic capabilities and features required for IMS data channel based services [Section 4].
2. Radio and packet core feature set [Section 5].
3. Common functionalities required across the protocol stack and subsystems [Section 3 and Section 4].
4. HTML, JavaScript and JavaScript Session Establishment Protocol [Section 6].

The main body of this PRD is applicable for the scenario where IMS based data channel services are deployed in 5G System (NG-RAN, 5GC, UE) or 4G System (E-UTRAN, EPC, UE) including interworking between 5G and 4G system.

NOTE: The data channel interworking between 4G/5G systems and 2G/3G is not supported.

To be fully compliant with this IMS Profile for data channel, the UEs and networks SHALL be compliant with all normative statements in the main body.

For 3GPP access, the present version of this PRD is restricted to profiling related to NG-RAN option SA NR (i.e. option 2) as defined in 3GPP TS 23.501 [8] and LTE connected to EPC as defined in 3GPP TS 23.401 [9].

In support of non-3GPP access to IMS Data Channel, references to GSMA PRD IR.92 [5] in this PRD are replaced by GSMA PRD IR.51 [75], and references to GSMA PRD NG.114 [7] are replaced by GSMA PRD NG.115 [74]. Additionally, clauses referred to in GSMA PRD IR.92 [5] and GSMA PRD NG.114 [7] are replaced by equivalent clauses in terms of clause title, rather than clause number, in GSMA PRD IR.51 [75] and GSMA PRD NG.115 [74] respectively.

1.2 Relationship to Existing Standards

1.2.1 3GPP and GSMA Specifications

This profile is based solely on the open and published 3GPP and GSMA specifications as listed in section 1.5. IMS features are based on 3GPP Release 16 unless otherwise stated including those features required to support interworking with EPS. When GSMA documents are referenced, the 3GPP release reference is specified in those GSMA documents.

1.2.2 IETF Specifications

This profile is based solely on the open and published IETF specifications as listed in section 1.5. The present version of this PRD is restricted to profiling IETF RFC 8831 [10], WebRTC based data channels.

1.2.3 W3C Recommendations

This profile is based on the open and published W3C recommendations as listed in section 1.5. The present version of this PRD is restricted to profiling the data channel related subset of WebRTC 1.0 [20] API required to implement data channel media type.

NOTE: The further work is required to document W3C WebRTC1.0 API gaps and to specify W3C WebRTC1.0 WebIDL API usage scenario by 3GPP TS 26.114[1] and the minimal IETF and W3C set of requirements to support IMS data channel.

1.3 Scope

This document defines a profile for IMS data channel services over IMS by listing a number of E-UTRAN/NG-RAN, EPC/5GC, IMS core and UE features and procedures that are considered essential to launch interoperable end to end services. The defined profile is compliant with and based on:

1. 3GPP/GSMA specifications related to voice, video and data channel services over IMS.
2. IETF specifications related to the WebRTC data channels and the general WebRTC protocol.
3. Ecma International ECMAScript standard supporting interoperability and the client site scripting for the W3C defined WebRTC 1.0 [20] data channel API component required to implement data channel media type.

The scope of this profile includes both the User to Network Interface (UNI) and Network to Network Interface (NNI),that is the interfaces between the User Equipment and the network as well as between the networks themselves. The NNI interface in this PRD is to be used in conjunction with GSMA PRD IR.95 [72]. The document also profiles DCMTSI client in terminal capabilities and the selected aspects of JavaScript API.

The profile does not limit, by any means, deploying other standardized features or optional features, in addition to those defined in this profile.

1.3.1 Out of Scope

The following features are not in scope of this PRD since either the existing 3GPP standards do not specify those specific aspects at all, or the relevant 3GPP specifications are ambiguous and force vendor specific implementations which might not be interoperable.

- The interworking between mobile and fixed networks
- The remote network's data channel capability discovery by UEs using the mechanisms defined in IETF RFC 3264 [13].
- Data channel capability discovery in roaming
- Data channel capability discovery in session and service continuity scenarios
- The data channel capability interactions with the IMS multimedia supplementary services
- Multiple data channel applications support, that is the scenario when both peers run at least two or more data channel applications at the same time and those applications require to establish and use their own dedicated application data channels concurrently.
- JavaScript API profile used to establish data channel connectivity layer.
- Consent and consent refresh to mitigate DoS attacks.
- Data channel support for European General Data Protection Regulation (GDPR)

1.4 Definition of Acronyms and Terms

1.4.1 Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
5GS	5G System
API	Application Programming Interface
APN	Access Point Name
Blob	Binary large object
CSS	Cascading Style Sheets
DCAR	Data Channel Application Repository
DCS	Data Channel Server
DNN	Data Network Name
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ECMA	European Computer Manufacturers Association
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FASG	Fraud and Security Group
GDPR	General Data Protection Regulation
HPMN	Home Public Mobile Network

Acronym	Description
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ICE	Interactive Connectivity Establishment
IETF	Internet Engineering Task Force
II-NNI	Inter-IMS Network to Network Interface
IMS	IP Multimedia Subsystem
IMS-AGW	IMS Access Gateway
IMS-ALG	IMS Application Level Gateway
IP	Internet Protocol
ISIM	IP Multimedia Services Identity Module
JSEP	Java Script Session Establishment Protocol
LTE	Long Term Evolution
MRFC	Multimedia Resource Function Control
MRFP	Multimedia Resource Function Processor
MTSI	Multimedia Telephony Service for IMS
N9HR	N9 Home Routing
NAT	Network Address translation
NEF	Network Exposure Function
NNI	Network to Network Interface
NR	New Radio
O/A	Offer/Answer
PRD	Permanent Reference Document
RA	Routing Area
S8HR	S8 Home Routing
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
STUN	Session Traversal Utilities for NAT
TA	Tracking Area
TCB	Trusted Computing Base
UI	User Interface
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card (UICC)
UNI	User to Network Interface
URL	Uniform Resource Locator
VoIMS	Voice and Video over IMS

Acronym	Description
VPMN	Visited Public Mobile Network
WebRTC	Web Real-Time Communication

1.4.2 Terms

Term	Description
Application Programming Interface	A specification of a set of calls and events, usually tied to a programming language or an abstract formal specification such as WebIDL.
Application Layer Protocol	Protocol used and controlled by the data channel application to communicate on the end to end basis with its peer entity. It is used to implement the application business logic and it may carry the application layer content, e.g. application multimedia content ,location information, graphical artefacts, and the application layer signalling, e.g. application flow control, application consent to use remote camera/gyroscope. The application layer protocol does not carry any speech, video or real-time textmedia content for IMS Multimedia Telephony Service (MMTel) as defined in 3GPP TS 22.173, i.e. when MMTel-AS is used to control session since GSMA PRD IR.92 , GSMA PRD IR.94 and GSMA PRD NG.114 native media types must be used for MMTel. For other IMS Multimedia Service types, e.g. AR/VR, no restrictions apply and the application layer protocol might carry any content.
Application Data Channel(s)	An IMS data channel(s) (based on WebRTC data channel defined in [10]) with the stream ID starting with 1000 and above used by the data channel application for the data transfer and the back end business logic execution.
Bootstrap Data Channel(s)	An IMS data channel(s) (based on WebRTC data channel as defined in [10]) with the stream IDs below 1000.
Data Channel API Run Time	UE components that implements the data channel JavaScript API, e.g. W3C WebRTC1.0 or other API used by the operator. The data channel API is consumed by the data channel JavaScript application when it needs to establish the WebRTC data channels [10] based connectivity layer. The initial release of GSMA PRDs profiling data channels is based on W3C WebRTC1.0 API usage to implement IMS data channels
Data Channel Application	HTML web page, JavaScript(s), image(s) and style sheet(s) used to implement 3GPP TS 26.114 [1] defined data channel front end business logic.
Data Channel Server	3GPP TS 26.114 [1] defined network function responsible for handling the data channel control and media plane
Data Channel SDP media description fragment	SDP lines as profiled in Table 4.2.1-1 and describing the application or bootstrap data channel(s) only. Those lines contain no speech media or video media information and must contain the mandatory and may contain the optional data channel media parameters.
DCMTSI client	A data channel capable MTSI client supporting data channel media as defined in clause 6.2.10 of 3GPP TS 26.114 [1].
DCMTSI client in terminal	A DCMTSI client that is implemented in a terminal or UE. The term "DCMTSI client in terminal" is used in this document when entities such as MRFP, MRFC or media gateways are excluded. 3GPP defined term “DCMTSI client in terminal” extends functionally “MTSI client in terminal” specified in 3GPP TS 26.114 [1] and the term definition is limited to UNI procedures and the protocol stack but without support for specific JavaScript API , asynchronous constructs , or the application life cycle handling (loading, initiation, destruction with the run time garbage collection). It is essentially 3GPP compliant SIP User Agent with the additional support for IETF RFC 8831 defined data channels. The user interface of DCMTSI service, that is the dialler, is not part of 3GPP TS 26.114 specification.

Term	Description
Dialler	The mobile device human to machine interface function allowing users to enter telephone numbers in E.164 format, have access to call status information and other notifications, i.e. the component enabling the interaction between the user and DCMTSI service. 3GPP does not specify the dialler component.
Error	ISO/IEC/ IEEE 24765 [71] term 3.1441 defined as human action that produces an incorrect result [IEEE 1044-2009 IEEE Standard Classification for Software Anomalies, difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. erroneous state of the system [ISO/IEC 15026-1:2013 Systems and software engineering — Systems and software assurance —Part 1: Concepts and vocabulary, 3.4.4] cf. failure, defect
Exception	ISO/IEC/ IEEE 24765 [71] term 3.1496 defined as event that causes suspension of normal program execution indication that an operation request was not performed successfully
External Server	An application server located outside the operator's administrative domain, providing service logic and/or media resource associated to a data channel application.
External Server with Data Channel Capability	An external server that has data channel capability.
External Server without Data Channel Capability	An external server that has no data channel capability.
Failure	ISO/IEC/ IEEE 24765 [71] term 3.1560 defined as termination of the ability of a system to perform a required function or its inability to perform within previously specified limits; an externally visible deviation from the system's specification
ICE Lite	The lite implementation of the Interactive Connectivity Establishment (ICE) specified in IETF RFC 8445 [62] /IETF RFC 5245 [70]
MTSI client	A function in a terminal or in a network entity (e.g. a MRFP) that supports MTSI.
MTSI client in terminal	An MTSI client that is implemented in a terminal or UE. The term "MTSI client in terminal" is used in this document when entities such as MRFP, MRFC or media gateways are excluded.
Real-Time Text	Real time text conversational service defined in section 5.2.3 of 3GPP TS 26.114 [1].
Root application	It's the data channel application list downloaded from the DCS (local network DCS or remote network DCS) by the DCMTSI client in terminal, and it's the root page which includes all data channel applications that the subscriber could select and use.
Voice and Video over IMS	GSMA PRD IR.65 [23] defined term denoting the support for GSMA PRD IR.92, GSMA PRD IR.94, GSMA PRD IR.51, GSMA PRD NG.114 and GSMA PRD NG.115.
WebIDL	Language used to define interfaces/data types in a way that is independent of the programming language and the operating system. It specifies only the syntax used to define the data types and interfaces.

1.5 Document Cross-References

Ref	Doc Number	Title
[1]	3GPP TS 26.114	IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction
[2]	3GPP TS 24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[3]	IETF RFC 4145	TCP-Based Media Transport in the Session Description Protocol
[4]	3GPP TS 29.165	Inter-IMS Network to Network Interface (NNI)
[5]	GSMA PRD IR.92	IMS Profile for Voice and SMS
[6]	GSMA PRD IR.94	IMS Profile for Conversational Video Service
[7]	GSMA PRD NG.114	IMS Profile for Voice, Video and Messaging over 5GS
[8]	3GPP TS 23.501	System architecture for the 5G System (5GS)
[9]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[10]	IETF RFC 8831	WebRTC Data Channels
[11]	IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
[12]	IETF RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words
[13]	IETF RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
[14]	IETF RFC 4960	Stream Control Transmission Protocol
[15]	IETF RFC 8261	Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets
[16]	IETF RFC 4566	SDP: Session Description Protocol
[17]	IETF RFC 8829	JavaScript Session Establishment Protocol (JSEP)
[18]	IETF RFC 8864	Negotiation Data Channels Using the Session Description Protocol (SDP)
[19]	IETF RFC 5688	A Session Initiation Protocol (SIP) Media Feature Tag for MIME Application Subtypes
[20]	W3C Recommendation WebRTC 1.0	WebRTC 1.0: Real-Time Communication Between Browsers https://www.w3.org/TR/webrtc/
[21]	IETF RFC 6809	Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)
[22]	GSMA PRD NG.113	5GS Roaming Guidelines
[23]	GSMA PRD IR.65	IMS Roaming, Interconnection and Interworking Guidelines
[24]	W3C Recommendation HTML5	HTML5 https://dev.w3.org/html5/spec-LC/
[25]	IETF RFC 8841	Session Description Protocol (SDP) Offer/Answer Procedures for Stream Control Transmission Protocol (SCTP) over Datagram Transport Layer Security (DTLS) Transport

Ref	Doc Number	Title
[26]	IETF RFC 8842	Session Description Protocol (SDP) Offer/Answer Considerations for Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS)
[27]	3GPP TS 23.002	Network architecture
[28]	IETF RFC 3261	SIP: Session Initiation Protocol
[29]	IETF RFC 7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
[30]	IETF RFC 7721	Security and Privacy Considerations for IPv6 Address Generation Mechanisms
[31]	IETF RFC 1808	Relative Uniform Resource Locators
[32]	3GPP TS 33.328	IP Multimedia Subsystem (IMS) media plane security
[33]	3GPP TS 23.334	IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures descriptions
[34]	3GPP TS 23.228	IP Multimedia Subsystem (IMS); Stage 2
[35]	IETF RFC 791	Internet Protocol
[36]	IETF RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
[37]	IETF RFC 2616	Hypertext Transfer Protocol -- HTTP/1.1
[38]	IETF RFC 1771	A Border Gateway Protocol 4 (BGP-4)
[39]	W3C Recommendation CSS2.1	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification https://www.w3.org/TR/2011/REC-CSS2-20110607/
[40]	ECMAScript 6	ECMAScript® 2015 Language Specification https://262.ecma-international.org/6.0/
[41]	void	
[42]	void	
[43]	IETF RFC 8827	WebRTC Security Architecture
[44]	IETF RFC 6347	Datagram Transport Layer Security Version 1.2
[45]	IETF RFC 5705	Keying Material Exporters for Transport Layer Security (TLS)
[46]	IETF RFC 5763	Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)
[47]	IETF RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams
[48]	IETF RFC 8835	Transports for WebRTC
[49]	void	
[50]	void	
[51]	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
[52]	GSMA PRD FS.38	SIP Network Security
[53]	IETF RFC 7675	Session Traversal Utilities for NAT (STUN) Usage for Consent Freshness
[54]	3GPP TS 22.011	Service accessibility

Ref	Doc Number	Title
[55]	GSMA PRD TS.32	Technical Adaptation of Devices through Late Customisation
[56]	W3C Media Capture and Streams	https://www.w3.org/TR/mediacapture-streams/
[57]	IETF RFC 2818	HTTP Over TLS
[58]	IETF RFC 6455	The WebSocket Protocol
[59]	IETF RFC 1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
[60]	IETF RFC 8839	Session Description Protocol (SDP) Offer/Answer Procedures for Interactive Connectivity Establishment (ICE)
[61]	IETF RFC 5340	OSPF for IPv6
[62]	IETF RFC 8445	Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal
[63]	3GPP TS 24.173	IMS multimedia telephony communication service and supplementary services; Stage 3
[64]	IETF RFC 3312	Integration of Resource Management and SIP
[65]	IETF RFC 4032	Update to the Session Initiation Protocol (SIP) Preconditions Framework
[66]	IETF RFC 8865	T.140 Real-Time Text Conversation over WebRTC Data Channels
[67]	Recommendation ITU-T T.140	Protocol for multimedia application text conversation
[68]	WHATWG HTML, 14 October 2022	HTML Living Standard
[69]	WHATWG FETCH, 14 October 2022	FETCH Living Standard
[70]	IETF RFC 5245	Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
[71]	ISO/IEC/IEEE 24765:2017	Systems and software engineering — Vocabulary
[72]	GSMA PRD IR.95	SIP-SDP Inter-IMS NNI Profile
[73]	3GPP TS 24.186	IMS Data Channel Applications ; Protocol Specifications
[74]	GSMA PRD NG.115	IMS Profile for Voice, Video, and Messaging over WLAN connected to 5GC.
[75]	GSMA PRD IR.51	IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access

1.6 Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2 IMS Data Channel Reference Architecture

2.1 Workflow for IMS Data Channel

The IMS data channel subsystem SHALL support the workflow defined in section 6.10.2.1 of 3GPP TS 26.114 [1] and shown in Figure 2.1-1. When a UE is registered in 5GC then it SHALL support GSMA PRD NG.114 [7] and when it is registered in EPC then it SHALL support GSMA PRD IR.92 [5] in addition to the provisions of this document.

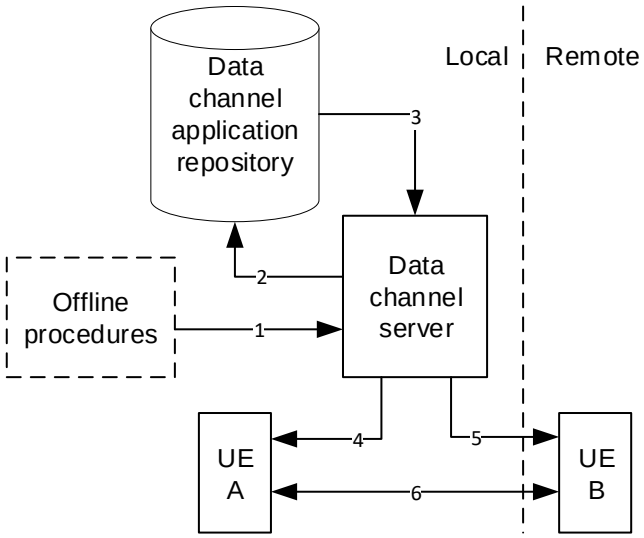

Figure 2.1-1: IMS Data Channel workflow defined in 3GPP TS 26.114 [1]

The IMS data channel implementation SHALL support the Data Channel Application Repository (DCAR) and the Data Channel Server (DCS) according to section 6.2.10.1 of 3GPP TS 26.114 [1]. The data channel content MAY transit through the Data Channel Server. When A-party and B-party belong to different operators' networks, the data channel content MAY pass across the Network to Network Interface (NNI).

2.1.1 Data Channel Protocol Stack

A DCMTSI client SHALL support the user plane protocol stack according to section 4.2 of 3GPP TS 26.114 [1] and depicted in Figure 2.1.1-1. For brevity, henceforth in accordance 3GPP TS 26.114 [1], an MTSI client supporting data channel will be denoted as a DCMTSI client or DCMTSI client in terminal.

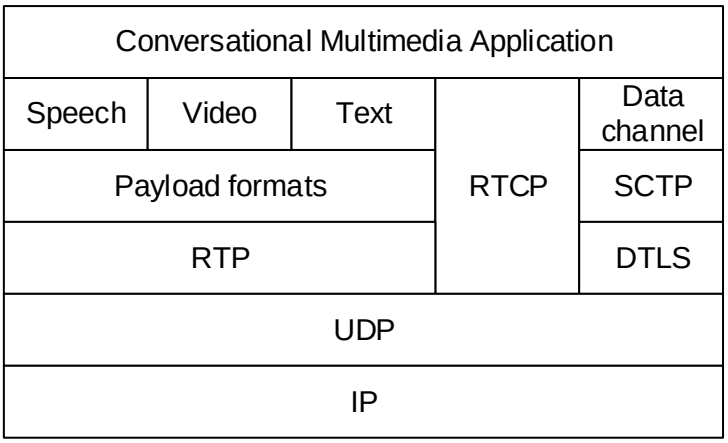

Figure 2.1.1-1: User plane protocol stack for a basic DCMTSI client defined in 3GPP TS 26.114 [1]

The data channels SHALL use SCTP (IETF RFC 4960 [14]) over DTLS (IETF RFC 8261 [15]) required by WebRTC data channels specification (IETF RFC 8831 [10]).

The DCMTSI client or DCMTSI client in terminal SHALL:

- use SDP as described in 3GPP TS 26.114 [1] for data channel media descriptions.
- apply IMS SIP signalling as specified in 3GPP TS 24.229 [2] and TS 26.114 [1].
- set-up and control of the individual data channel stream using IETF RFC 8831 [10], IETF RFC 8864 [18] and 3GPP TS 26.114 [1].

3 IMS Data Channel Feature Capabilities

The IMS data channel profile lists the mandatory and optional capabilities over the Gm, and II-NNI reference points in addition to capabilities described by GSMA PRD NG.114 [7] and GSMA PRD IR.92 [5] and required to support the WebRTC based data channels [10].

The IMS data channel feature is applicable only to a Native IMS Client as defined in section 1.4.2 of GSMA PRD NG.114 [7]. Downloadable IMS Clients are out of scope for this profile.

NOTE: GSMA PRD IR.92 [5] does not use the term “Native IMS Client” but the definition applies to LTE. The scope of this profile is limited only to 4G and 5G IMS clients that are provided as part of the handset implementation of a device carrying a UICC and accessing the credentials on that UICC.

3.1 SIP Registration

A DCMTSI client or DCMTSI client in terminal as defined in 3GPP TS 26.114 [1], SHALL support the IMS registration; details of IMS registration requirements are specified in section 2.2.1 of GSMA PRD IR.92 [5] for EPC and section 2.2.1.6 of NG.114 [7] for 5G Core. The registration options and IMS well-known APN/DNN SHALL be supported as specified in section 2.2.1.1 of GSMA PRD NG.114 [7] and section 2.2.1 of GSMA PRD IR.92 [5].

3.1.1 Data Channel Service Specific Aspects in Registration

According to section 2.2.1.8 of GSMA PRD NG.114 [7], section 2.2.1 of GSMA PRD IR.92 [5], section 6.2.10.1 of 3GPP TS 26.114 [1] and IETF RFC 5688 [19], a DCMTSI client or DCMTSI client in terminal SHALL include the "+sip.app-subtype" media feature tag with a value of "webrtc-datachannel".

3.1.2 SIP Re-registration

Section 2.2.1 of GSMA PRD IR.92 [5] and section 2.2.1.6 of GSMA PRD NG.114 [7] applies.

3.2 Capability Discovery

The IMS data channel discovery uses the existing signalling procedures defined in 3GPP TS 24.229 [2], IETF RFC 3264 [13] and IETF RFC 6809 [21].

3.2.1 UE Capability Discovery for IMS Data Channel

The network discovers its UE's data channel capability using the IMS REGISTER procedure defined in clause AC.8.1 of 3GPP Release 18 TS 23.228 [34], clause 5.4.1.2.2 of 3GPP Release 18 TS 24.229 [2], and clause 9.2.1 of 3GPP Release 18 TS 24.186 [73].

Home Network Discovery of the Data Channel Capability of its own UE

According to clause 5.1.1 of 3GPP TS 24.229 [2], the UE SHALL include in the Contact header of REGISTER request, a +sip.app-subtype media feature tag, as specified by RFC 5688 [19], with a value of "webrtc-datachannel" to indicate to the home network that it supports data channel capability.

According to clause 5.4.1.7 of 3GPP TS 24.229 [2], the IMS AS MAY discover the UE's data channel capability by inspecting whether a +sip.app-subtype media feature tag, which is transmitted in the Contact header field of user-initiated REGISTER request contained in the body of the third-party REGISTER request received from the S-CSCF, holds a value of "webrtc-datachannel".

3.2.2 UE Discovery for Network Support of IMS Data Channel

The UE discovers the home network's data channel capability using the mechanism defined in AC.8.1 of 3GPP Release 18 TS 23.228 [34], clause 5.4.1.2.2 of 3GPP Release 18 TS 24.229 [2], and clause 9.2.1 of 3GPP Release 18 TS 24.186 [73].

3.2.3 IMS Session Support for Data Channel

To identify how IMS data channel applications can be used in an IMS session, the SDP O/A negotiation is applied.When an originating SDP offer with data channel capability in the SDP media description is included in an IMS session to a target without data channel capability, the target SHALL set the port number in the data channel stream in the SDP answer to zero to reject the offered data channel stream, as specified in section 6 of IETF RFC 3264 [13]. In this case the IMS session does not support DC.

NOTE: What is displayed by the originating UE in the case of data channel media SDP O/A negotiation failure depends on UE's implementation.

3.3 IMS Data Channel at II-NNI

Based on inter-operator agreement, IMS data channel MAY be supported at II-NNI as specified in the section 33 of 3GPP TS 29.165 [4] and GSMA PRD IR.95 [72].

4 IMS Data Channel Media Type

SDP (IETF RFC 4566 [16]) SHALL be used to describe the bootstrap data channel and application data channel requirements. The data channel applications use the W3C WebRTC1.0 recommendation [20] to implement Data Channel API Run Time.

NOTE: Peer-to-peer connections described in Section 4 of WebRTC1.0 [20] and Peer-to-peer Data API described in Section 6 of WebRTC1.0 [20] represent the minimal API subset required to implement 3GPP TS 26.114 [1] defined data channels.

The data channel application creates the data channel SDP media description fragment by invoking Data Channel API Run Time primitive, e.g. using createOffer().

4.1 SDP Considerations for IMS Data Channel

Section 6.2.10 of 3GPP TS 26.114 [1] applies for both the UE and the entities in the IMS core network that terminate the IMS user plane.

The hosts IP address, UDP port and SCTP port SHALL be constant in one SDP media description. If there is a need to use the data channel with different IP addresses, different UDP ports, or different SCTP ports, then separate data channel SDP media descriptions SHALL be used as specified in section 6.2.10 of 3GPP TS 26.114 [1].

IETF RFC 8864 [18] specifies that the "dcmap-stream-id" parameter indicates the SCTP stream ID within the SCTP association used to form the data channel. Data channel stream IDs below 1000 SHALL be reserved for using the HTTP protocol, and are named as "bootstrap data channels" and described in section 6.2.10 of 3GPP TS 26.114 [1]. Data channel stream IDs starting from 1000 are used by the data channel application itself, henceforth denoted in this PRD as "application data channels". The data channel application uses W3C WebRTC1.0 [20] data channel API to establish the data channel application connectivity layer that transports the application layer protocol.

The data channel media description attribute "a=3gpp-qos-hint" carried in the SDP SHOULD be used if there is specific loss or latency requirements on the data channel, as specified in 3GPP TS 26.114 [1].

Application data channels specific parameters "max-retr" and "max-time" specified in IETF RFC 8864 [18] SHOULD be used to indicates the maximal number of times a message will be retransmitted and the time given in milliseconds after which the message will no longer be transmitted or retransmitted.

According to Table 6.2.10.1-2 of 3GPP TS 26.114 [1], bootstrap data channels MAY be established:

- between the originating UE and the originating network or between the originating UE and the terminating network; or

- between the terminating UE and the terminating network or between the terminating UE and the originating network.

According to Table 6.2.10.1-2 of 3GPP TS 26.114 [1], application data channels MAY be established:

- between the originating UE and the terminating UE;
- between the originating UE and the originating network or between the originating UE and the terminating network; or
- between the terminating UE and the terminating network or between the terminating UE and the originating network.

4.2 IMS Data Channel Establishment and Termination

This section specifies the requirements for support of bootstrap data channel and application data channel. The bootstrap data channel(s) and the application data channel(s) SHALL be established and transported over the IMS well-known APN/DNN as defined in GSMA PRD IR.88 [51].

4.2.1 SDP Media Description of IMS Data Channel

According to section 6.2.10 of 3GPP TS 26.114 [1], the following rules apply when a DCMTSI client is constructing IMS data channel SDP media descriptions:

- SDP media-level attributes "a=dcmap" SHALL be included in each data channel media negotiation and "a=dcsa" MAY be included. Both are specified in IETF RFC 8864 [18], and are used to negotiate data-channel-specific and subprotocol-specific parameters.
- As described in section 6.2.10.1 of 3GPP TS 26.114 [1], a data channel SDP media description SHALL NOT be placed before the first SDP speech media description. The receiving UE SHALL be tolerant to the order of SDP media descriptions.
- The bootstrap data channels and the application data channels SHOULD use different "m=" lines".

> NOTE: Multiple data channels could use the same transport end point and map to a single data channel SDP media description, each with a corresponding "a=dcmap" SDP attribute and stream IDs that are unique within that media description as described in section 6.2.10.1 of 3GPP TS 26.114 [1]. However it is not defined how this can be used in a standardized way.

- A bootstrap data channel SHALL be configured as ordered, reliable, with normal SCTP multiplexing priority, and using HTTP as subprotocol. Separate SDP media descriptions SHALL be used by a UE establishing bootstrap SCTP association with the local network and the remote network respectively.

- If there is a need to use data channels with either different transport IP addresses, different UDP ports, or different SCTP ports, separate data channel SDP media descriptions SHALL be used, as IP address, UDP port and SCTP port are all constant per SDP media description.
- The mandatory mapping between stream ID and bootstrap data channel of application content sources described in Table 6.2.10.1-2 of 3GPP TS 26.114 [1] SHALL be used. The stream ID values starting from 1000 are used for application data channel.
- As described in section 6.2.10.2 of 3GPP TS 26.114 [1], a data channel media description with specific QoS loss or latency requirements SHOULD use non-authoritative "a=3gpp-qos-hint" in the SDP offer.
- As described in section 5.8 of IETF RFC 8829 [17], the data channel media SDP parser implemented by UE SHALL reject any attribute it doesn't understand. The rejected attribute MAY led to data channel media negotiation failure. In that case DCMTSI client in terminal will not download any data channel applications, the data channel application will not be available. The application or bootstrap data channel SDP media negotiation failure SHALL NOT have any impact on establishment of GSMA PRD IR.92 [5], GSMA PRD IR.94 [6] or GSMA PRD NG.114 [7] media, i.e. the speech, video or real-time text media.
- As described in section 6.1.2, SDP media-level attribute "a=candidate" MAY be included in each data channel media negotiation and SDP session-level attribute "a=ice-lite" MAY be included.

NOTE 1: It is left up to UE implementation how the user is notified when the establishment of data channel fails.

NOTE 2: WebRTC1.0 SDP supports multiplexing of all media types to the same transport address, but this is not supported in IMS session, i.e. 3GPP TS 26.114 [1] and TS 24.229 [2]. It is recommended that the DCMTSI client in terminal does not use multiplexing.

Data channel SDP media description fragment SHALL be created for the bootstrap data channel and the application data channel.

Table 4.2.1-1 below specifies all the Data Channel SDP media description fragment attributes that MAY be used by the bootstrap data channel and the application data channel. The lines marked as mandatory in Table 4.2.1-1 represent the minimal required set of parameters needed by data channel session.

Parameter/ Attribute	Mandatory / Optional	Reference	Source of SDP line	Default Value
m=application	Mandatory	IETF RFC 4566 [16] 3GPP TS 26.114 [1]	DCMTSI client in terminal	N/A
c=IN	Optional		DCMTSI client in terminal and/or Core network	N/A
b=AS	Mandatory		Data channel application	N/A
a=max-message-size	Optional	IETF RFC 8841 [25]	DCMTSI client in terminal	64K

a=sctp-port	Mandatory		DCMTSI client in terminal	N/A
a=setup	Mandatory	IETF RFC [3] IETF RFC 8841 [25] IETF RFC 8842 [26]	DCMTSI client in terminal	'actpass' in the SDP offer and 'active' or 'passive' in the SDP answer
a=fingerprint	Mandatory	IETF RFC 4572	DCMTSI client in terminal	N/A
a=tls-id	Mandatory	IETF RFC 8842 [26]	DCMTSI client in terminal	N/A
a=dcmap	Mandatory	IETF RFC 8864 [18]	Value of parameter "subprotocol", "max-time", "max-retr", "priority" and "ordered" are provided by Data Channel application. Stream ID and value of parameter "label" are provided by DCMTSI client in terminal	N/A
a=dcsa	Optional		Data channel application	N/A
a=3gpp-qos-hint	Optional	3GPP TS 26.114 [1]	Data channel application	N/A
a=candidate	Optional	IETF RFC 8839 [60]	DCMTSI client in terminal	N/A
a=ice-lite	Optional	IETF RFC 8839 [60]	Core network	N/A

Table 4.2.1-1: IMS Data Channel SDP media description parameters and attributes

NOTE 3: If neither “a=ice-lite” nor “a=candidate” attributes are present for a data channel media description, it indicates that the SDP sender uses SDP “c=” and “m=” lines instead of “a=candidate” line to convey host address and port information.

4.2.2 Establishment and Termination of IMS Bootstrap Data Channel

The UE SHALL and the network MAY support the bootstrap data channel defined in section 6.2.10 of 3GPP TS 26.114 [1], so the network MAY provide the data channel application(s). The bootstrap data channel SHALL be supported by Mb media plane interface defined in 3GPP TS 23.002 [27] and where applicable by the Izi media plane interface defined in 3GPP TS 29.165 [4].

After the successful initial SDP Offer/Answer (O/A) negotiation defined in 3GPP TS 26.114 [1] of the bootstrap data channel media description, the DCMTSI client in terminal SHALL execute the following sequence of actions.

1. Initiate the DTLS association using the procedures described in section 3 of IETF RFC 8842 [26] and once successful

2. Initiate the SCTP association over DTLS association using the procedures described in section 5 of IETF RFC 4960 [14] and section 9 of IETF RFC 8841 [25] and
3. Send HTTP requests to the Data Channel Server to download the root application over this SCTP association using the stream identified by the corresponding "a=dcmap" line in the data channel SDP media description. Once the transport layer is available or enters the "established" state the bootstrap data channel(s) between the DCMTSI client in terminal and Data Channel Server in the local network and when required also with the Data Channel Server in the remote network are available. The stream identifier in the corresponding "a=dcmap" line MAY be set to values 0, 10, 100 or 110, as specified in Table 6.2.10.1-2 of 3GPP TS 26.114 [1].
4. Finally, for example, as described in NOTE 3 of section 6.2.10.1 of TS 26.114 [1], user selects any of the data channel applications from the menu. The selected application should be downloaded to the DCMTSI client in terminal in the local network and/or in the remote network but over different stream IDs, once the root application is successfully downloaded.

The failure to establish the transport layer DTLS / SCTP associations SHALL lead to the bootstrap data channel establishment failure. The bootstrap data channel media negotiation failure, or any other bootstrap data channel failures during the active session, e.g. data channel application download failure, SHALL NOT have any impact on the associated IMS audio/video/real-time text session.

NOTE 1: What the UE displays and whether user is informed when the bootstrap data channel fails depends on the UE's implementation.

When the network(s) and both UE support the bootstrap data channel then

1. There SHALL be one bootstrap SCTP association established between the DCMTSI client in terminal and the Data Channel Server of the local network provider in case the UE decides to consume content from the local network. There SHALL be a second bootstrap SCTP association established between the DCMTSI client in terminal and the data channel server of the remote network provider in case the UE decides to consume content from the remote network.

The bootstrap data channel SHOULD be available, i.e. the transport layer is available, for the duration of the IMS session. During the IMS session, any number of data channel applications MAY be downloaded through the established bootstrap data channels from the sources allowed by 3GPP TS 26.114 [1] but only one data channel application SHALL be active on each UE establishing application data channels towards its peer. When an IMS session associated with the bootstrap data channel is terminated normally or abnormally by DCMTSI client in terminal or network, as described in IETF RFC 3261 [28], all the SCTP associations and the DTLS associations between the DCMTSI client in terminal and the Data Channel Server will be released. It means that all the bootstrap data channels are terminated.

NOTE 2: In SDP O/A negotiation of the data channel media description, the SDP answerer could reject some bootstrap data channels by removing the corresponding "a=dcmap" lines in the generated SDP answer as described in section 6.5 of IETF RFC 8864 [18]. When it is required to reject all offered

data channels, that is the entire SCTP association, the port of the corresponding "m=application" line in SDP answer SHALL be set to 0 (zero), as described in section 6.2.10.3 of 3GPP TS 26.114 [1].

The bootstrap data channel failure during the call SHALL be handled following IETF RFC 7231 [29] or section 6.2.7.4.1 of 3GPP TS 26.114 [1] or IETF RFC 8841 [25] as follows:

- A bootstrap data channel failure due to a DCS error SHALL be handled following IETF RFC 7231 [29]. That is when HTTP request fails with 5XX error code e.g. HTTP 503, UE should invoke the recovery mechanism specific to the code received and if the mechanism fails then deem the HTTP failure permanent and the bootstrap data channel unavailable.
- A bootstrap data channel failure due to media bearer carrying the bootstrap data channel being dropped by the network due to insufficient resources should be handled as per clause 6.2.7.4.1 of 3GPP TS 26.114 [1].
- A bootstrap data channel failure due to SCTP associations closed without SDP signalling SHALL be handled as per clause 9.3 of IETF RFC 8841 [25].

4.2.3 Data Channel Application Retrieval and Synchronisation

The data channel application SHALL be retrieved by the DCMTSI client in terminal through a bootstrap data channel (see section 4.2.2) as soon as that bootstrap data channel is successfully opened, using the HTTP [37] protocol GET and the root (“/”) URL without any specified host part, as described by 3GPP TS 26.114 [1] section 6.2.10.1.

The bootstrap data channel is opened for issuing the first HTTP GET when SDP Offer/Answer [18][28], DTLS handshake, and SCTP association setup have all successfully concluded [10]. This applies for both originating and terminating DCMTSI clients in terminal.

NOTE 1: It is possible to provide per-subscriber customizable data channel applications through the nondescript root (“/”) HTTP URL starting point, if the Data Channel Server is aware of the call context, e.g., the SIP identity of a recognized subscriber being included as calling or called party.

NOTE 2: Since both originating and terminating DCMTSI clients in terminals starts the HTTP bootstrap process by issuing an HTTP GET towards the Data Channel Server, there’s no need for the Data Channel Server to start the bootstrap through HTTP PUSH or POST towards the DCMTSI clients in terminals.

NOTE 3: An HTTP request to receive the root data channel content is mandated to use the root URL. The data channel application can, as for any web page, consist of multiple components in potentially multiple hierarchical levels, such as, for example, images, style sheets, and JavaScripts. Such additional components are typically automatically fetched through multiple, separate HTTP transactions with other than root URLs over the bootstrap data channel, even without user interaction such as actively clicking on document links; see default fetching of images and other HTML document resources in [68][69].

NOTE 4: User interaction with the data channel application JavaScript logic and HTML content can, as for any web page, trigger further HTTP transactions with other than root URLs over the bootstrap data channel with, potentially, corresponding updates to the data channel application and logic in the DCMTSI client in terminal.

As described by Table 6.2.10.1-2 and Figure 6.2.10.1-3 in 3GPP TS 26.114 [1] section 6.2.10.1, a data channel application retrieved from a Data Channel Server by a local user through a bootstrap channel with stream ID 10, SHALL correspond to the application retrieved from the same Data Channel Server by a peer user in the same call through a separate bootstrap channel with stream ID 110.

NOTE 5: The Data Channel Server has access to all required IMS call context information to ensure the correlation of data channel applications that it sends through its managed bootstrap channels. Therefore, DCS ensures that both peers in a call have matching data channel applications. One example of such corresponding pair of bootstrap channels as seen from a single Data Channel Server is stream ID 10 to the local user and stream ID 110 to the peer user, as described by 3GPP TS 26.114 [1] section 6.2.10.1.

In case a subscriber has multiple data channel applications available in the Data Channel Server, the root application returned by the Data Channel Server to the DCMTSI client in terminal SHOULD include a possibility to choose among the available data channel applications, e.g., some type of menu functionality.

NOTE 6: 3GPP TS 26.114 [1] section 6.2.10.1 does not mandatorily specify how to design or perform such data channel application choice but suggests that the Data Channel Server provides the functionality through bootstrap channel stream ID 0, which is then used to decide which data channel application the Data Channel Server provides through bootstrap channel stream ID 10.

Since it is essential that both peers in a call that intend to use an application data channel to exchange end-to-end data (see section 4.2.4) use corresponding applications in both ends, at most one peer SHALL be given opportunity to choose which data channel application to use in any given pair of corresponding bootstrap data channels from a single Data Channel Server. Corresponding data channel applications based on that single choice SHALL be returned by the Data Channel Server to both peers in the call.

NOTE 7: 3GPP SA2 Rel-18 work may impact the existing 3GPP TS 26.114 [1] solution and may require changes both to TS 26.114 in 3GPP SA4, and to future versions of this document.

4.2.4 Establishment and Termination of IMS Application Data Channel

1. Section 6.2.10.2 of 3GPP 26.114 [1] mandates that once the UE retrieves a data channel application from the network repository, and the user invokes the application service logic that requires an application data channel, then the media re-negotiation will be performed to establish the required application data channel(s). The media re-negotiation for application data channel establishment subsequently follows clause

6.2.10.2 in 3GPP TS 26.114 [1] and SHALL be triggered only upon the invocation of JavaScript API request to create the application data channel(s).

2. Once the SDP O/A re-negotiation succeeds, the DCMTSI client in terminal SHALL establish the transport layer connectivity by executing the following steps:
    1.Initiate the DTLS association according to section 3 of IETF RFC 8842 [26] and once successful, then
    2.Initiate the SCTP association over DTLS association according to section 5 of IETF RFC 4960 [14] and section 9 of IETF RFC 8841 [25].

NOTE 1: The interface between Data Channel API Run Time, e.g. JSEP, and DCMTSI service, i.e. SIP/SDP stack, is UE implementation specific and is local in a sense that the way each UE implement this function does not impact bits on the wire or application.

Once the transport layer is established successfully between the DCMTSI client in terminal and its peer, the application layer protocol can be transferred over the application data channel.

The failure to establish DTLS association or SCTP association SHALL lead to the application data channel establishment failure, and the JavaScript exception SHALL be raised to the data channel application. The application SHALL then determine its most appropriate course of action.

The application data channel media negotiation failure, or any other application data channel failure during the active session, e.g. failure to send traffic over an application data channel or data channel bearer drop by the network, SHALL NOT have any impact on the associated IMS audio/video session.

NOTE 2: What the UI displays and whether user is informed when the application data channel fails depends on the UE's implementation.

When an IMS session associated with application data channel is terminated normally or abnormally, as according to procedures described in IETF RFC 3261 [28], then upon session release all SDP "m=" lines should be released including all data channel media. This will result in the closure of SCTP/DTLS associations. It means that the application data channels are terminated.

4.2.5 Exception Handling for IMS Data Channel

IMS data channel failures might be recoverable (e.g. subsequent attempt is made to use the same ID for the newly established data channel) or non-recoverable (e.g. JavaScript heap out-of-memory, network failure).

Following principles apply for handling the IMS data channel events:

- As specified in clause 9.4 of 3GPP TS 24.186 [73], the failure to establish IMS data channel or the failure to maintain the established IMS data channel SHALL not impact the other media types associated with the same IMS session (e.g. speech, video, etc.).
- A DCMTSI client can request additional data channel media within the same SIP session by using SIP Re-INVITE, after other media (e.g. speech, video, etc.) has

been established. If the establishment of the additional data channel media fails, then neither the existing data channel media nor the other media types associated with the same IMS session SHALL be impacted.

- As specified in section 6.2.7.4.1 of 3GPP TS 26.114 [1], if a data media GBR bearer that was set up with 3gpp-qos-hint information is dropped by the network due to insufficient resources, an attempt to re-establish the bearer SHOULD be made by the DCMTSI client in terminal through a re-offer in an Re-INVITE with less demanding QoS values included in the 3gpp-qos-hint and/or bandwidth attributes.
- A DCMTSI client SHOULD monitor the status of SCTP path for data channel media by using SCTP Heartbeat mechanism which is specified in IETF RFC 4960 [14], once the data channel has been established successfully established. Upon detection of SCTP association failure, the SCTP layer of the DCMTSI client SHOULD report the failure to the upper layer (e.g. SIP layer, data channel application) of the DCMTSI client, as specified in section 8 of IETF RFC 4960 [14]. The DCMTSI client thus determines corresponding actions, e.g. either to re-establish the DTLS/SCTP association by SIP Re-INVITE or terminate the IMS data channel session.
- When data channel failure occurs the JavaScript run-time environment SHALL raise the exception so the data channel application can process the event and take the required action, e.g. recovery or application closure.
- In the case of recoverable failure, the data channel application SHOULD try to recover by invoking the exception handler, i.e. JavaScript try/catch block and in the case of non-recoverable failure the data channel application SHALL terminate and inform the user about the error.

NOTE 1: An error is an event that is visible to the user while the exception is an event that visible to the program and handled by the respective exception handler. How errors are presented to the user is outside the scope of current version of the document.

4.3 Single and Multiple IMS Data Channels per SIP Session

4.3.1 Number of IMS Data Channels per SIP Session

As described in section 6.2.10.1 of 3GPP TS 26.114 [1]:

- Each DCMTSI client in terminal SHOULD send bootstrap Data Channel establishment request for both local and remote network. The root application will be retrieved from local or remote DCSs respectively. Those root applications SHOULD be opened in a separate tab, or some corresponding user interface construct.
- UE can terminate an application data channel either on another UE or on a network element supporting application data channel termination, i.e. UE-to-UE or UE-to-network.
- Multiple application data channels MAY be opened by a single data channel application, which means that one application may need to use multiple application data channels and these data channels can be included in one “m=” line when QoS parameters of the “m=” line satisfy their QoS requirement.

4.3.2 Stream ID Numbering of Multiple IMS Data Channels

According to section 6.2.10.1 of 3GPP TS 26.114 [1], data channel stream ID numbering SHALL comply with the following rules:

- Stream ID 0-999 SHALL be used for bootstrap data channels.

NOTE 1: When both the originating network and the terminating network support IMS data channel capability, two different bootstrap data channels with the same stream ID 100 in an IMS session will be established. That is, each network establishes a bootstrap data channel with its remote UE, whose stream ID is 100. As a result, the DCS in either network is not able to distinguish the “m=” line of SDP offer for bootstrap data channel it requires to process with. There is no standardized mechanism to handle this, and as such it needs to be addressed by proprietary means.

- Stream IDs starting from 1000 SHALL be used for application data channels.

4.3.3 Bandwidth of Multiple IMS Data Channels

According to section 6.2.7.2 of 3GPP TS 26.114 [1], the "b=AS" bandwidth modifier is used at media level, i.e. m=line, to describe the maximum bandwidth for the receiving direction of offerer, and the IP/UDP/DTLS/SCTP overhead is included in the bandwidth value for data channel media, which may contain both bootstrap data channel(s) and application data channel(s). The bandwidth value is an integer and the unit is kbps.

As described in section 6.2.10.1 of 3GPP TS 26.114 [1], the aggregate of all defined data channels in an SDP media description, including the bootstrap data channel(s) and the application data channel(s), SHALL be keep within the set bandwidth limit.

As described in section 6.2.7.2 of 3GPP TS 26.114 [1], once the DCMTSI client in terminal detects that the negotiated downlink QoS Maximum Bit Rate (MBR) value differs from the b=AS bandwidth modifier value in the sent SDP, no matter whether at session setup or at session re-negotiation, DCMTSI client in terminal SHOULD try to align to the downlink MBR(s) allocated for the bearer(s) in a subsequent SDP offer-answer.

4.3.4 QoS of Multiple IMS Data Channels

According to section 6.2.7.4.1 of 3GPP TS 26.114 [1], when multiple application data channels have different QoS requirements expressed by "a=3gpp-qos-hint" line, then each should have the dedicated SDP media description.

4.4 Standalone IMS Data Channels

Standalone IMS data channels, i.e. IMS data channels without accompanying audio/video media, are not supported in this revision of this document.

5 Radio and Packet Core Feature Set for IMS Data Channel

5.1 General

The radio and packet core features described in section 4 of GSMA PRD IR.92 [5] and section 4 of GSMA PRD NG.114 [7] SHALL be applied.

5.2 QoS Flow Management for IMS Data Channel

For E-UTRAN/EPC, section 4 of GSMA PRD IR.92 [5] SHALL be applied for the PDN connection and EPS bearer management. For NG-RAN/5GC, section 4 of GSMA PRD NG.114 [7] SHALL be applied for PDU session and QoS flow management.

It is recommended that the network supports the mapping between various media types and different QCI/5QI that are described in Table E.0 of 3GPP TS26.114 [1] section E.1. However different mappings are also allowed based on the operator policies.

5.3 Session and Service Continuity

For E-UTRAN/EPC, PDN connection service continuity SHALL be supported, as specified in section 4.3 of GSMA PRD IR.92 [5]. For NR-RAN/5GC, PDU session service continuity SHALL be supported, as specified in section 4.5, 4.6 and 4.8 of GSMA PRD NG.114 [7]

5.4 P-CSCF Discovery

The UE and network (i.e. EPC, or 5GC) SHALL support the P-CSCF discovery procedure specified in section 4.4 of GSMA PRD IR.92 [5], or section 4.7 of GSMA PRD NG.114 [7].

NOTE: It is recommended to configure all P-CSCFs in the PLMN with same capability as specified in 3GPP TS 26.114 [1] and 3GPP TS 24.229 [2] for supporting IMS Data Channel.

6 Common Functionalities for IMS Data Channel

6.1 Common HTML, JavaScript and CSS Functionalities

JavaScript Session Establishment Protocol for Data Channels

DCMTSI client in terminal implementing the Data Channel API Run Time for IMS data channels defined in 3GPP TS 26.114 [1] SHALL follow IETF RFC 8829 [17] only to the extend required by IETF RFC 8831 [10]. It is not necessary for UE to comply with the other aspects of IETF RFC 8829. JSEP baseline is used since otherwise without globally standardized API framework a data channel application will not work between different UEs and/or different networks.

NOTE 1: A behavioural and WebIDL specification constitutes full API definition and 3GPP 26.114 [1] has not provided one for DCMTSI client in terminal.

The JSEP implements only the data channel connectivity layer described in section 6.2.10 of 3GPP TS 26.114 [1] and SHALL support the methods for creating the application data channels, e.g. createDataChannel and the event handlers to notify the remote peer application once the data channel is created, e.g. ondatachannel. Therefore, the JSEP run

time environment SHALL support the required JavaScript asynchronous concepts, e.g. Promise, Async/Await, so the code will not be blocking in single threaded environment.

NOTE 2: The data channel application business logic is outside the scope of this document and the programmer can use any API or JavaScript constructs with the exceptions of those that are prohibited by this document.

3GPP TS 26.114 [1] compliant Data Channel API Run Time implementation SHALL generate only the required data channel SDP media description fragment and no other media descriptions. It SHOULD generate a blob of SDP containing the supported data channel configurations for the session and SDP blob should in general be transparent to the application programmer with the exception of those application parameters that are explicitly required to be set by 3GPP TS 26.114 [1] and characterize the data channel application business requirements.

DCMTSI client in terminal implementation of Data Channel API Run Time SHOULD construct the 3GPP TS 26.114 [1] compliant and complete SDP (i.e. combine the initial offer GSMA PRD IR.92 [5] or GSMA PRD NG.114 [7] SDP fragment and the subsequent data channel SDP fragment) according to the rules described by IETF RFC 3264 [13] and use its SIP User Agent, i.e. DCMTSI service, to invoke and execute the required Offer/Answer exchange.

NOTE 3: How JSEP implementation interacts with the browser and/or the dialler is left open for the OEM manufacturers to decide. Any function that does not impact 3GPP TS 26.114 [1] data channel on-the-wire UNI protocol or JavaScript API can be implemented in a vendor specific way since it does not impact the interoperability between systems nor the application code. That is those functions represent the local system support function with only the local scope.

In all cases, DCMTSI client in terminal SHALL ensure that correct SDP is constructed and sent. And Data Channel API Run Time implementation SHALL ensure that only syntactically correct SDP fragment are made available to DCMTSI client in terminal. The JavaScript objects SHALL have their life-cycle tied to the context that created them, that is the VoIMS session. It means that JavaScript objects can be safely garbage collected once the VoIMS sessions terminates.

NOTE 4: The current version of this document assumes that the application is only available with VoIMS connection. Future versions of this document might relax this requirement and allow the usage of HTML5 Application Cache, i.e. data channel application caching, and accessibility without VoIMS connection as specified in section 5.6.2 of HTML5 [24]. This scenario is left for future analysis.

The non-functional behaviour of Data Channel API Run Time and HTML, i.e. JavaScript garbage collection, performance, security, asynchronous processing, etc, SHALL follow IETF RFC 8827 [43], W3C and ECMAScript recommendations.

NOTE 5: The future GSMA PRD will describe in detail the API specification, i.e. provide functional and non-functional behavioural specification, provide WebIDL description, and give non-normative code examples.

ICE/STUN/TURN

UE supporting Full ICE SHALL use host candidate address only. Network SHALL support ICE Lite and MAY support Full ICE [62][60] for IMS data channel defined in 3GPP TS 26.114 [1] over UNI. The UE and the network MAY send its host candidate address as “a=candidate” line in SDP Offer/Answer, in addition to address and port information in “c=” and “m=” lines. When “a=candidate” lines are present, the information MUST match corresponding “c=” and “m=” lines. When no “a=candidate” lines are present, the UE and the network identify the peer host candidate address and port by checking “c=” and “m=” lines of SDP Offer/Answer.

HTML/JavaScript/CSS

According to section 6.2.10.1 of 3GPP TS 26.114 [1], the data channel application SHALL consist of Hyper Text Markup Language (HTML) web pages including JavaScript(s) and MAY include image(s) and Cascading Style Sheet(s) (CSS) transferred through the bootstrap data channels at the User-Network Interface (UNI). In addition, when

- the user is roaming, then the data channel content is delivered across the S8HR or N9HR interface, and/or when.
- the inter-PLMN data channel capable call takes place then the data channel content is delivered across Inter-IMS Network to Network Interface (II-NNI).

The W3C Hypertext Markup Language Revision 5 (HTML5) [24] and W3C CSS Level 2 Revision 1 (CSS 2.1) [39] SHOULD be used for the data channel application content, layout and style.

The JavaScript specification ECMAScript 6 [40], also known as ECMAScript 2015, SHOULD be used for implementing data channel application interactive content.

According to section 6.2.10.1 of 3GPP TS 26.114 [1], the bootstrap data channel SHALL use HTTP as subprotocol (not encapsulating HTTP in TCP) to transfer data channel application content and the HTTP version is HTTP/1.1 as specified in IETF RFC 2616 [37].

3GPP has no restriction on the application layer protocol, that is the data channel application MAY use any protocol to control its application peer entity but it SHALL use Data Channel API Run Time to establish and control the connectivity layer with its peer. The application layer protocol content and the application layer specific signalling across UNI and NNI is transferred using the services of DCMTSI client in terminal providing the data channel connectivity layer controlled by the application JavaScript logic.

NOTE: For GSMA PRD IR.92 [5], GSMA PRD IR.94 [6] and GSMA PRD NG.114 [7] media types DCMTSI client in terminal interacts and might be controlled by the dialler component of UE.

Common IMS Functionalities

6.1.2 IMS Data Channel Security Features

In compliance with GSMA guidelines which recommend addressing the security concerns of any new or the existing technology this section profiles the key IMS data channel security domains including the UE security, Data Channel API Run Time, and the network security including the "mediasec" header field required for e2ae mode. It also refers to the optional denial of service mitigation method using consent process and the relevant mandatory regional regulatory aspect.

The security profile is required to guarantee the secure IMS data channel interworking between data channel applications.

UE Security

The DCMTSI client in terminal is the IMS data channel application Trusted Computing Base (TCB), that is the set of software and hardware components on which the security of IMS data channel application depends. All data channel application related security guarantees committed to the user, e.g. IETF RFC 8827 [43], are delivered by Data Channel API Run Time e.g. W3C WebRTC1.0 implementation instance. Data Channel API Run Time environment SHOULD be trusted and the user SHALL be able to execute any JavaScript application script provided by Data Channel Server (DCS) or any other server, including those that have the malicious intent. It means that the Data Channel API Run Time SHALL implement a sandbox isolating user from the script e.g. as it is done in general for web apps.

NOTE 1: It is not possible to stop the data channel application once it is running. The Data Channel Server or other server inserted in the API flow controls both the communication channel and the running JavaScript. Therefore, the rendered User Interface (UI) content will be under the control of that server chain.

The IMS session context information provided by the dialler and the IMS home domain name, a private and public identity, a secret key used for authentication / registration that are provided by UICC/ISIM SHALL be trusted.

DCMTSI client in terminal SHALL support the origination and termination of the encrypted bootstrap data channels and the origination and termination of the encrypted application data channels traffic over 3GPP TS 23.002 [27] defined Mb interface using DTLS (i.e. IETF RFC 6347 [44]) and provide the confidentiality, source authentication and integrity-protection as defined in IETF RFC 8831 [10].

IMS Data Channel Security

IMS data channel traffic is encrypted by DCMTSI client in terminal.

DCMTSI client in terminal SHALL use the self-signed certificates transported in the media plane for securing and authenticating DTLS associations. The “a=fingerprint” SDP attribute identifying the key that will be presented during the DTLS handshake SHALL be used, as per IETF RFC 5763 [46] to bind the signalling and the media plane.

NOTE: The security guarantees offered by the DTLS connection depend on the verification of the self-signed DTLS certificates using the fingerprints. Since the Identity Provider is not used the binding of the user identity and the fingerprint will not be computed and no such information will be present in the SDP offers and answers.

IETF RFC 8827 [43] mandates that WebRTC1.0 [20] implementations SHALL NOT offer or select if offered the SDP security descriptions specified in IETF RFC 4568 [47]. Therefore, IMS network will not see those originate from DCMTSI client in terminal implementing data channels based on W3C WebRTC1.0 [20].

IETF RFC 8827 [43] SHALL apply only with respect to the IETF defined WebRTC data channels on-the-wire transport protocols specified in IETF RFC 8835 [48] and used over IMS UNI and needed by 3GPP TS 26.114 [1] . It is not necessary to comply to other aspects e.g. third party Identity Providers, etc. Either DCMTSI client in terminal or network MAY chose to fail to implement other than data channel on-the-wire related provisions in IETF RFC 8827[43] and IETF RFC 8835 [48].

Network Security

Section 4.2 of 3GPP TS 33.328 [32] provisions for the end to access edge encryption (e2ae) and the end to end encryption (e2ee) of the IMS user plane. Both are optional and by default VoIMS media plane is unencrypted as per section 2.14.1 in GSMA PRD IR.65 [23] while IMS data channel is encrypted by default. Since DCMTSI client in terminal implementation will encrypt data channel traffic presented to the IMS network, then the network SHOULD support end to access edge encryption (e2ae) of the IMS data channels.

NOTE 1: The network MAY support the end to end encryption (e2ee) of IMS data channels when the network supports it and it is allowed by the local regulation. The future releases of this document will clarify the usage of e2e security mode.

When e2ae is used then only Mb interface defined by 3GPP TS 23.002 [27] is encrypted and when e2ee is used then all data channel media plane interfaces are encrypted: Mb interface and, where applicable, the Izi interface as defined in 3GPP TS 29.165 [4].

In all cases regardless of whether IMS data channel is supported or not, the IMS security methods defined in 3GPP TS 33.203 [49], 3GPP TS 33.210 [50] and IMS media plane security for RTP and MSRP based media specified in 3GPP TS 33.328 [32] apply and MAY be used as required by the HPMN or VPMN. 3GPP TS 33.203 [49] and 3GPP TS 33.210 [50] defined authorisation and authentication mechanisms SHALL be supported over UNI.

The "mediasec" header field parameter referenced in section 7.2A.7 of 3GPP TS 24.229 [2] SHALL be used with e2ae mode and DCMTSI client in terminal enables e2ae media security by sending "*3ge2ae: requested*" in the SDP to IMS-AGW that responds with "3ge2ae: applied" when the request is successfully applied. The encrypted IMS data channel stream is terminated locally by IMS-AGW and IMS-AGW MAY act as DTLS client or DTLS server as described in section 5.20.2 of 3GPP TS 23.334 [33]. DCMTSI client in terminal SHALL insert *"*3ge2ae: requested*"* into SDP sent to the network. According to section 7.5.2.2 of TS

24.229 [2], end-to-access-edge media security indicator "3ge2ae: requested" is encoded as a media-level SDP attribute and can be applied to the data channel as shown in figure N.3.2-1 of TS 33.328 [32].

NOTE 2: IMS registration does not need to carry 3ge2ae indication in SIP registration since Annex N of 3GPP TS 33.328 [32] suggests that when P-CSCF is aware that the terminating UE is DCMTSI client in terminal supporting WebRTC then it can automatically apply e2ae security for terminating calls.

DTLS (i.e. IETF RFC 6347 [44]) encryption and the integrity service MAY be applied at II-NNI interface specified in the section 33 of 3GPP TS 29.165 [4].

Secure Mb interface defined in 3GPP TS 23.002 [27] interworking with an external 3rd party web content server over IMS APN (i.e. section 6.3.2 of GSMA PRD IR.88 [51]) and using the required mechanisms (e.g. URL resolution, security screening or redirection) SHOULD be supported.

NOTE 3: None of GSMA PRD profiles media plane security i.e. GSMA PRD IR.92 [5], GSMA PRD NG.114 [7] or GSMA PRD FS.38 [52]. The text above does clarify those aspects.

Denial of Service

NOTE: Denial of Service (DoS) attacks are notoriously difficult to prevent and present the threat to availability. Since an arbitrary JavaScript code can be executed it might impact the network or UE availability. WebRTC1.0 supports the “maxChannels” parameters that limits the maximum number of RTCDataChannel's that can be used simultaneously but the “b=AS” line is not enforced therefore enabling potentially unauthorized bandwidth consumption. The DoS protection and data channel consent to send/receive needs to be addressed in a future release of the document including the impact on the battery life-cycle.

Regulatory

NOTE: The data channels are subject to the Lawful Interception requirements based on the national regulations. The technical solution will be profiled in this document once 3GPP SA3 work is completed.

6.1.2 Roaming Considerations

The UE and the network supporting IMS data channel per clause 6.2.10 of 3GPP TS 26.114 [1] SHALL comply with GSMA PRD IR.65 [23] and support S8 Home Routing (S8HR) and N9 Home Routing (N9HR) roaming architectures for Evolved Packet System (EPS) and 5G System (5GS). For more information on the IMS data channel roaming see GSMA PRD NG.113 [22] and IR.65 [23].

6.1.3 3GPP PS Data Off

NOTE: This section should be validated for alignment with 3GPP R18 SA2 once released.

3GPP PS Data Off service is defined in section 1.2.1 of 3GPP TS 22.011 [54] and the IMS data channel SHOULD be defined as 3GPP PS Data Off based on operator policies.

Therefore, its treatment follows that of the MMTEL video and the IMS settings in Table 6 of GSMA PRD TS.32 [55] are interpreted as follows:

- VxLTE1.51=0 indicates that that the IMS data channel is 3GPP PS Data Off and VxLTE1.51=1 indicates that IMS data channel is 3GPP PS Data Off Exempt.
- GSMA TSG PRD TS.32 [55] defines the default value VxLTE1.51=0 ,i.e. Not Exempt, and that should be the default IMS data channel behaviour.

PS Data Off applies to both the bootstrap data channels and the application data channels, so when activated no packet SHALL be sent for either of those channels.

All other 3GPP Data Off provisions SHALL follow GSMA PRD NG.114 [7], GSMA PRD IR.92 [5] and GSMA PRD IR.94 [6] , e.g. with respect to reporting its status change, etc.

6.1.4 Other Considerations for IMS Data Channel

SIP Forking

When IMS data channel is initiated simultaneously with the IMS voice or/and IMS video media, the UE SHALL include an Accept-Contact header field containing the "sip.app-subtype" media feature tag with a value of "webrtc-datachannel" to express the multimedia telephony participants data channel preferences as specified in section 5.2 of 3GPP Release 17 TS 24.173 [63] . The network and UE SHALL follow section 2.2.7 of GSMA NG.114 [7] or section 2.2.5 of GSMA PRD IR.92 [5] when processing respectively EPC or 5GC forked requests during the session establishment.

NOTE: Forking does not apply for the application data channel establishment subsequent to successful IMS voice/video setup, i.e. SIP re-INVITE as specified in section 6.2.10.2 of 3GPP TS 26.114 [1].

SIP Preconditions

SIP preconditions mechanism, as specified in IETF RFC 3312 [64] and IETF RFC 4032 [65] SHALL be disabled for the IMS data channel.

NOTE: SIP preconditions may be enabled for IMS data channels subject to further 3GPP SA2 conclusions once the relevant 3GPP studies are completed.

IMS Data Channel Early Media

The early media mechanism, as specified in section 2.2.7 of GSMA PRD IR.92 [5], section 2.2.3 of GSMA PRD IR.94 [6] and section 2.2.6 of GSMA PRD NG.114 [7], MAY be applied to IMS data channel when IMS data channel is initiated together with IMS voice or/and IMS video media. That is, IMS data channel media streams MAY be exchanged before an IMS session is accepted by the called party.

Section 2.2.4 of GSMA PRD NG.114 [7] or section 2.2.4 of IR.92 [5] applies accordingly for 5GC and EPC.

IP Versions Interworking

Section 4.9 of GSMA PRD NG.114 [7] or section 5.1 of GSMA PRD IR.92 [5] SHALL apply accordingly for 5GC and EPC.

Annex A (Informative): SDP Examples

A.1 Bootstrap Data Channel Establishment - Initial Offer SDP Example

The VoIMS session follows the initial offer media negotiation procedures described in 3GPP TS 24.229 [2]. VoIMS session with the data channel adds the data media, also referred as SDP data media fragment in this document, and executes the additional data channel negotiation procedures described in section 6.2.10 of 3GPP TS 26.114 [1].

The basic SDP offer and answer exchange for establishing bootstrap data channel for UE A and UE B belonging to the different networks is annotated below. Each network has its own Data Channel Server, e.g. DCS-A and DCS-B.

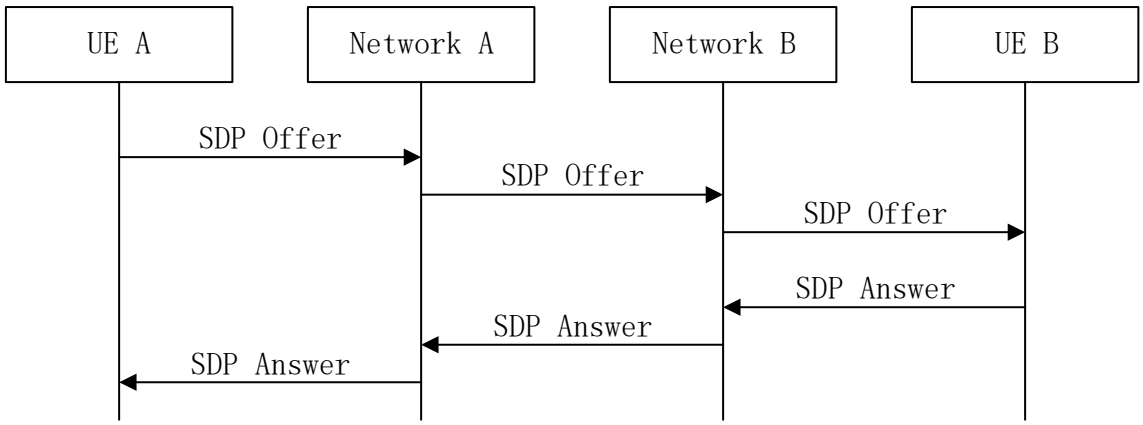

Figure A.1-1: Basic SDP offer and answer exchange for establishing bootstrap data channel.

Initial SDP offer over UNI (UE A – Network A)
m=audio 10000 RTP/AVP 0 b=AS:200 a=rtpmap:0 PCMU/8000 m=video 10002 RTP/AVP 98 b=AS:1000 a=rtpmap:98 H264/90000 m=application 52718 UDP/DTLS/SCTP webrtc-datachannel b=AS:500 a=max-message-size:1024 a=sctp-port:5000 a=setup:actpass a=fingerprint:SHA-1 4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB a=tls-id: abc3de65cddef001be82 a=dcmap:0 subprotocol="http" a=dcmap:10 subprotocol="http"   m=application 52720 UDP/DTLS/SCTP webrtc-datachannel b=AS:500

```
a=max-message-size:1024
a=sctp-port:5000
a=setup:actpass
a=fingerprint:SHA-1 4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AC
a=tls-id: abc3de65cddef001be84
a=dcmap:100 subprotocol="http"
a=dcmap:110 subprotocol="http"
```

Table A.1-1: Example of SDP initial offer from UE A to Network A

As shown in Table A.1-1, UE A creates the initial offer and indicates that it allows data channel applications from all sources specified by 3GPP TS 26.114 [1] and it is UE B that will determine what sources will be used. The "local", i.e. DC stream ID 0, DC stream ID 10, and "remote", i.e. DC stream ID 100, DC stream ID 110 sources are logical concepts and are stored respectively by the DCS-A and the DCS-B when defined from the perspective of UE A which initiates the offer. The IP addresses of the DCS-A and the DCS-B are determined by the network as part of the initial offer and those addresses are transparent to UE.

Initial SDP offer over NNI (Network A to Network B)

```
m=audio 10000 RTP/AVP 0
b=AS:200
a=rtpmap:0 PCMU/8000

m=video 10002 RTP/AVP 98
b=AS:1000
a=rtpmap:98 H264/90000

m=application 52720 UDP/DTLS/SCTP webrtc-datachannel
b=AS:500
a=max-message-size:1024
a=sctp-port:5000
a=setup:actpass
a=fingerprint:SHA-1 …
a=tls-id: …
a=dcmap:100 subprotocol="http"
a=dcmap:110 subprotocol="http"
```

Table A.1-2: Example of initial SDP offer from Network A to Network B

Initial SDP offer over UNI (Network B – UE B)

```
m=audio 10000 RTP/AVP 0
b=AS:200
a=rtpmap:0 PCMU/8000

m=video 10002 RTP/AVP 31
b=AS:1000
a=rtpmap:31 H261/90000

m=application 52718 UDP/DTLS/SCTP webrtc-datachannel
b=AS:500
a=max-message-size:1024
a=sctp-port:5000
a=setup:actpass
```

```
a=fingerprint:SHA-1 …
a=tls-id: …
a=dcmap:0 subprotocol="http"
a=dcmap:10 subprotocol="http"


m=application 52720 UDP/DTLS/SCTP webrtc-datachannel
b=AS:500
a=max-message-size:1024
a=sctp-port:5000
a=setup:actpass
a=fingerprint:SHA-1 …
a=tls-id: …
a=dcmap:100 subprotocol="http"
a=dcmap:110 subprotocol="http"
```

Table A.1-3: Example SDP offer from Network B to UE B

SDP answer over UNI (UE B to Network B)
m=audio 20000 RTP/AVP 0 b=AS:200 a=rtpmap:0 PCMU/8000 m=video 20002 RTP/AVP 31 b=AS:1000 a=rtpmap:31 H261/90000 m=application 52720 UDP/DTLS/SCTP webrtc-datachannel b=AS:500 a=max-message-size:1024 a=sctp-port:5002 a=setup:passive a=fingerprint:SHA-1 5B:AD:67:B1:3E:82:AC:3B:90:02:B1:DF:12:5D:CA:6B:3F:E5:54:FA a=tls-id: dcb3ae65cddef0532d42 a=dcmap:110 subprotocol="http"

Table A.1-4: Example SDP answer from UE B to Network B

As shown in Table A.1-4, UE B only receives applications from the network A using stream ID "110" data channel, so the only applications that are available to users are those offered by the network A.

SDP answer over NNI (Network B to Network A)
m=audio 20000 RTP/AVP 0 b=AS:200 a=rtpmap:0 PCMU/8000 m=video 20002 RTP/AVP 31 b=AS:1000 a=rtpmap:31 H261/90000 m=application 52720 UDP/DTLS/SCTP webrtc-datachannel b=AS:500 a=max-message-size:1024

```
a=sctp-port:5002
a=setup:passive
a=fingerprint:SHA-1 …
a=tls-id: …
a=dcmap:110 subprotocol="http"
```

Table A.1-5: Example SDP answer from Network B to Network A

SDP answer over UNI (Network A to UE A)

```
m=audio 20000 RTP/AVP 0
b=AS:200
a=rtpmap:0 PCMU/8000

m=video 20002 RTP/AVP 31
b=AS:1000
a=rtpmap:31 H261/90000

m=application 52718 UDP/DTLS/SCTP webrtc-datachannel
b=AS:500
a=max-message-size:1024
a=sctp-port:5010
a=setup:active
a=fingerprint:SHA-1 BC:8A:99:A0:E3:28:CA:B3:09:20:1B:FD:21:D5:AC:B6:F3:5E:45:AF
a=tls-id: cd3bea56dced0f35d224
a=dcmap:0 subprotocol="http"
a=dcmap:10 subprotocol="http"
```

Table A.1-6: Example SDP answer from Network A to UE A

Once the initial SDP offer and answer negotiation annotated above succeeds, then both peers are connected to the same Data Channel Server and therefore can download the same content.

- 2 bootstrap data channels are established between UE A and the DCS-A, i.e. DC stream ID 0, DC stream ID 10 and no bootstrap data channels between UE A and the DCS-B. Then UE A sends HTTP GET to its own root "/" URL to download its application list. The bootstrap data channels between UE A and the DCS-A are used to download list of available applications to UE A and select the application(s).
- UE A opens 2 "tab" or other interface constructs, i.e. one per each bootstrap data channel content source.
- 1 bootstrap data channel is established between UE B and the DCS-A, i.e. DC stream ID 110 and no bootstrap data channels are established between UE B and the DCS-B. Therefore, UE B does not send HTTP GET to its own root "/" URL hosted by DCS-B but it sends HTTP GET to DCS-A to download its application list.
- UE B opens 1 "tab" or another interface construct.

A.2 Application Data Channel Establishment – Subsequent Offer SDP Example

Once the relevant interface constructs are presented to the user then the user MAY chose a specific application to invoke. The JavaScript code needs to be downloaded from the DCS and according to 3GPP TS 26.114 [1] the following principles apply:

- Stream IDs 10 and 110 are associated together by the DCS and represent the transport level mechanism giving access to the same application to both peers.
- UE A uses the "menu selection" mechanism to choose an application from the list of the DCS-A available applications and UE A then initiates the application business logic using the stream ID of the associated interface construct to which the application belongs to download its code. That is the application downloaded by UE A over the stream ID 10 and by remote UE B using stream ID 110.
- When the DCS-A receives the request to download an application from the initiating UE A over local stream ID then it automatically knows that the same application should be made available on the UE B when needed. And the DCS-A will resolve UE B HTTP GET uniquely to the same application over the NNI and UNI. That is streams ID 10 and stream ID 110 are associated to the same content.

The data channel application download does not generate any SDP offers/answers. After the successful download of data channel application is completed the data channel business logic might create subsequent offer, i.e. re-invite, when application data channel needs to be created. Table A.17.6 of 3GPP TS 26.114 [1] provides SDP example for re-invite.

Annex B (Informative): IMS Data Channel Application Developer Device APIs

B.1 JavaScript API Requirements for the Device

IMS data channel applications can use any JavaScript APIs but in this version of the document the W3C Media Capture and Streams [56] usage to generate WebRTC1.0 media types of speech and video is prohibited since GSMA PRD IR.92 [5], IR.94 [6] and GSMA PRD NG.114 [7] media types are mandated.

Annex C (Informative) : Implementation Proposal for External Content Access within SIP session

Annex C contains the implementation proposal for a use case that is not supported yet by 3GPP TS 26.114. It is included only for information purposes.

C.1 Access to External Servers within SIP session

The IMS data channel application service logic and media content MAY be either provided by the Data Channel Server inside the operator's administrative domain, or by an External Server which is deployed outside the operator's administrative domain.

NOTE: The origin of application service logic and media content might be the same or different. For example, the operator hosted DCS can deliver to UE the business logic to execute and later when the business logic is applied and the data channel is created it might exchange media content with an external server e.g. to download something from the web server when the application itself was not downloaded from the web server. This simply means that UE can consume a content from different sources during the data channel call.

The UE SHALL and the network MAY support enriching IMS data channel session with a content provided by an external source. That is the source of the content consumed during the data channel session SHOULD NOT be limited to only the content hosted by the IMS network in which the subscriber has registered.

C.2 General Principles

The workflow defined in section 6.10.2.1 of 3GPP TS 26.114 [1] applies and the informative Annex D describes two possible models by allowing IMS data channel session to access the external media content. Annex C only focuses on UNI and NNI aspects.

C.3 Selection of Content Source

Only the data channel application SHALL select the external content source and the network MAY respect that decision. The network MAY also decide to either reject the request or redirect it to other content source when required e.g. to avoid location tracking as described in IETF RFC 7721 [30].

An external server and the associated content SHOULD be referenced using the standardized and accepted methods, including but not limited to:

- Transport addresses (i.e. combination of IP address and port for a particular transport protocol)
- Uniform Resource Locators (URL) as defined by IETF RFC 1808[31].

The reference MAY be hard coded by the application, dynamically calculated by the Data Channel Server (e.g. function of location), resolved by some other dynamic methods or entered by subscriber. But in all cases it is the data channel application action that SHALL initiate the transaction towards the element providing the external egress interface.

C.4 External Content Delivery over UNI

Section 4.2.2 of 3GPP TS 33.328 [32] mandates always including the IMS Access Gateway (IMS-AGW) in the media path when e2ae (End-to-access-edge**)** security is required even if the involvement of the IMS-AGW would otherwise not be needed, e.g. if traffic could be routed only between two terminals in the same IMS domain. Accordingly for all e2ae scenarios application data channel path SHALL be anchored to the IMS-AGW and the following procedures apply:

- Mb interface is used to exchange the data channel external content between the DCMTSI client in terminal and the server in question. The procedures defined in section 6.2.10 of 3GPP TS 26.114 [1] are used to establish the data channel that transports external content over UNI. This interface SHALL support the bootstrap data channel and the application data channel content transfer in a fashion that is independent of location of the Data Channel Application Repository (DCAR), Data Channel Server or any external content servers. In all cases regardless of whether the server is internal or external to the network hosting 3GPP TS 26.114 [1] defined Data Channel Server, the UE SHALL use only IMS APN to carry the data channel content towards and from the external server. The data channel traffic exchanged over HTTP between the UE and the Data Channel Server SHALL be transmitted over UDP/DTLS/SCTP. The Mb interface SHOULD be enhanced with data channel capability as recommended in section 5.20.1 of 3GPP TS 23.334 [33]. If so, the IMS-AGW SHALL perform necessary DTLS and SCTP handling as specified in section 5.20.2 of 3GPP TS 23.334 [33], and forwards data channel traffic between the UE and the Data Channel Server.
- Gm interface as specified in 3GPP TS 23.228 [34] SHALL support the required signalling procedures to establish the data channel and the transport of data channel media. When a DCMTSI client in terminal decides to invoke an external data channel application, it SHALL initiate SIP re-INVITE with subsequent SDP Offer by adding corresponding "a=dcmap" and (optionally) "a=dcsa" lines as specified in section 6.2.10.2 of 3GPP TS 26.114 [1], to establish a data channel for the target data channel application.
- An individual SCTP (IETF RFC 4960 [14]) connection over DTLS (IETF RFC 8261 [15]) SHALL be established between the DCMTSI client in terminal and the remote server (i.e. the Data Channel Server, or the External Server) that provides the target data channel application. If multiple data channels are required to set up connection to the same external server and to set up end-to-end connection to a remote UE, multiple m-lines should be used, each m-line with a corresponding "a=dcmap" SDP attribute and stream IDs that are unique within that media description, as specified in 3GPP TS 26.114 [1].
- DCMTSI client SHALL follow procedures described in section 5.1 of GSMA PRD IR.92 [5] and section 4.9 of GSMA PRD NG.114 [7] when requesting network to allocate IP address for IMS session. Once it has discovered the P-CSCF and registered to IMS with a particular IP address, it SHALL use this IP address for all SIP communication for as long as the IMS registration is valid. For data channel media types, the DCMTSI client MAY use different UDP ports, or different SCTP ports other than those parameters UE used for IMS voice media types, as specified in

section 6.2.10 of 3GPP TS 26.114 [1]. All addresses used for transport of external content SHALL be routable.

- The network MAY modify the externally routable data channel IP address for reasons different from NAT traversal as per local requirements (e.g. to avoid location tracking as described in IETF RFC 7721 [30]).

The UNI specification SHALL be invariant with respect to the model used i.e. regardless of whether the content is provided by the operator network or external network the same 3GPP TS 26.114 [1] defined procedures are executed. The UE SHALL NOT need to know the model used to deliver the data channel content and the UE SHOULD NOT need to implement any specific routing method.

C.5 External Data Network IP Level Interface

The external server is hosted by IETF RFC 1930 [59] defined autonomous system towards which DCMTSI client has an external routing policy.

NOTE 1: The section does not use the term NNI in order not to confuse this interface with Inter-IMS Network to Network Interface (II-IMS) defined in 3GPP TS 29.165 [4]. The reference point in question is the interface between the data channel subsystem and the external public IP Data Network (DN) hosting the external server. The IMS data channel connectivity service enabling the exchange of PDUs between a DCMTSI client and a DN is used upon the request from the data channel application. The interworking between IMS and DN requires IP (i.e. IETF RFC 791 [36]) level interworking provided by 3GPP TS 23.501 [8] defined N6 interface or 3GPP TS 23.401 [9] defined SGi interface. The external server uses DN specific protocol stack e.g. HTML/JavaScript over HTTP over TCP. The network SHOULD support the required interfaces and protocols depending on the service requirement, e.g. TCP/TLS (IETF RFC 5246 [36]) for HTTP (IETF RFC 2616 [37]) content, etc.

The network MAY require the exterior routing protocols such as BGP described in IETF RFC 1771 [38] or at minimum OSPF [61] to advertise the data channel IP addresses to the external networks.

The current version of this document only profiles HTTP server (i.e. the external server in Model A) or HTTP server enhanced with IETF RFC 8831 [10] support (i.e. the external server in Model B). Accordingly:

- Model A: the Data Channel Server acts as the inter-system relay between DCMTSI client in terminal and the external server. It SHALL support the necessary HTTP transport level interworking i.e. from HTTP over UDP/DTLS/SCTP to HTTP over TCP/TLS, and vice versa.
- Model B: the data channel media path MAY be established directly between the UE and the External Server when e2e security mode is allowed and packets are forwarded transparently. The external routing policy SHALL be configured in the operator network to support routing the data channel application traffic towards the External Server.

NOTE 2: The end to end (e2e) security does not have the anchoring requirement and it should in principle allow true peer to peer transport of data channel traffic. As mentioned in 3GPP TS 33.328 [32] the pre-requisite for support of e2e security is that media packets are forwarded transparently by any nodes present in the media path.

Annex D (Informative): Communication Model for Accessing External Server

The data channel enriches the VoIMS session with an arbitrary content that can be served during the call (i.e. in in-call fashion) and may come from the server hosted by the network where UE has registered or from any other external source. This section describes the scenario that an External Server is deployed outside the operator's administrative domain and provides service logic and/or media content for the data channel application. Depending on whether the external server supports WebRTC protocol stack specified in IETF RFC 8831 [10] two models are listed in the following sections.

D.1 Model A: HTTP Server without IETF RFC 8831 Data Channel Support

The external server supports only HTTP protocol and responds to DCMTSI service requests for the data channel content. This content invokes the designed business logic on the device and drives the interaction between the user and server.

The model A uses end-to-access edge (e2ae) encryption; therefore all data channel traffic is anchored in IMS network and it is transported unencrypted from IMS-AGW towards the external entities.

The use cases for this model might include.

1. two people playing a game hosted on the internet, or A-Party sharing in the real time the browser screen when looking up the stock prices and discussing it with B-Party.
2. call to enterprise customer care where during the call an agent pushes a login page for one of its customers to have access to the current status of the order.

In those examples, the service would offer the best effort 5QI=9.

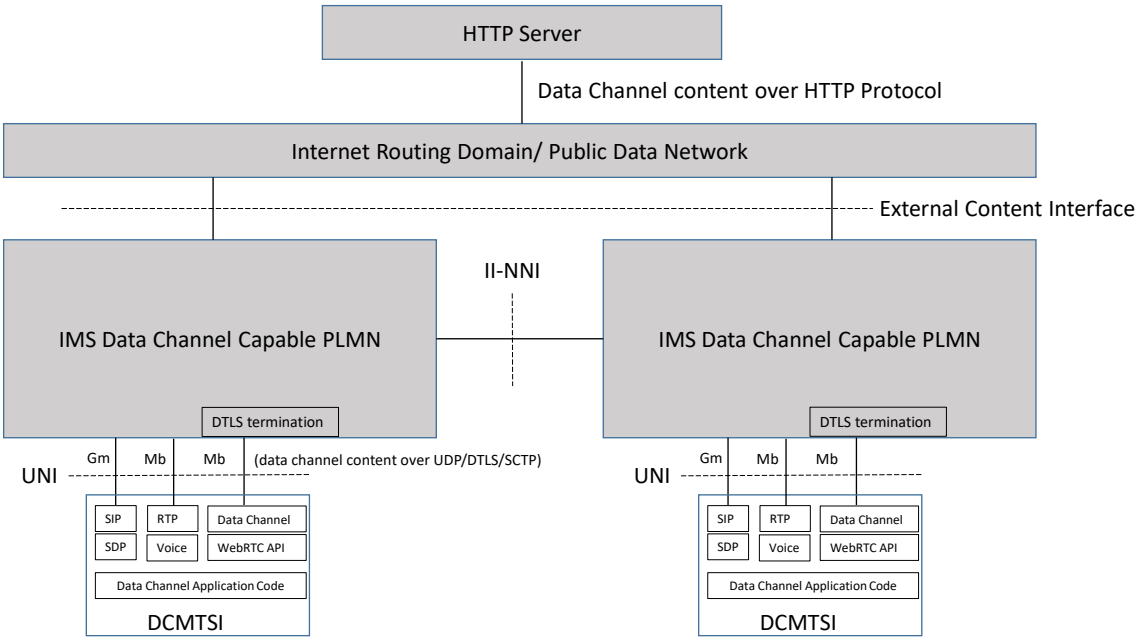

Figure C.1-1: Model A – IMS data channel access to external HTTP Server

In this model, the following principles are applied:

- The data channel is established between the DCMTSI client in terminal and the IMS. An SCTP connection over DTLS over UDP is established between the DCMTSI client in terminal and the IMS-AGW, as described in 3GPP TS 23.334 [33]. Based on "a=setup" SDP attribute the IMS-AGW might act as DTLS client or DTLS server (i.e. "a=active" indicates that IMS-AGW acts as DTLS server and it acts as DTLS client when value "a=passive" is received).
- It shall be noted that the data channel termination (i.e. DTLS and SCTP termination) and the data channel content termination (i.e. endpoints of application data channel content exchanges) are different in this case since that data channel terminates in IMS network but the data channel content is provided from outside of IMS network, i.e. the data channel transport layer is applied on Mb interface but data channel content layer is served between the external server and UE.
- The data channel is encrypted over Mb interface (i.e. UNI) but it is unencrypted over other interfaces.
- NAT/NAPT can be applied on the egress IMS-AGW interface as per Annex G of 3GPP TS 23.228 [34].
- The Data Channel Server MAY interwork with the External Server via application specific protocol (e.g. TCP/HTTP based), e.g. exchange the data channel content from/to the external server.
- The data channel content that is HTML, JavaScript and CSS is served from external server and controls the DCMTSI client in terminal data channel connectivity layer, the User Interface content and the interaction with the user.

Model A is fully supported by 3GPP Release 16 and section 5.20.1 of 3GPP TS 23.334 [33] recommends end-to-access-edge (e2ae) security for data channel.

D.2 Model B: HTTP Server with IETF RFC 8831 Data Channel Support

The external server supports both HTTP and IETF RFC 8831 [10] WebRTC data channel protocols. The server responds to DCMTSI service requests for the data channel content but the content driving the interaction with the server is delivered over the data channel. The external server appears as WebRTC data channel compatible end point i.e. it can successfully communicate with other entities supporting WebRTC data channel protocol but may fail to meet any other requirements e.g. does not have to support WebRTC API.

To establish the WebRTC data channel a signalling channel is required e.g. to exchange fingerprints binding the certificates. In that case WebSocket (i.e. IETF RFC 6455 [58]) or HTTPS (i.e. IETF RFC 2818 [57]) may be used.

This model uses end-to-end (e2e) encryption for the data channel as specified in IETF RFC 8831 [10] and IETF RFC 8827 [43] therefore IMS network needs to support this mode.

The use cases for this model could include XR and MEC use cases where media needs to be rendered, delivered in secure manner over high throughput links with e.g. 5QI=71. A XR game provider could use wholesale agreement with IMS network provider to offer the security and throughput on the end to end basis. The two typical scenarios could include.

1. Communication service provider including 3rd party application in its business product catalogue and the application referring to the external content when required i.e. the application could open an application data channel towards an external content.
2. Communication service provider serving both the bootstrap and the application content from an external server.

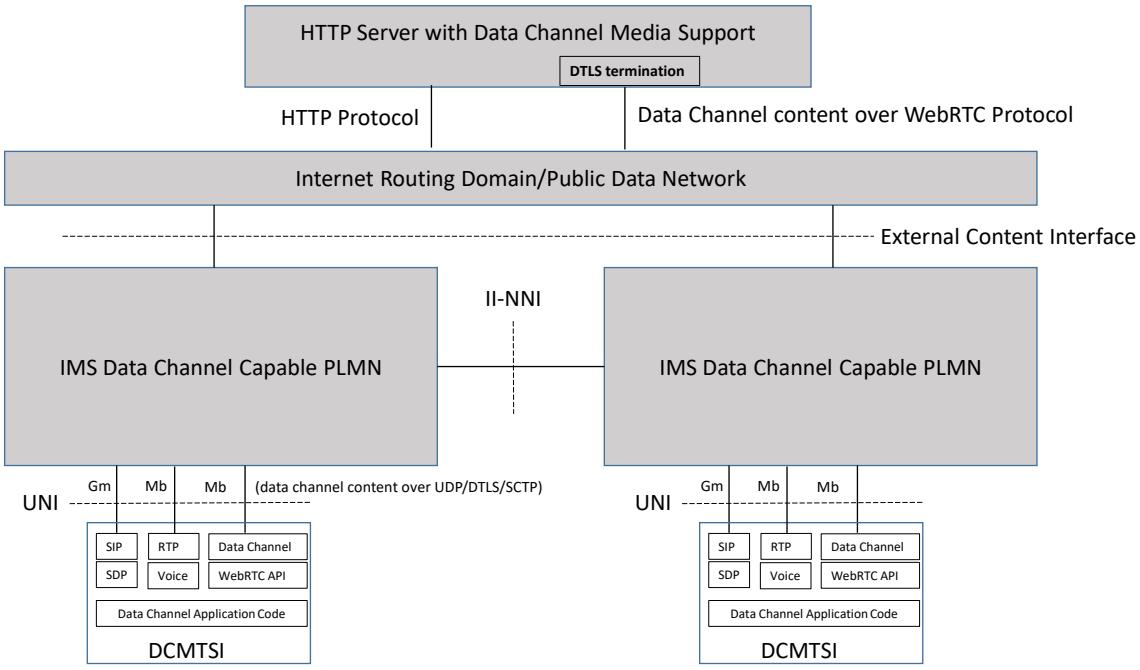

Figure C.2-1: Model B, IMS data channel access to external HTTP Server with Data Channel Support

In this model, the following principles are applied:

- The application data channel is established between the DCMTSI client in terminal and the External Server. An SCTP connection over DTLS over UDP is established directly between the DCMTSI client in terminal and the external server.
- NAT/NAPT can be applied on the egress IMS-AGW interface as per Annex G of 3GPP TS 23.228 [34].
- IMS-AGW MAY remain in the media plane path e.g. for the purpose of media plane optimization specified in section U.2.4 of 3GPP TS 23.228 [34] and section 5.20.3 of 3GPP TS 23.334 [33]. In this case, the IMS-AGW is transparent to the DCMTSI client in terminal and it tunnels through the SCTP over DTLS and the associated signalling. Therefore, IMS-AGW needs to support the transparent media plane transport and the transparent forwarding of SDP attributes related to data channel to the next node.
- The data channel content is provided directly from the External Server to the UE. The data channel termination (i.e. DTLS and SCTP termination) and the data channel content termination (i.e. endpoints of application data channel content exchanges) are the same for model B as opposed to Model A.
- The originating DCMTSI client in terminal establishes two application data channels one to the terminating party and the second to the external server (i.e. 2 in total), or both UEs establish application channels between themselves and also each has dedicated application data channel to the external server (i.e. 3 in total), or each UE only establishes application data channel to the external server (i.e. 2 in total).
- An external signalling channel e.g. XMPP is required to establish the WebRTC data channel.

Model B is not supported by 3GPP Release 16 / 17 compliant IMS-AGW but is required to comply to IETF RFC 8831 [10] which mandates the use of end-to-end (e2e) security for WebRTC applications.

Annex E Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	January 27, 2022	Skeleton revision 0.1 approved	IDCTF	Walter Zielinski (Huawei)
0.2	April 19,2022	The following sections implemented. Introduction Section 1.1-1.6, Workflow for IMS Data Channel Section 2.1, IMS Data Channel Feature Set General Comments Section 3, SIP Registration Section 3.1, IMS Data Channel at II-NNI Section 3.4, SDP Considerations for IMS Data Channel Section 4.1, Radio and Packet Core Feature Set Section 5.1-5.3,IMS Data Channel Roaming Considerations Section 6.4	IDCTF	Walter Zielinski (Huawei)
0.3	August 30,2022	The following sections implemented. pCR to NG.134 v0.2 IMS application developer APIs – Annex B Communication Models for Accessing External Servers -Annex C Data Off Service - 6.5 Capability Discovery - 3.2 SDP Media Description - 4.2.1 Interaction with Supplementary Services – 3.3 Establishment and termination of bootstrap data channels - 4.2.2 Establishment and termination of application data channels - 4.2.3 Access to external server -4.5 HTML/JavaScript/CSS - 6.2 Security Features – 6.3 Data Off Service - 6.5	IDCTF	Walter Zielinski (Huawei)

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.4	November 3, 2022	The following sections implemented. pCR to NG.134 v0.3 IMS data channel not associated with an IMS call – 4.4. ICE/STUN/TURN – 6.1.2 Other considerations for IMS data channel – 4.6 Data channel application retrieval and synchronization – 4.2.3 JSEP – 6.1.1 Exception handling for IMS data channel – 4.2.5 Single and multiple IMS data channels per SIP session - 4.3 Informative SDP examples – Annex A	IDCTF	Walter Zielinski (Huawei)
0.5	Feb 16, 2023	pCR to NG.134 v0.4	IDCTF	Walter Zielinski (Huawei)
1.0	April 2023	CR1001 – First version	NG	Walter Zielinski (Huawei)
2.0	Feb 13, 2024	CR1002 – Alignement of IMS Data Channel Description CR1003 – Reference Correction CR1004 – Early Media	NG	Walter Zielinski (Huawei)
3.0	June 2024	CR1027_N32 via NEW 5G Control Roaming N9 via DATA Roaming VLAN R0.3	NG	Walter Zielinski (Huawei)

Other Information

Type	Description
Document Owner	GSMA NG
Editor / Company	Walter Zielinski / Huawei

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

Your comments or suggestions & questions are always welcome.