ETSI TS 124 371 V12.1.0 (2015-04)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
Web Real-Time Communications (WebRTC) access to the IP Multimedia (IM) Core Network (CN) subsystem (IMS);
Stage 3;
Protocol specification
(3GPP TS 24.371 version 12.1.0 Release 12)

Reference

RTS/TSGC-0124371vc10

Keywords

LTE,UMTS

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides the details for allowing Web Real-Time Communication (WebRTC) IMS Clients (WIC) to access the IP Multimedia (IM) Core Network (CN) subsystem.

The present document is applicable to WebRTC IMS client (WIC), eP-CSCF, WebRTC Web Server Function (WWSF) and WebRTC Authorization Function (WAF).

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

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

[3] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[4] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".

[5] IETF RFC 5763: "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)".

[6] IETF RFC 5764: "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)".

[7] 3GPP TS 22.173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1".

[8] 3GPP TS 24.173: "IMS multimedia telephony communication service and supplementary services; Stage 3".

[9] 3GPP TS 33.203: "Access security for IP based services".

[10] RFC 6750 (October 2012): "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[11] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2".

[12] RFC 5009 (September 2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[13] 3GPP TS 23.334: "IMS Application Level Gateway (IMS-ALG) – IMS Access Gateway (IMS-AGW) interface".

[14] RFC 4145 (September 2005): "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[15] RFC 4572 (July 2006): "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)".

[16] draft-ietf-rtcweb-data-channel-13 (January 2015): "WebRTC Data Channels".

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

[17] draft-ietf-rtcweb-data-protocol-09 (January 2015): "WebRTC Data Channel Establishment Protocol".

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

[18] draft-ietf-mmusic-sctp-sdp-012 (January 2015): "Stream Control Transmission Protocol (SCTP)-Based Media Transport in the Session Description Protocol (SDP)".

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

[19] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[20] RFC 3264 (June 2002): "An Offer/Answer Model with the Session Description Protocol (SDP)".

[21] draft-ietf-rtcweb-stun-consent-freshness-11(December 2014): "STUN Usage for Consent Freshness".

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

[22] RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[23] draft-ietf-tsvwg-sctp-dtls-encaps-08 (January 2015): "DTLS Encapsulation of SCTP Packets".

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

[24] RFC 6455 (December 2011): "The WebSocket Protocol".

[25] draft-ietf-mmusic-sdp-bundle-negotiation-16 (January 2015): "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)".

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

[26] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[27] draft-yusef-sipcore-sip-oauth-01 (October 2014): "The Session Initiation Protocol (SIP) OAuth".

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

[28] RFC 6544 (March 2012): "TCP Candidates with Interactive Connectivity Establishment (ICE)".

[29] draft-nandakumar-mmusic-proto-iana-registration-00 (September 2014) " IANA registration of SDP 'proto' attribute for transporting RTP Media over TCP under various RTP profiles".

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

[30] draft-ietf-rtcweb-overview-12 (October 2014): "Overview: Real Time Protocols for Brower-based Applications".

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

[31] draft-alvestrand-rtcweb-gateways-01 (October 2014): "WebRTC Gateways".

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

[32] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[33] RFC 4169 (November 2005): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2".

[34] 3GPP TS 26.114: "IP multimedia subsystem (IMS); Multimedia telephony, Media handling and interaction".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [4] annex U apply:

P-CSCF enhanced for WebRTC (eP-CSCF)
WebRTC Authorization Function (WAF)
WebRTC IMS Client (WIC)
WebRTC Web Server Function (WWSF)

Editor's note: Terminology from draft-ietf-rtcweb-overview needs to be endorsed as part of the terminology of this document. This document uses the terms "WebRTC device" which it is understood will be changed to "non-WebRTC browser".

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CN	Core Network
CSCF	Call Session Control Function
eP-CSCF	enhanced Proxy CSCF
IM	IP Multimedia
IP	Internet Protocol
WAF	WebRTC Authorization Function
WebRTC	Web Real-Time Communication
WWSF	WebRTC Web Server Function

4 Overview of WebRTC access to IMS

4.1 General

The relationship between functional entities for the interface at the W1 reference point, between the WWSF and the UE, the interface at the W2 reference point, between the eP-CSCF and the UE, the interface at the W3 reference point, between the UE and the eIMS-AGW, and the interface at the W4 reference point, between the WWSF and the WAF, are defined in annex U of 3GPP TS 23.228 [4].

The relationship between the functional entities for interface at the Mw reference point, between the eP-CSCF and the remainder of the IP multimedia core network subsystem, is defined in 3GPP TS 23.228 [4].

A number of appropriate mechanisms exist for signalling communication between the WIC and the eP-CSCF. Sucessful use of a mechanism other than those specified in this document will require some form of prior agreement between the operator of the WWSF and the operator of the eP-CSCF, as to the nature of the signalling mechanism that is to be adopted, and therefore the interworking required at the eP-CSCF. The mechanism of prior agreement and the nature of such agreement is not defined in this document.

A signalling transport mechanism for SIP is standardised in this release of this document, i.e. SIP over websockets (see RFC 7118 [2]), but this is not a mechanism that has to be supported by all eP-CSCFs.

When SIP over websockets is used, it can be appropriate for the SIP used to conform to the definitions for SIP on the Gm reference point as specified in 3GPP TS 24.229 [3]. Such a requirement is not mandatory, but where other SIP mechanisms are used:

a) the usage will require some form of prior agreement with the operator of the eP-CSCF, as to the nature of the signalling mechanism that is to be adopted; and

b) the SIP mechanisms will have to enable the eP-CSCF to conform to the SIP requirements over the Mw reference point to the remainder of the IP multimedia core network subsystem as specified in 3GPP TS 24.229 [3].

SDP is used for the signalling session information between the WIC and the eP-CSCF. Such SDP conforms to requirements for SDP on the Gm reference point.

5 Functional entities

5.1 General

5.2 WIC (WebRTC IMS Client)

A WebRTC IMS Client (WIC) establishing the service control signalling path over W2 interface, that is compliant with this specification shall implement the role of WIC capabilities defined in subclause 6.2, subclause 7.2 and subclause 8.2.

Where SIP over websockets is used, as specified in RFC 7118 [2], and no alternative SIP profiles have been agreed between the operator of the eP-CSCF and the operator of the WWSF, then the SIP used by the WIC over the W2 reference point shall conform to the requirements for UE over the Gm reference point as specified in 3GPP TS 24.229 [3].

When the WebSocket protocol is used, the WIC shall act as a WebSocket Client, as defined in RFC 6455 [24].

The SDP used shall conform to the requirements for UE over the Gm reference point as specified in 3GPP TS 24.229 [3].

Editor's note: If specific exceptions are identified in this document, then this subclause will also need to point to those exceptions.

5.3 WWSF (WebRTC Web Server Function)

The WebRTC Web Server Function (WWSF) is the initial point of contact in the Web that controls access to the IMS communications services for the WIC as specified in 3GPP TS 23.228 [4].

5.4 WAF (WebRTC Authorisation Function)

The WebRTC Authorisation Function (WAF) issues authorization tokens that are provided to the WIC via the WWSF as specified in 3GPP TS 23.228 [4] and 3GPP TS 33.203 [9].

NOTE: The WWSF and the WAF realisations can be physically co-located or physically separate.

5.5 eP-CSCF (P-CSCF enhanced for WebRTC)

For the Mw reference point, the eP-CSCF shall conform to the requirements for the P-CSCF as specified in 3GPP TS 24.229 [3].

Where SIP over websockets is used, as specified in RFC 7118 [2], and no alternative SIP profile have been agreed between the operator of the eP-CSCF and the operator of the WWSF, then the SIP used by the eP-CSCF over the W2 reference point shall conform to the requirements for P-CSCF over the Gm reference point as specified in 3GPP TS 24.229 [3].

The SDP used by the eP-CSCF over the W2 reference point used shall conform to the requirements for UE over the Gm reference point as specified in 3GPP TS 24.229 [3].

Editor's note: If specific exceptions are identified in this document, then this subclause will also need to point to those exceptions.

5.6 eIMS-AGW (IMS Access GateWay enhanced for WebRTC)

5A Data transport

5A.1 General

Data transport is the support of TCP, UDP and the means to securely set up connections between entities, as well as the functions for deciding when to send data: Congestion management, bandwidth estimation and so on.

5A.2 UE

A UE supporting WebRTC shall support the WebRTC device functionality as specified in draft-ietf-rtcweb-overview [30] clause 4, excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 4.

Editor's note: This clause references draft-ietf-rtcweb-transports-06 which uses the terminology "WebRTC browser", "WebRTC endpoint" and "WebRTC device" for both ends of the transport. STUN and TURN introduce further "server" and "client" terminology that has to be allowed for.

5A.3 WWSF (WebRTC Web Server Function)

There are no data transport requirements for the WWSF.

NOTE: Any application downloaded from the WWSF that requires data transport is expected to use it in accordance with WebRTC device support of data transport.

5A.4 eP-CSCF (P-CSCF enhanced for WebRTC)

The eP-CSCF and eIMS-AGW in conjunction shall support the WebRTC gateway functionality as specified in draft-ietf-rtcweb-overview [30] clause 4 as modified by draft-alvestrand-rtcweb-gateways [31], excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 4.

5B Data framing and securing

5B.1 General

Data framing RTP and other data formats that serve as containers, and their functions for data confidentiality and integrity.

5B.2 UE

A UE supporting WebRTC shall support the WebRTC endpoint functionality as specified in draft-ietf-rtcweb-overview [30] clause 5, excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 5.

Editor's note: This clause references RFC 3550 which uses the terminology "RTP implementation" for both ends of the RTP. This clause references draft-ietf-rtcweb-rtp-usage which uses the terminology "WebRTC endpoint" for both ends of the RTP, but also uses other terms e.g. "RTP endpoint".

5B.3 WWSF (WebRTC Web Server Function)

There are no data framing requirements for the WWSF.

NOTE: Any application downloaded from the WWSF that requires data framing is expected to use it in accordance with WebRTC device support of data framing.

5B.4 eP-CSCF (P-CSCF enhanced for WebRTC)

The eP-CSCF and eIMS-AGW in conjunction shall support the WebRTC gateway functionality as specified in draft-ietf-rtcweb-overview [30] clause 5 as modified by draft-alvestrand-rtcweb-gateways [31] and excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 5.

5C Data formats

5C.1 General

Data format is codec specifications, format specifications and functionality specifications for the data passed between systems. audio and video codecs, as well as formats for data and document sharing, belong in this category.

5C.2 UE

A UE supporting WebRTC shall support the WebRTC device functionality as specified in draft-ietf-rtcweb-overview [30] clause 6, excluding requirements to implement specific audio and video codecs.

A UE offering WebRTC access to the IMS via GPRS IP-CAN (as described in 3GPP TS 24.229 [3], annex B) or EPS IP-CAN (as described in 3GPP TS 24.229 [3], annex L) shall support the speech codecs according to 3GPP TS 26.114 [34] clause 5 and the front-end handling as specified in 3GPP TS 26.114 [34] clause 11.

A UE supporting WebRTC access to the IMS via GPRS IP-CAN (as described in 3GPP TS 24.229 [3], annex B) or EPS IP-CAN (as described in 3GPP TS 24.229 [3], annex L) and supporting video communication shall support the video codecs according to 3GPP TS 26.114 [34].

Editor's note: This clause references draft-ietf-rtcweb-audio which uses the terminology "WebRTC clients" for both ends of the RTP. The terminology used here needs to be aligned to cater for these inconsistencies.

Editor''s note (WID:IMS-WebRTC, CR#0003): Specifications to be referenced for media related requirements relating to specific codecs, if any, to be supported by a UE supporting WebRTC access to the IMS via IP-CAN other than GPRS IP-CAN and other than EPS IP-CAN, will be determined by SA4.

5C.3 WWSF (WebRTC Web Server Function)

There are no data format requirements for the WWSF.

NOTE: Any application downloaded from the WWSF that requires data formats is expected to use it in accordance with WebRTC device support of data formats.

5C.4 eP-CSCF (P-CSCF enhanced for WebRTC)

The eP-CSCF and eIMS-AGW in conjunction shall support the WebRTC gateway functionality as specified in draft-ietf-rtcweb-overview [30] clause 6 as modified by draft-alvestrand-rtcweb-gateways [31], excluding requirements to implement specific audio and video codecs.

An eP-CSCF and eIMS-AGW supporting UEs offering WebRTC access to the IMS via GPRS IP-CAN (as described in 3GPP TS 24.229 [3], annex B) or EPS IP-CAN (as described in 3GPP TS 24.229 [3], annex L) shall support the codecs according to 3GPP TS 26.114 [34] clause 5.

An eP-CSCF receiving an SDP offer from the IMS core network should retain the received codecs in the SDP offer it sends towards the UE to avoid transcoding.

Editor"s note (WID:IMS-WebRTC, CR#0003): Specifications to be referenced for media related requirements relating to specific codecs, if any, to be supported by a eP-CSCF supporting WebRTC access to the IMS via IP-CAN other than GPRS IP-CAN and other than EPS IP-CAN, will be determined by SA4.

5D Connection management

5D.1 General

Connection management is setting up connections, agreeing on data formats, changing data formats during the duration of a call; SIP and Jingle/XMPP belong in this category.

5D.2 UE

A UE supporting WebRTC shall support the WebRTC browser or WebRTC device functionality as specified in draft-ietf-rtcweb-overview [30] clause 7 as appropriate, excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 7.

Editor's note: This clause references draft-ietf-rtcweb-jsep which uses the terminology "browser". The terminology used here needs to be aligned to cater for these inconsistencies.

5D.3 WWSF (WebRTC Web Server Function)

There are no connection management requirements for the WWSF.

NOTE: Any application downloaded from the WWSF that requires connection management is expected to use it in accordance with WebRTC device support of connection management.

5D.4 eP-CSCF (P-CSCF enhanced for WebRTC)

The eP-CSCF and eIMS-AGW in conjunction shall support the WebRTC gateway functionality as specified in draft-ietf-rtcweb-overview [30] clause 7 as modified by draft-alvestrand-rtcweb-gateways [31] and excluding requirements, if any, relating to specific audio and video codecs that are indirectly referenced within the draft-ietf-rtcweb-overview [30] clause 7.

5E Presentation and control

5E.1 General

Presentation and control is what needs to happen in order to ensure that interactions behave in a non-surprising manner. This can include floor control, screen layout, voice activated image switching and other such functions - where part of the system require the cooperation between parties.

5E.2 UE

A UE supporting WebRTC as a WebRTC browser shall support the WebRTC browser functionality as specified in draft-ietf-rtcweb-overview [xx] clause 8.

Editor's note: This clause only references APIs produced by W3C.

5E.3 WWSF (WebRTC Web Server Function)

There are no presentation and control requirements for the WWSF.

NOTE: Any application downloaded from the WWSF that requires presentation and control is expected to use it in accordance with WebRTC browser support of presentation and control.

5E.4 eP-CSCF (P-CSCF enhanced for WebRTC)

There are no presentation and control requirements for the eP-CSCF.

5F Local system support functions

5F.1 General

Local system support functions is what needs to happen in order to ensure that interactions behave in a non-surprising manner. This can include floor control, screen layout, voice activated image switching and other such functions - where part of the system require the cooperation between parties.

5F.2 UE

Editor's note (WID:IMS-WebRTC, CR#0003): reference to the draft-ietf-rtcweb-overview [30], clause 9 is FFS. The current version of the draft-ietf-rtcweb-overview [30], clause 9 does not contain any requirements that need to be referenced.

Void.

5F.3 WWSF (WebRTC Web Server Function)

Editor's note (WID:IMS-WebRTC, CR#0003): reference to the draft-ietf-rtcweb-overview [30], clause 9 is FFS. The current version of the draft-ietf-rtcweb-overview [30], clause 9 does not contain any requirements that need to be referenced.

There are no local system support requirements for the WWSF.

5F.4 eP-CSCF (P-CSCF enhanced for WebRTC)

There are no local system support functions for the eP-CSCF.

6 Registration and authentication

6.1 General

This clause specifies procedures that are related to registration of a WIC in the IM CN subsystem that are required for support of WebRTC.

There are the following IMS registration scenarios defined in 3GPP TS 23.228 [4] Annex U. 3GPP TS 33.203 [9] specifies the following authentication methods applying to different IMS registration scenarios separately.

a) Scenario 1: The WIC registration of individual public user identity using IMS authentication. There are two authentication methods specified in 3GPP TS 33.203 [9], corresponding to this scenario:

1) SIP Digest authentication scheme; and

2) use of IMS AKA authentication scheme.

b) scenario 2: The WIC registration of individual public user identity based on web authentication.

1) Web authentication scheme: The registration procedure between the eP-CSCF and the IM CN subsystem reuses the Trusted Node Authentication (TNA) procedure specified in 3GPP TS 33.203 [9]; or

c) scenario 3: The WIC registration of individual public user identity from a pool of public user identities.

1) Web authentication scheme: The registration procedure between the eP-CSCF and the IM CN subsystem reuses the Trusted Node Authentication (TNA) procedure specified in 3GPP TS 33.203 [9]. The registration procedure of scenario 3 is basically the same with scenario 2, with the difference that, in scenario 3 it is assumed that the WWSF is provided with a pool of public user identities and can assign public user identities within this pool.In all the registration scenarios, it is assumed that HTTP or HTTPS connection is used between the WIC and the WWSF, where HTTPS connection is recommended due to the security considerations.

The structure of subclause 6 is divided by functional entity as the first level, and in each subclause of a specific functional entity, all the authentication solutions are described in the sequence of registreation scenarios.

As the media plane security mechanisms for WebRTC, i.e. DTLS-SRTP for RTP based media and DTLS/SCTP for non-RTP based media, are mandatory to be supported in WIC and eP-CSCF, there is no need to indicate the media plane security mechanisms in the Security-Client header field of the REGISTER request and in the Security-Server header field of the 200 (OK) response to the REGISTER request.

The WIC and the eP-CSCF using Gm shall follow the registration procedures as described in 3GPP TS 24.229 [3] and the procedures as described in this document in addition. For the WIC and eP-CSCF using Gm, the appropriate signalling protocol is defined in 3GPP TS 24.229 [3] and this document.

For the WIC and eP-CSCF using non-Gm or non-SIP, the registration procedures and the signalling protocol are out of scope of this document.

6.2 WIC (WebRTC IMS Client)

6.2.1 WIC registration of individual Public User Identity using IMS authentication

6.2.1.1 General

When using SIP over Websockets as signalling protocol on the W2 interface:

1) when the WIC uses registration using SIP Digest it shall follow the procedures as described in subclause 6.2.1.2; and

2) when the WIC uses registration using IMS-AKA it shall follow the procedures described in subclause 6.2.1.3.

6.2.1.2 W2 using SIP Digest credentials

When using SIP over Websockets as signalling protocol on the W2 interface and using registration based on SIP Digest credentials, the WIC shall use the procedures for "SIP Digest without TLS" as specified in 3GPP TS 24.229 [3].

NOTE: The WIC uses the TLS connection that was established during the WebSocket connection setup.

6.2.1.3 W2 using IMS-AKA

When using SIP over Websockets as signalling protocol on the W2 interface and when IMS AKA is used for authenticating the WIC, the WIC shall use the IMS-AKA procedures defined in 3GPP TS 24.229 [3] with the following modifications:

1) HTTP Digest AKAv2 as defined in RFC 4169 [yy] is used instead of HTTP Digest AKA defined in RFC 3310 [xx]; and

2) IPSec security association set-up is not performed at the final stage of the authentication.

NOTE: The WIC uses the TLS connection that was established during the WebSocket connection setup to protect the IMS signalling between the WIC and the eP-CSCF.

On sending a REGISTER request as defined in 3GPP TS 24.229 [3] for IMS AKA, the WIC shall:

1) additionally populate the Authorization header field with the "algorithm" header field parameter set to "AKAv2-SHA-256" as defined in RFC 4169 [yy]; and

2) not include the Security-Client header in the REGISTER request.

On receiving the 200 (OK) response to the REGISTER request the WIC shall not set the IPSec security association and associated lifetime.

6.2.2 WIC registration of individual public user identity based on web authentication

In this subclause it is assumed that SIP over Websockets is used as the signalling protocol on the W2 interface and the user has a subscription with an individual IMPU, but uses a web identity and authentication scheme, e.g. OAuth 2.0, to authenticate with the WWSF or the WAF.

As specified in 3GPP TS 33.203 [9], after receiving the authorization token from WWSF, which is issued by WAF, the WIC shall:

- send a SIP REGISTER request, which includes the authorization token as described in draft-yusef-sipcore-sip-oauth-00 [27], to the eP-CSCF via the Websockets connection.

Editor's note: The draft-yusef-sipcore-sip-oauth-00 has not been well defined yet, so how to include the authorization token in SIP REGISTER request message still needs ffs.

6.2.3 WIC registration of individual public user identity from a pool of public user identities

In this scenario it is assumed that the WWSF is provided with a pool of public user identities and can assign public user identities within this pool. The WIC procedure is as specified in subclause 6.2.2, with the difference that the public user identity (and private user identity) is temporarily assigned to the user and there is no linkage between the user"s web identity that may be authenticated by an authentication service and the assigned IMS identities.

6.3 WWSF (WebRTC Web Server Function) and WAF (WebRTC Authorisation Function)

6.3.1 WIC registration of individual public user identity using web credentials

The WWSF pushes WebRTC JavaScript to theWIC, authenticates the WIC"s web credentials and forwards the authorization token to the WIC which is issued by WAF. Detailed web authentication procedures related to the WWSF in W1 and W4 interface are described in 3GPP TS 33.203 [9] and will not be specifed in this document.

6.3.2 WIC registration of individual public user identity from a pool of public user identities

The WWSF and the WAF procedure is the same as specified in subclause 6.3.1, with the exception that in this scenario the WAF authenticates only the WWSF without user involvement, and the WWSF may choose not to authenticate the user if the user is to remain anonymous.

6.4 ePCSCF (P-CSCF enhanced for WebRTC)

6.4.1 WIC registration of individual Public User Identity using Digest authentication

6.4.1.1 Determination of IMS authentication mechanism

When the eP-CSCF receives a REGISTER request using SIP over Websockets as signalling protocol on the W2 interface, the eP-CSCF determines which IMS authentication mechanism to use as described in annex P of 3GPP TS 33.203 [9].

6.4.1.2 W2 using SIP Digest credentials

When the eP-CSCF receives a REGISTER request for "SIP Digest with TLS" using SIP over Websockets as signalling protocol on the W2 interface, then the procedures as defined in 3GPP TS 24.229 [3] subclause 5.2.2 apply. In addition the eP-CSCF shall:

1) if the REGISTER request was received on a pre-established TLS then:

   a) if the REGISTER request does not map to an existing TLS association, and does not contain a challenge response, not include the "integrity-protected" header field parameter;

   b) if the REGISTER request does not map to an existing TLS association, and does contain a challenge response, include an "integrity-protected" header field parameter with the value set to "tls-pending";

   c) if the REGISTER request does map to an existing TLS association, include an "integrity-protected" header field parameter with the value set to "tls-protected";

   d) if the "rport" header field parameter is included in the Via header field, set the value of the "rport" header field parameter in the Via header field to the source port of the received REGISTER request; and

   e) insert the "received" header field parameter in the Via header field containing the source IP address that the request came from, as defined in RFC 3581 [26].

NOTE: As defined in RFC 3581 [26], the P-CSCF will insert a "received" header field parameter containing the source IP address that the request came from, even if it is identical to the value of the "sent-by" component.

When the eP-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the eP-CSCF shall:

1) send the 401 (Unauthorized) response to the UE using the TLS session with which the associated REGISTER request was protected.

When the eP-CSCF receives a 200 (OK) response to a REGISTER request as defined, and the registration expiration interval value is different than zero, the eP-CSCF shall additionally:

- create an TLS association by storing and associating the UEs IP address and port of the TLS connection with the TLS Session ID, the private user identity and all the successfully registered public user identities related to that private user identity; and

- send the 200 (OK) response to the REGISTER request within the same TLS session to that in which the request was protected.

Editor"s Note: It is ffs whether the text in this sub-clause can be included in TS 24.229

6.4.1.3 W2 using IMS-AKA

When the eP-CSCF receives a REGISTER request from the WIC for IMS-AKA over a TLS session set-up prior registration:

1) not including the Security Client header field; and

2) containing an Authorization header field with an "algorithm" header field parameter set to "AKAv2-SHA-256";

the eP-CSCF shall:

a) include the "integrity-protected" header field parameter with the value set to "tls-connected" in the Authorization header field;

b) if the "rport" header field parameter is included in the Via header field, then set the value of the "rport" header field parameter in the Via header field to the source port of the received REGISTER request; and

c) insert the "received" header field parameter in the Via header field containing the source IP address that the request came from, as defined in RFC 3581 [26]:

NOTE: As defined in RFC 3581 [26], the P-CSCF will insert a "received" header field parameter containing the source IP address that the request came from, even if it is identical to the value of the "sent-by" component.

before forwarding the REGISTER request.

When the eP-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the eP-CSCF shall:

1) send the 401 (Unauthorized) response to the UE using the TLS session with which the associated REGISTER request was protected.

When the eP-CSCF receives a 200 (OK) response to a REGISTER request, and the registration expiration interval value is different than zero, the eP-CSCF shall additionally:

- create an association by storing and associating the UEs IP address and port of the TLS connection with the TLS Session ID, the private user identity and all the successfully registered public user identities related to that private user identity; and

- protect the 200 (OK) response to the REGISTER request within the same TLS session to that in which the request was protected.

6.4.2 WIC registration of individual public user identity using web credentials

In this subclause it is assumed that SIP over Websockets is used as the signalling protocol on the W2 interface. Upon receiving the SIP REGISTER request from the WIC, the eP-CSCF shall extract the authorization token and validate it as specified in 3GPP TS 33.203 [9] Annex X. If the authorization token is verified valid, the eP-CSCF obtains the associated authorization information, including the private user identity and public user identity of the associated user, the WWSF identity, and the authorization information scope.

The eP-CSCF inserts the obtained private user identity and public user identity in the SIP REGISTER request, where the Authorization header in SIP REGISTER request, as specified in 3GPP TS 33.203 [9] Annex U, contains the private user identity, and the To header field in the SIP REGISTER request contains the public user identity.

NOTE: The eP-CSCF will overwrite the To header field value received in the SIP REGISTER request from the WIC.

Then the eP-CSCF performs as the trusted node in TNA scheme specified in 3GPP TS 33.203 [9] Annex U. The eP-CSCF forwards the SIP REGISTER request to the S-CSCF as specified in 3GPP TS 24.229 [3], where the Authorization header in SIP REGISTER request, as specified in 3GPP TS 33.203 [9] Annex U, contains the user"s private user identity, an "integrity-protected" header field set to "auth-done ", and an empty "response" header field.

If the WAF, which authorizes the WIC to access the IMS core and issues the authorization token, is located in third party domain, the eP-CSCF shall also include the WAF identity in the REGISTER request, using the Authorization header field, with the "authorization-entity" header field parameter set to the value of the WAF identity.

Editor's note: How to include the WWSF identity in the register request is ffs.

Upon receiving the SIP 200 (OK) response from the S-CSCF, the eP-CSCF forwards SIP 200 (OK) response to the WIC. When TLS is used between the WIC and the eP-CSCF, the eP-CSCF shall additionally create an association between the UE and the TLS connection as specified in 3GPP TS 24.229 [3] subclause 5.2.2.4.

6.4.3 WIC registration of individual public user identity from a pool of public user identities

As specified in subclause 6.4.2.

6A Deregistration

6A.1 General

This clause specifies procedures that are related to deregistration in the IM CN subsystem that are required for support of WebRTC.

The WIC and the eP-CSCF using Gm shall follow the deregistration procedures as described in 3GPP TS 24.229 [3] and the procedures as described in this document in addition. For the WIC and the eP-CSCF using Gm, the appropriate signalling protocol is defined in 3GPP TS 24.229 [3] and this document.

For the WIC and eP-CSCF using non-Gm or non-SIP, the deregistration procedures and the signalling protocol are out of scope of this document.

6A.2 WIC (WebRTC IMS Client)

It is assumed that the WIC has previously registered, and the signalling protocol between the WIC and the eP-CSCF applies SIP over WebSockets where the SIP procedures conform to the definitions for SIP on the Gm reference point as specified in 3GPP TS 24.229 [3].

The WIC shall follow the deregistration procedures speicifed in 3GPP TS 24.229 [3] subclause 5.1.1.6 and subclause 5.1.1.7.

If the WIC have no more public user identities registered in the IM CN subsystem, the WebSockets connection between the WIC and the eP-CSCF shall be removed.

6A.3 eP-CSCF (P-CSCF enhanced for WebRTC)

The eP-CSCF shall follow the deregistration procedures speicifed in 3GPP TS 24.229 [3] subclause 5.2.5.1 and subclause 5.2.5.2.

NOTE: In the scenario that individual public user identity is assigned by the WWSF or the WAF from a pool of public user identities, as an implementation specific option, when the public user identity has been deregistered in the IM CN subsystem, the eP-CSCF can indicate to the WAF that a certain public user identity can be re-assigned, while the procedures for the interface between the eP-CSCF and the WAF is out of scope of this specification.

7 Call origination and termination

7.1 General

This clause specifies procedures that are related to call origination and termination in the IM CN subsystem that are required for support of WebRTC.

It is assumed that prior to the call origination and termination procedure, a WebSockets connection hase been established between the WIC and the eP-CSCF. The call control signalling between the WIC and the eP-CSCF is transport over the WebSockets connection.

The WIC shall support ICE procedures as described in RFC 5245 [22] and RFC [6544] [28], with the additions specified in draft-ietf-rtcweb-stun-consent-freshness-03 [21]. The WIC shall perform ICE procedures when initiated by other subclauses in this document.

Editor's note: IETF RTCWEB WG has the concensus that ICE-TCP candidates are permitted, as specified in draft-ietf-rtcweb-transports-05 that "ICE-TCP candidates [RFC6544] MUST be supported." RTP media stream transported over TCP or over TLS in "m=" line can be described using draft-nandakumar-mmusic-proto-iana-registration [29]. Procedures how to signal the transport address shift between UDP candidate and TCP candidate, when there are both UDP candidates and TCP candidates in a call need to be added.

7.2 WIC (WebRTC IMS Client)

7.2.1 General

The WIC shall support RFC 5763 [5] and RFC 5764 [6].

The WIC using Gm shall follow the procedures as described in 3GPP TS 24.229 [3]. For the WIC using Gm, the appropriate signalling protocol is defined in 3GPP TS 24.229 [3].

The WIC using non-Gm SIP shall support RFC 3261 [19]. For the WIC using non-Gm, the appropriate signalling protocol is defined in RFC 3261 [19].

The WIC using non-SIP shall support RFC 3264 [20]. For the WIC using non-SIP, the appropriate signalling protocol is out of scope of this specification.

7.2.2 WIC originating call

When the WIC originates a call, the WIC shall:

a) perform the ICE procedures as defined in RFC 5245 [22] and possibly RFC 6544 [28]; and

b) generate an SDP offer and send it towards the eP-CSCF using the appropriate signalling protocol as described in subclause 7.2.1.

Upon generating an SDP offer with RTP based media, for each RTP based media, the WIC

a) shall offer UDP transport protocol according RFC 5763 [5], with the proto field in the "m=" line containing the "UDP/TLS/RTP/SAVPF" value according to RFC 5764 [6];

b) may additionally, within the same "m=" line, offer TCP transport protocol with appropriate ICE candidates according to RFC 6544 [28]; and

c) shall additionally, within the same "m=" line, indicate an SDP "a=3ge2ae:requested" attribute.

7.2.3 WIC terminating call

Upon receipt of an SDP offer, the WIC shall:

a) perform the ICE procedures as defined in RFC 5245 [22] and possibly RFC 6544 [28]; and

b) generate an SDP answer and send it towards the eP-CSCF using the appropriate signalling protocol as described in subclause 7.2.1.

Upon receiving an SDP offer containing an RTP based media:

- transported using RFC 5763 [5], with the proto field in the "m=" line containing the "UDP/TLS/RTP/SAVPF" value according to RFC 5764 [6]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the RTP based media, then the UE shall generate the SDP answer with the related RTP based media transported. In order to do so, the UE:

a) shall use RFC 5763 [5], and provide the proto field in the "m=" line containing the "UDP/TLS/RTP/SAVPF" value according to RFC 5764 [6]; and

b) may additionally, within the same "m=" line, offer TCP transport protocol with appropriate ICE candidates according to RFC 6544 [28].

7.2.4 WIC emergency call

A WIC shall not attempt to establish a session when the WIC can detect that the number dialled is an emergency number.

Note: Emergency calls originated from a WIC are not supported in this version of the specification.

Editor's note: It needs to be studied how the WIC reacts on a negative response that it receives as answer for an UE non-detected emergency call.

7.3 WWSF (WebRTC Web Server Function)

No additional procedure is specified for WWSF.

7.4 eP-CSCF (P-CSCF enhanced for WebRTC)

7.4.1 General

The eP-CSCF using Gm towards the WIC shall follow the procedures as described in 3GPP TS 24.229 [3]. For the eP-CSCF using Gm, the appropriate signalling protocol is defined in 3GPP TS 24.229 [3].

The eP-CSCF using non-Gm SIP towards the WIC shall support RFC 3261 [19]. For the eP-CSCF using non-Gm, the appropriate signalling protocol is defined in RFC 3261 [19].

The eP-CSCF using non-SIP towards the WIC shall support RFC 3264 [20]. For the eP-CSCF using non-SIP, the appropriate signalling protocol is out of scope of this specification.

The eP-CSCF shall support RFC 5763 [5] and RFC 5764 [6].

7.4.2 WIC originating call

Upon receipt of an SDP offer, the eP-CSCF shall:

a) perform ICE procedures as defined in 3GPP TS 24.229 [3]; and

b) generate an SDP offer based on the SDP offer received from the WIC and forward it using the appropriate signalling protocol as described in subclause 7.4.1. The eP-CSCF shall replace the SDP offer with updated SDP provided by eIMS-AGW, which contains the eIMS-AGW IP addresses and ports. The eP-CSCF shall not use bundled media as described in draft-ietf-mmusic-sdp-bundle-negotiation [25], i.e. the eP-CSCF shall remove the SDP group attribute BUNDLE value, and any m- line that in the received SDP offer contained an SDP "bundle-only" attribute, from the SDP offer.

NOTE: At this point, the eP-CSCF interacts with eIMS-AGW to reserve resources and provide the information needed for media handling. The details of the interaction between eP-CSCF and eIMS-AGW are out of scope of this document.

Upon receiving an SDP offer from the served WIC containing an DTLS-SRTP based media stream with end-to-access-edge protection, i.e. an "m=" line:

- with the proto field containing the "UDP/TLS/RTP/SAVPF" value as specified in RFC 5764 [6]; and

- with the SDP "a=3ge2ae:requested" attribute or, if permitted by operator policy, without the SDP "a=3ge2ae:requested" attribute;

the eP-CSCF shall invoke IMS-ALG procedures, shall remove the SDP "a=3ge2ae:requested" attribute, if included, and the SDP fingerprint attribute and shall act as defined in 3GPP TS 24.229 [3] as far as SDP and RTP is concerned.

Upon receiving an SDP answer over the Mw interface, for each DTLS-SRTP based media stream with end-to-access-edge protection of the SDP offer from the served WIC which is accepted in the received SDP answer, the eP-CSCF shall invoke IMS-ALG procedures.In the SDP answer to served WIC the transport protocol, the eP-CSCF

a) shall use to RFC 5763 [5] and shall provide the proto field in the "m=" line withthe "UDP/TLS/RTP/SAVPF" value according to RFC 5764 [6]; and

b) may additionally, within the same "m=" line, offer TCP transport protocol with appropriate ICE candidates according to RFC 6544 [28].

If the SDP offer contained bundled media as described in draft-ietf-mmusic-sdp-bundle-negotiatio [25], the eP-CSCF shall reject the bundling of media, i.e. the eP-CSCF shall not add a SDP group BUNDLE attribute to the SDP answer, and the eP-CSCF shall assign a zero port value to any m- line that in the SDP offer contained an SDP "bundle-only" attribute.

NOTE: Stage 2 has specified that the architecture does not support media multiplexing that is defined for WebRTC, so the SDP answer sent to the served WIC will not contain bundled media.

7.4.3 WIC terminating call

Upon receiving an SDP offer over the Mw interface with an RTP based media, for each RTP based media, the eP-CSCF:

1) shall invoke IMS-ALG procedures;

2) shall perform ICE procedures as defined in 3GPP TS 24.229 [3]; and

3) in the SDP offer to served WIC:

- shall indicate the transport protocol according to RFC 5763 [5], with the proto field in the "m=" line containing the "UDP/TLS/RTP/SAVPF" value according to RFC 5764 [6];

- may additionally, within the same "m=" line, offer TCP transport protocol with appropriate ICE candidates according to RFC 6544 [28]; and

- shall include the SDP "a=3ge2ae:applied" attribute.

NOTE: Stage-2 has specified that the architecture does not support media multiplexing that is defined for WebRTC, so the SDP offer sent to the served WIC will not contain bundled media.

Upon receipt of an SDP answer, the eP-CSCF:

a) shall perform ICE procedures as defined in3GPP TS 24.229 [3];

b) shall generate an SDP answer based on the SDP answer received from the WIC and forward it using the appropriate signalling protocol as described in subclause 7.4.1;

c) for each RTP based media of the SDP offer from the remote UE which is accepted in the SDP answer:shall remove the SDP fingerprint attribute; and

d) shall act as defined in 3GPP TS 24.229 [3] as far as SDP and RTP is concerned.

7.4.4 WIC emergency call

If the eP-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user, the eP-CSCF shall inspect the Request-URI. The eP-CSCF shall consider the Request URI of the initial request as a emergency service identifier, if it is an emergency numbers or an emergency service URN from the configurable lists that are associated with:

1) the country of the operator to which the eP-CSCF belongs to; and

2) the country of roaming partners, if the request originates from a different country then the country of the network to which the eP-CSCF belongs to. If Gm based W2 is used, then access technology specific procedures are described in each access technology specific annex of 3GPP TS 24.229 [3] to determine from which country and roaming partner the request was originated; and

3) if the country from which the request originates cannot be determined then all lists are associated.

If the eP-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method matches one of the emergency service identifiers in the associated lists then the eP-CSCF shall:

A) If item 1) applies then determine whether the request originates from the same country as the country of the network to which the eP-CSCF belongs. If Gm based W2 is used, then access technology specific procedures are described in each access technology specific annex of 3GPP TS 24.229 [3] to determine from which country and roaming partner the request was originated. If the request originates from the same country, then the eP-CSCF depending on operator policy shall:

   a) reject the request as appropriate for the signalling in use. If Gm based W2 is used, then send 380 (Alternative Service) response; or

   b) proceed the request as specified in of 3GPP TS 24.229 [3] sub-clause 5.2.10.4 for the case where the request is not rejected; or

B) in all other cases the eP-CSCF shall reject the request as appropriate for the signalling in use. If Gm based W2 is used, then send a 380 (Alternative Service) response.

Editor's note: The contents of 380 (Alternative Service) response requires further study.

8 Data channel open and close

8.1 General

This clause specifies the procedures for negotiating usage of, and opening and closing of, a WebRTC data channel between the WIC and the eP-CSCF.

WebRTC data channels are realized using an SCTP association running on top of DTLS, as described in draft-ietf-tsvwg-sctp-dtls-encaps [23] and draft-ietf-rtcweb-data-channel [16]. Once the SCTP association has been negotiated and established, the WIC and eIMS-AGW (controlled by the eP-CSCF) use the Data Channel Establishment Protocol (DCEP) for opening and closing data channels, as described in draft-ietf-rtcweb-data-protocol [17].

Editor's note (WI: IMS_WebRTC): A mechanism for the WIC and eP-CSCF to inform each other, during the negotiation of the SCTP association, for what purposes data channels will be used, is outside the scope of the current release of the specification. Before DCEP is used to open the data channels, knowledge about the purpose of the data channels might be based e.g. on configuration, or might be implicitly determined based on information carried in the signalling protocol between the WIC and the eP-CSCF.

Editor's note: Use of data channel to transport other protocols, e.g. MSRP, BFCP and T.140 is ffs.

8.2 WIC (WebRTC IMS Client)

8.2.1 General

The WIC shall follow the general call establishment procedures in subclause 7. This subclause defines the additional procedures for establishing WebRTC data channels within the call.

8.2.2 WIC originating call

Upon generating an SDP offer, the WIC shall insert an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the fmt value set to "webrtc-datachannel" according to draft-ietf-mmusic-sctp-sdp [18], in the SDP offfer. In addition, the WIC shall insert an SDP sctp-port attribute according to draft-ietf-mmusic-sctp-sdp [18].

8.2.3 WIC terminating call

Upon receiving an SDP offer, with an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the "m=" line fmt value set to "webrtc-datachannel", the WIC shall follow the procedures in draft-ietf-mmusic-sctp-sdp [18] for generating the associated SDP answer. In addition, the WIC shall insert an SDP sctp-port attribute according to draft-ietf-mmusic-sctp-sdp [18].

8.3 WWSF (WebRTC Web Server Function)

8.4 eP-CSCF (P-CSCF enhanced for WebRTC)

8.4.1 General

The eP-CSCF shall follow the general call establishment procedures in clause 7. This subclause defines the additional procedures for establishing WebRTC data channels within the call.

In the current release of the specification, the eIMS-AGW will act as an endpoint for all WebRTC data channels established between the eIMS-AGW and the served WIC. If the eIMS-AGW is able to perform transport protocol interworking for a media transported between the eIMS-AGW and the served WIC using a data channel, and between the eIMS-AGW and the remote user using another transport protocol, the eP-CSCF can instruct the eIMS-AGW to perform transport protocol interworking between the data channel and the other transport protocol.

Editor's note: The H.248 procedures needed for the eP-CSCF to establish and control a data channel in the eIMS-AGW are still to be defined.

8.4.2 WIC originating call

Upon receiving an SDP offer from the served WIC, with an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the fmt value set to "webrtc-datachannel", according to draft-ietf-mmusic-sctp-sdp [18], the eP-CSCF shall:

- remove the "m=" line from the SDP offer; and
- for each media transported between the WIC and the eIMS-AGW using a data channel, and for which the eIMS-AGW is able to perform transport protocol interworking between a data channel and another transport protocol, insert an "m=" line describing the media and the transport protocol used for the media in the SDP offer;

before forwarding the SDP offer towards the remote user.

Upon receiving an SDP answer to the SDP offer, the eP-CSCF shall:

- remove each "m=" line associated with an "m=" line that the eP-CSCF inserted in the associated SDP offer from the SDP answer;
- insert an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the fmt value set to "webrtc-datachannel" according to draft-ietf-mmusic-sctp-sdp [18], in the SDP answer;
- insert an SDP sctp-port attribute according to draft-ietf-mmusic-sctp-sdp [18], in the SDP answer; and
- for each media accepted by the remote user, for which the eIMS-AGW can perform transport protocol interworking between a data channel and another transport protocol, instruct the eIMS-AGW to perform the transport protocol interworking;

before forwarding the SDP answer towards the served WIC.

8.4.3 WIC terminating call

Upon receiving an SDP offer from the remote user, the eP-CSCF shall:

- remove each "m=" line that describes media which is transported between the WIC and the eIMS-AGW using a data channel from the SDP offer;
- insert an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the fmt value set to "webrtc-datachannel" according to draft-ietf-mmusic-sctp-sdp [18], in the SDP offer; and
- insert an SDP sctp-port attribute according to draft-ietf-mmusic-sctp-sdp [18], in the SDP answer;

before forwarding the SDP offer towards the served WIC.

Upon receiving an SDP answer to the SDP offer, with an "m=" line with the proto value set to "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP", and the fmt value set to "webrtc-datachannel", according to draft-ietf-mmusic-sctp-sdp [18], the eP-CSCF shall:

- remove the the "m=" line from the SDP answer;
- for each media which the eIMS-AGW is able to perform transport protocol interworking between a data channel and another transport protocol, and for which the SDP offer contained an "m=" line, insert an "m=" line describing the media and the transport protocol used for the media in the SDP answer; and
- for each media accepted by the remote user, for which the eIMS-AGW can perform transport protocol interworking between a data channel and another transport protocol, instruct the eIMS-AGW to perform the transport protocol interworking;

before forwarding the SDP answer towards the remote user.

9 Call modification

WIC and eP-CSCF shall behave in accordance with the procedures specified in subclause 7. There is no additional requirement specified within this release.

10 IP multimedia application support in the IM CN subsystem using webRTC

10.1 General

10.2 Access to MMTel and supplementary services using webRTC

10.2.1 General

This clause describes the procedures for interaction of WebRTC based access to the IM CN subsystem and the execution of supplementary service as described in 3GPP TS 22.173 [7].

10.2.2 WIC (WebRTC IMS Client)

10.2.2.1 SIP based protocol used by the WIC

If the protocol between the WIC and the eP-CSCF is based on SIP, then in order to support an MMTel supplementary service, the SIP procedures shall conform to the SIP procedures specified in the 24 series specification of the respective supplementary service. 3GPP TS 24.173 [8] lists the documents defining the MMTel supplementary services.

10.2.2.2 non-SIP based protocol used by the WIC

The support of MMTel supplementary services when accessing the IM CN subsystem with non-SIP based protocol is not specified in this version of the specification.

10.2.3 WWSF (WebRTC Web Server Function)

10.2.4 eP-CSCF (P-CSCF enhanced for WebRTC)

When a SIP is used on the W2 interface, then there are no supplementary specific requirements defined for the eP-CSCF.

When a non-SIP protocol is used on the W2 interface, then the eP-CSCF has to map information elements from non-SIP based protocol on W2 interface to the corresponding SIP information elements on the Mw reference point.

Annex A (informative): Example signalling flows

A.1 Scope of signalling flows

This annex gives examples of signalling flows for IMS based WebRTC, and the W2 interface is based on SIP protocol.

A.2 Void

A.3 Signalling flows for registration

A.3.1 Void

A.3.2 WIC registration of individual public user identity based on web authentication

Figure A.3.2-1 shows the registration signalling flow for the scenario when the user has a subscription with an individual public user identity, but uses a web identity and authentication scheme, e.g. OAuth 2.0, to authenticate with the WWSF or the WAF.

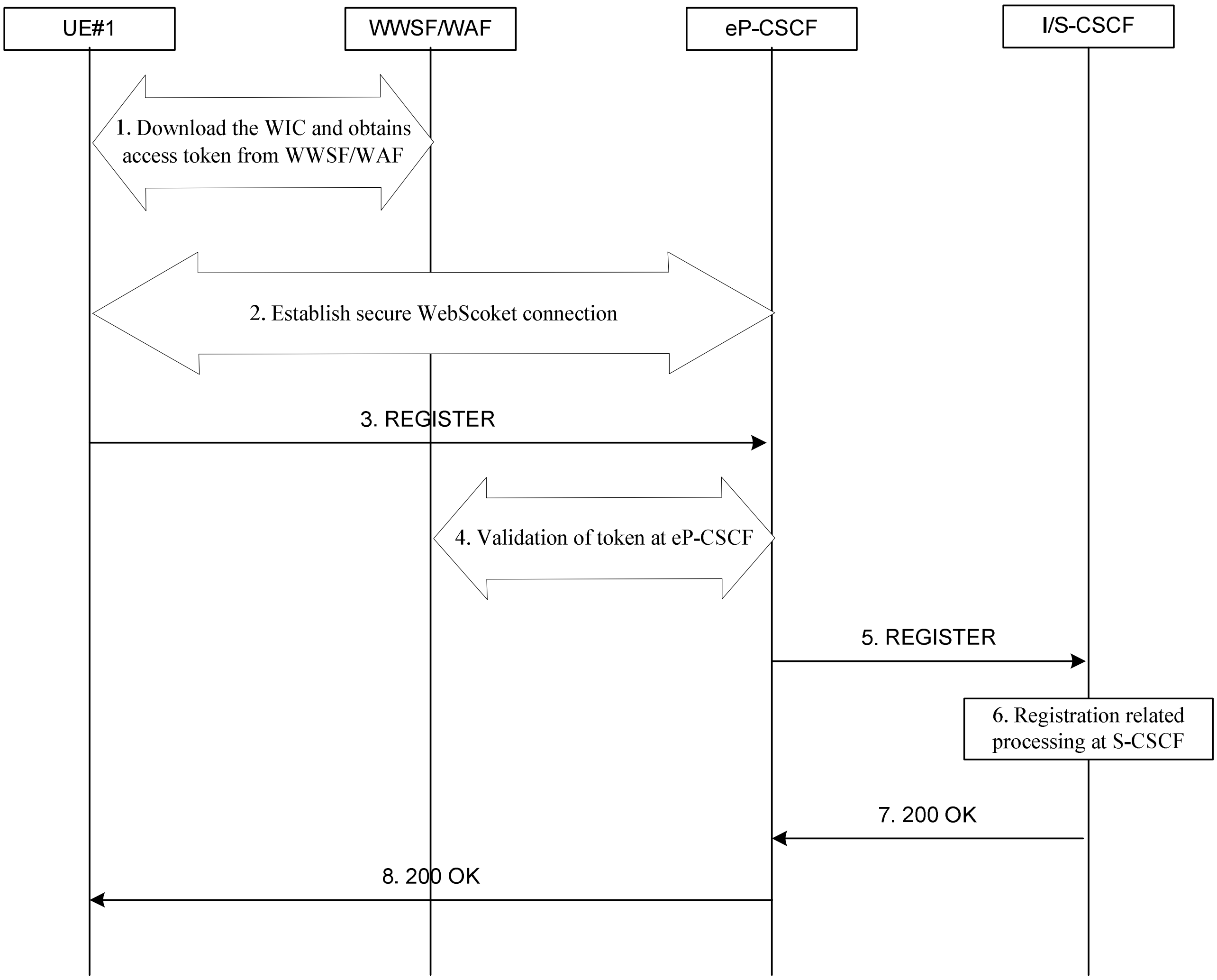
UE#1
WWSF/WAF
eP-CSCF
I/S-CSCF
1. Download the WIC and obtains access token from WWSF/WAF
2. Establish secure WebScoket connection
3. REGISTER
4. Validation of token at eP-CSCF
5. REGISTER
6. Registration related processing at S-CSCF
7. 200 OK
8. 200 OK

Figure A.3.2-1: WIC registration of individual public user identity based on web authentication

1. Download WIC and obtain access token

The user accesses a WebRTC URI to the WWSF. The browser downloads and initializes the WIC from the WWSF. The WAF or WWSF, depending on the authorization flow (e.g. OAuth 2.0) used, authenticates the user via 'web credentials', i.e. credentials as commonly used for access to web based services, for example a username and password. The user's web identity is mapped to the corresponding IMS subscriber identity (i.e. private user identity and public user identity). The WWSF forwards the authorization token and the IMS indentity to the WIC.

2. Establishment of secure connection between WIC and eP-CSCF

The WIC opens a WSS (secure Web Socket) connection to the eP-CSCF. The TLS connection provides one-way authentication of the server based on the server certificate.

3. REGISTER request (WebRTC IMS Client to eP-CSCF)

The WebRTC IMS Client sends a REGISTER request to eP-CSCF. The REGISTER request includes an authorization token, which the WebRTC IMS Client has previously obtained.

Table A.3.2-1: Authorization header field in the REGISTER request (WIC to eP-CSCF)

```
Authorization: Bearer access_token="O91G451HZ0V83opz6udiSEjchPynd2Ss9......"
```

Authorization: It carries the authorization token previously obtained from WWSF/WAF in the web authentication procedure, and the type of the authorization token (i.e. bearer token in this example).

4. Validation of security token at eP-CSCF

The eP-CSCF extracts the authorization token and validates it in some unspecified manner ensuring that only an authorized source can have generated the authorization token. If the authorization token is valid the eP-CSCF obtains the associated authorization information, including the private user identity and public user identity of the associated user, the WWSF identity, and the authorization token scope.

5. REGISTER request (eP-CSCF to S-CSCF)

The eP-CSCF proceeds if the previous step has provided it with private user identity and public user identity(s) of the user requesting registration, an assurance that the user is authorised to use this private user identity and public user identity, and an identity of the WWSF and WAF. Then, the eP-CSCF generates a Authorization header and forwards the request to the S-CSCF (via the I-CSCF).

Table A.3.2-2: Authorization header field in the REGISTER request (eP-CSCF to I/S-CSCF)

```
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response="", integrity-protected="auth-done",
   authorization-entity="webrtc_authserver1@thirdparty.net"
```

Authorization: It contains the user"s private user identity, an "integrity-protected" header field set to "auth-done ", and an empty "response" header field. In addition, the eP-CSCF shall also include the WAF identity in the SIP REGISTER request, using the Authorization header field, with the "authorization-entity" header field parameter set to the value of the WAF identity.

6. S-CSCF Registration

Based on the presence of the "integrity-protected" directive set to indicate that authentication has already been performed, the S-CSCF knows that user"s authorization has already been validated by the Trusted Node. The S-CSCF informs the HSS that the user has been registered. Upon being requested by the S-CSCF, the HSS will also include the user profile in the response sent to the S-CSCF. If the S-CSCF receives the identity of the WAF in the authorization header field, the S-CSCF shall further checks whether the identity of the authorization entity received from the eP-CSCF, if any, is not barred, as described in 3GPP TS 33.203 [9] Annex U.

7. 200 (OK) response (S-CSCF to eP-CSCF)

The S-CSCF sends a 200 (OK) response to the eP-CSCF (via I-CSCF) indicating that Registration was successful.

When TLS is used between WIC and eP-CSCF, then, similar to the registration procedure for SIP Digest with TLS, the eP-CSCF associates the private user identity and all successfully registered public user identitis with the TLS Session ID when the 200 (OK) is received.

8. 200 (OK) response (eP-CSCF to UE)

The eP-CSCF forwards the 200 (OK) response to the WebRTC IMS Client indicating that Registration was successful.

A.3.3 Void

A.4 Void

A.5 Void

Annex B (informative): Change history

Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2014-04	CT1#86bis	C1-141590 C1-141591			Initial version		0.1.0
2014-05	CT1#87	C1-142082 C1-142326 C1-142327 C1-142328 C1-142408 C1-142409 C1-142433 C1-142435 C1-142523			This version contains the changes of agreed CRs at CT1#87		0.2.0
2014-07	CT1#88	C1-142859 C1-142861 C1-142863 C1-143208 C1-143209 C1-143210 C1-143211 C1-143213 C1-143220 C1-143279 C1-143280 C1-143281 C1-143328 C1-143330 C1-143332 C1-143377 C1-143378			This version contains the changes of agreed CRs at CT1#88		0.3.0
2014-09	CT-65	CP-140627			Version 1.0.0 presented for information at CT plenary	0.3.0	1.0.0
2014-10	CT1#88bis	C1-144087 C1-144094 C1-144187 C1-144190 C1-144227 C1-144258 C1-144272 C1-144273			This version contains the changes of agreed CRs at CT1#88bis	1.0.0	1.1.0
2014-11	CT1#89	C1-144313 C1-144894 C1-144915 C1-144916 C1-144917 C1-144993 C1-144994			This version contains the changes of agreed CRs at CT1#89	1.1.0	1.2.0
2014-12	CT-66	CP-140808			Version 2.0.0 presented for approval at CT plenary	1.2.0	2.0.0
2014-12	CT-66	CP-140990			Version 2.1.0 after approval and integration of CR in CP-141004	2.0.0	2.1.0
2014-12	CT-66				Version 12.0.0 after approval at CT plenary	2.1.0	12.0.0
2015-03	CT-67	CP-150072	0001	1	IMS WebRTC reference updates	12.0.0	12.1.0
2015-03	CT-67	CP-150072	0003	3	Codec support in IMS-WebRTC	12.0.0	12.1.0

History

Document history		
V12.0.0	January 2015	Publication
V12.1.0	April 2015	Publication