3GPP TR 23.701 V12.0.0 (2013-12)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Web Real Time Communication (WebRTC) access to IP Multimedia Subsystem (IMS); Stage 2 (Release 12)

Keywords
3GPP, IMS, LTE, Real-Time, Web

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report 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 contains a study on the potential modifications of the IMS architecture and stage 2 procedures as required by the support of Web Real Time Communication (WebRTC) clients access to IMS.

For this purpose the present document addresses (non exhaustive list):

- Architectural impacts for the support of different kinds of clients (operator / Third party) in different scenarios.
- The architecture (including the support of WebRTC clients access to IMS for clients on a 3GPP UE that are roaming at access level) for following scenarios:
  - when 3GPP or non-3GPP access is used (common IMS).
  - when the UE is not roaming at access level or when home-routed access is used (these scenarios have priority for the work).
  - evaluate/study whether IMS roaming architecture is used in case of 3GPP LBO.
- Media plane aspects e.g.:
  - architectural impacts related to the use of specific codecs: the study addresses transcoding aspects but also the case where the use of 3GPP codecs is possible from the UE.

NOTE: How a WebRTC client / the browser can access to 3GPP codecs on the UE is out of the SA WG2 study scope.

  - architectural impacts related to media plane security interworking.
- Authentication and Control plane security related aspects.
- Charging.
- PCC aspects.
- Usage of the 3GPP Packet Core Network to support WebRTC clients access to IMS.

For example the following points had been studied: the PDN connection / PDP context to be used by WebRTC traffic especially in roaming cases and the QoS control, e.g. how a WebRTC client can use the QoS supported / delivered by the 3GPP Packet Core.

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

[3] IETF draft, draft-ietf-rtcweb-jsep-03: "Javascript Session Establishment Protocol".

[4] IETF draft, draft-ietf-sipcore-sip-websocket-09: "WebSocket as a Transport for SIP".

[5] OMA Work Item 0284: "RESTful Network API for VVoIP".

[6] IETF draft, draft-ietf-mmusic-sdp-bundle-negotiation-04: "Multiplexing Negotiation Using Session .Description Protocol (SDP) Port Numbers".

[7] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".

[8] IETF draft, draft-ivov-mmusic-trickle-ice-01. "Trickle ICE: Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (ICE) Protocol".

[9] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[10] IETF draft, draft-ietf-avtcore-rtp-circuit-breakers-02: "Multimedia Congestion Control: Circuit Breakers for Unicast RTP Sessions".

[11] IETF draft, draft-muthu-behave-consent-freshness-03: "STUN Usage for Consent Freshness".

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

[13] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] IETF RFC 6714: "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

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

3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

3GPP	Third Generation Partnership Project
AF	Application Function
API	Application Programming Interface
APN	Access Point Name
BFCP	Binary Floor Control Protocol
CEMA	Connection Establishment for Media Anchoring
CSCF	Call State Control Function
DTLS	Datagram Transport Layer Security
DTLS-SRTP	Datagram Transport Layer Security SRTP
eIMS-AGW	IMS-AGW enhanced for WebRTC
eP-CSCF	P-CSCF enhanced for WebRTC
EPC	Evolved Packet Core
Gwebrtc	Interface between the WebRTC client and the WebRTC Signalling Function
Gwebrtcm	Interface between the WebRTC client and the WebRTC Media Function
GTT	Global Text Telephony
HSS	Home Subscriber Server
ICE	Interactive Connectivity Establishment
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
I-CSCF	Interrogating CSCF
JS	Javascript Session
JSEP	Javascript Session Establishment Protocol
JSON	JavaScript Object Notation

LBO	Local Breakout
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
P-CSCF	Proxy CSCF
PCC	Policy Control and Charging
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
QoS	Quality of Service
RCS	Rich Communication Suite
REST	Representational State Transfer
RFC	Request for Comments
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRTP	Secure RTP
TLS	Transport Layer Security
TNA	Trusted Network Access
WebRTC	Web Real-Time Communication
WebRTC Signalling Function	Mediation function between a WebRTC client and IMS for the control plane
WebRTC Media Function	Mediation function between WebRTC client and IMS for the media plane
WIC	WebRTC IMS Client
WWSF	WebRTC Web Server Function
XMPP	Extensible Messaging and Presence Protocol

4 Assumptions and architectural requirements

4.1 Assumptions

- SDP offer/answer exchange is the mechanism used for media plane feature negotiation.

- In this release, the architecture does not support media multiplexing that is defined for WebRTC clients.

NOTE 1: A JS downloaded in a WIC accessing to IMS services is not expected to allow usage of media multiplexing in the browser. If an SDP offer with media multiplexing was nevertheless sent to the network the part of the SDP offer associated with media multiplexing would be removed at the entry of the IMS network.

- In this release, WebRTC specific media plane extensions will be handled at the access edge and will not be propagated to other IMS functions.

- In this release, in case of a network based interworking between WebRTC and IMS, for 3GPP and EPC access from a WebRTC client:

  - There is no assumption on the APN being used by the WebRTC client, e.g. the signalling sent by the WebRTC client may use the same APN than the one used for plain Internet service.

  - Subject to inter-operator agreement and appropriate network configuration, EPC/GPRS roaming is supported for WebRTC client access using any available APN. Either LBO or home routing can be used subject to reachability.

  - Use of available techniques to select preferred access technologies and APNs, and to provide IP address continuity, are allowed but not described.

  - When the WebRTC client is served by an IP-CAN in a configuration that supports PCC, it shall be possible to request QoS within the IP-CAN for WebRTC media.

NOTE 2: To ensure full end to end QoS support, proper IP forwarding policies should be set in the path between the PGW and the Functions supporting media interworking to the IMS.

- QoS can be provided in configurations where the IMS can identify the transport (TCP-UDP/IP) addresses handled by the PCEF and where based on this information PCC functions can identify the UE media flows to prioritize.

4.2 Architectural requirements

The architecture shall fulfil the following requirements:

- WebRTC clients shall have access to the IMS through one or more mediation function(s) for signalling and media.
- The later normative work on WebRTC shall support WebRTC client access to the following media protocols (in addition to audio and video): MSRP, BFCP and T.140.

Editor's note: It is FFS if there is a need for a signalling reference protocol.

Editor's note: For 3GPP and EPC access, the assumptions of the underlying EPC network usage is FFS (including EPC roaming, LBO, APN handling/selection, access network selection, mobility issues etc).

Editor's note: QoS handling for WebRTC is FFS.

The following requirements for the signalling plane between WebRTC and IMS are defined:

- The architecture shall support control plane interworking procedures between a WebRTC client and IMS.
- The architecture shall support negotiation to ensure that RTP streams are not multiplexed onto the same port if entities anchoring the session media path in the IMS domain do not support that capability.
- The architecture shall support negotiation to ensure that RTP and RTCP flows of an RTP stream are not multiplexed onto the same port if entities anchoring the session media path in the IMS domain do not support that capability.
- The architecture shall support negotiation of media plane interworking between WebRTC and IMS.
- The architecture shall support negotiation of ICE procedures towards the WebRTC client to enable connectivity checks for establishing the media path.

Editor's note: How the user identification is authenticated is FFS.

The following requirements for the media plane between WebRTC and IMS are defined:

- The architecture shall support transcoding that may be required for audio and video traffic.
- The architecture shall support any necessary interworking between media plane security mechanisms provided by WebRTC and IMS.
- The architecture may support (de)multiplexing of RTP and RTCP flows onto the same port.
- The architecture shall support STUN for ICE connectivity checking.
- The architecture shall support STUN for the WebRTC "consent freshness" feature.

NOTE: Any interworking between disparate media plane procedures require e2ae procedures.

The architecture shall fulfil the following PCC related impacts for WebRTC media transport:

Editor´s note: The support of trickle ICE is FFS.

5 Solutions

Editor's note: The solution description needs to be updated to other agreed requirements.

5.1 Solution 1

5.1.1 Overview

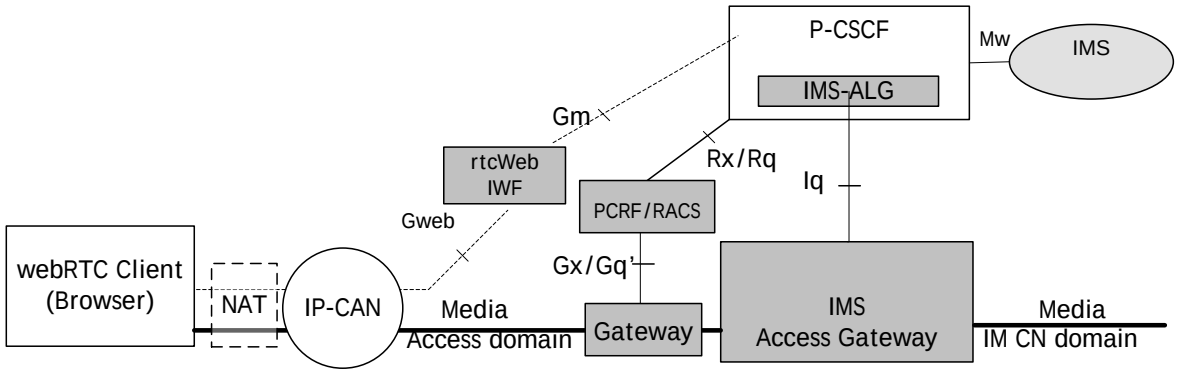


Figure 5.1.1-1: WebRTC access to IMS

In this alternative depicted in Figure 5.1.1-1, the WebRTC client communicates at the control plane with an InterWorking Function (IWF), the rtcWeb IWF, via the Gweb reference point.

The rtcWeb IWF communicates with the P-CSCF via the Gm reference point.

The rtcWeb IWF unit is typically owned by the IMS service provider, but may be owned by a third party as well.

This alternative has the following assumptions:

- The webRTC client has a downloaded Java script that supports the sip webSocket protocol.
- The rtcWeb IWF shall support all the necessary interworking aspects at the control plane to interwork with the P-CSCF.
- The P-CSCF shall support the necessary extensions to support rtcWeb clients.
- All interworking aspects at the media plane, in support of the webRTC client, are implemented within the IMS access gateway, where the media is anchored.

5.1.2 Description of the solution - Procedures

5.1.2.0 General Assumptions

The following assumptions are applicable for this solution:

- The protocol between the webRTC client and IWF is out of cope.
- There is a permanent signalling channel to the IWF/WebRTC client.
- IMS Access Gateway shall support DTLS /SRTP and perform necessary media adaptation.

5.1.2.1 Registration

5.1.2.1.1 WebRTC client-initiated registration

Assumptions

The call flow for this case depicted in Figure 5.1.2.1.1-1 has the following assumptions:

- The WebRTC client is aware of the IMS identity (IMPU) allocated to it as well as the associated credentials. The acquisition of the above by the WebRTC client is out of scope.
- Digest-Based authentication scheme is used between the WebRTC client and IWF, and between IWF and the IMS network.
- The WebRTC client initiates registration.
- The WebRTC has only WebRTC subscription with the IMS service provider.
- The IWF is owned by the IMS service provider.

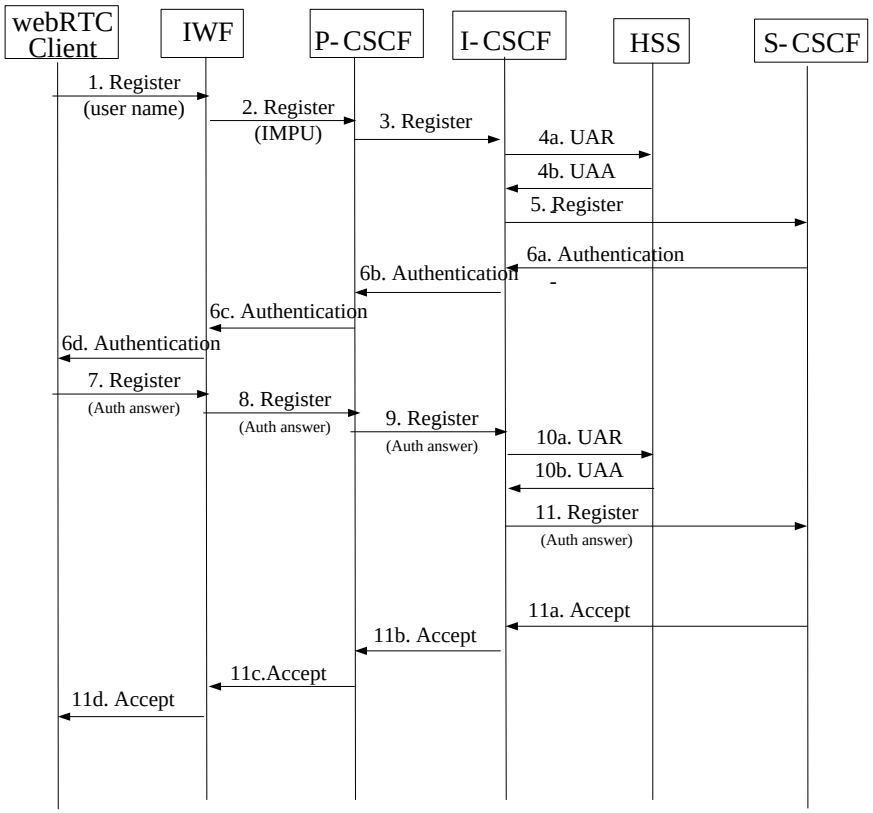


Figure 5.1.2.1.1-1: WebRTC client-initiated IMS registration

The following is a brief description of the steps in the call flow:

- The WebRTC client initiates registration by sending a Register request to the IWF that includes the IMPU as the username.
- Steps 2 to 6c are identical to a regular IMS registration procedure according to TS 24.229 [9].
- In step 6d, the WebRTC client is challenged. Note that in step 4a the I-CSCF derives the IMPI as specified in TS 24.229 [9].
- In step 6d, the WebRTC client is challenged.
- In step 7, the WebRTC client resends the Register Request with the proper authentication information.

- The remaining steps are identical to a regular IMS registration procedure.
- In step 11d, the registration is successful.

5.1.2.1.2 IWF acting as an IP-PBX

In this procedure, the IWF performs third-party registration on behalf of the WebRTC client.

Assumptions

- The IWF is a regular IMS subscriber.
- The WebRTC client has an IMS identity allocated to it by the IWF. The IWF maintains the binding between the WebRTC client user name and the IMS IMPU identity.

The call flow depicted in Figure 5.1.2.1.2-1 illustrates this case.

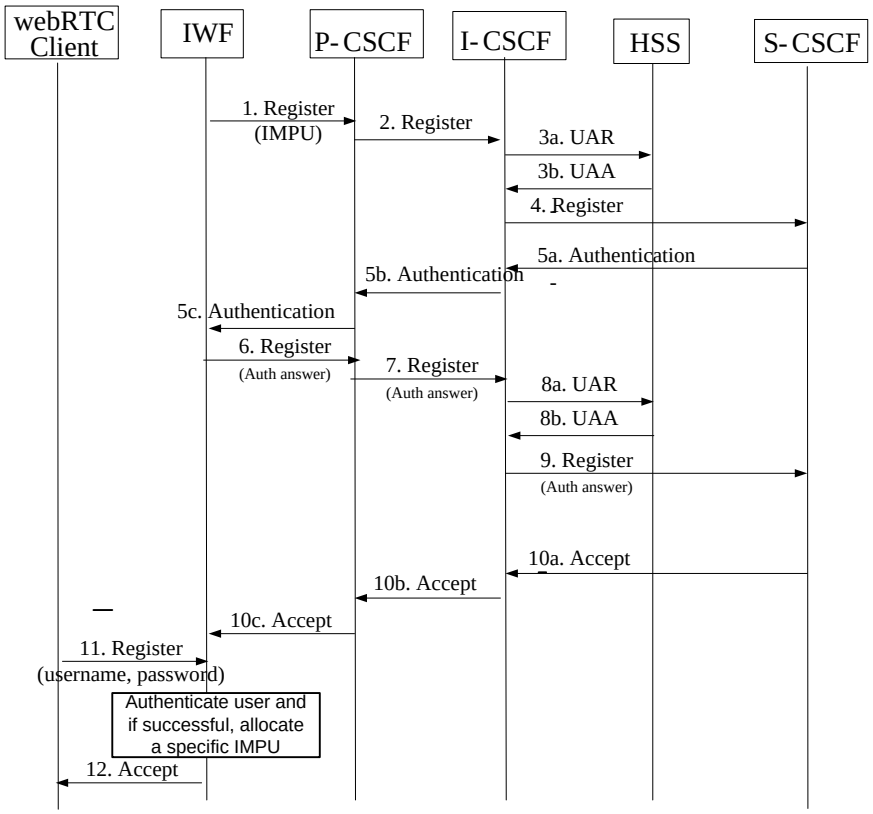


Figure 5.1.2.1.2-1: IWF as an IMS user

The following is a brief description of the steps in the call flow:

- The IWF is a regular IMS user and initiates IMS registration in steps 1 till 10c. These steps are identical to an IMS registration according to TS 24.229 [9].
- In step 10c, the IWF receives the wIMPU allocated to the IWF within the ISR.
- In step 12, the WebRTC client registers with the IWF and includes its username and appropriate credentials, such as a password. These are access related credentials.
- After successful authentication, the IWF creates a binding between the username and the specific IMPU allocated to the WebRTC client. The IWF then sends a success response to the WebRTC client.

Editor's note: It is FFS whether the allocated specific IMPU by the IWF is returned to the WebRTC client.

5.1.2.2 Session handing

5.1.2.2.0 Assumptions

The call flows depicted in Figures 5.1.2.2.1-1, and 5.1.2.2.1-2 assumes the following:

- The P-CSCF is conformant to TS 24.229 [9] clause 5.7.2.7 (IMS-ALG in P-CSCF for support for ICE) and thus performs ICE procedures towards the IWF/WebRTC client. The IMS Access gateway, having via P-CSCF received ICE credentials from the WebRTC client and having sent its own back, intercepts and responds to all ICE STUN messages received from the WebRTC client.
- The IMS Access Gateway shall be able to receive a STUN request for consent freshness and responds to it.
- The IMS Access Gateway shall handle audio/video transcoding.
- The signalling between the WebRTC client and the IWF includes the necessary addressing information to enable ICE connectivity checks to be performed between the WebRTC Client and the IMS Access Gateway.
- The signalling between the WebRTC client and the IWF includes the necessary addressing information to enable STUN consent signalling towards the IMS Access Gateway.

5.1.2.2.1 Handling of outgoing sessions

The call flow depicted in Figure 5.1.2.2.1-1 illustrates this case.

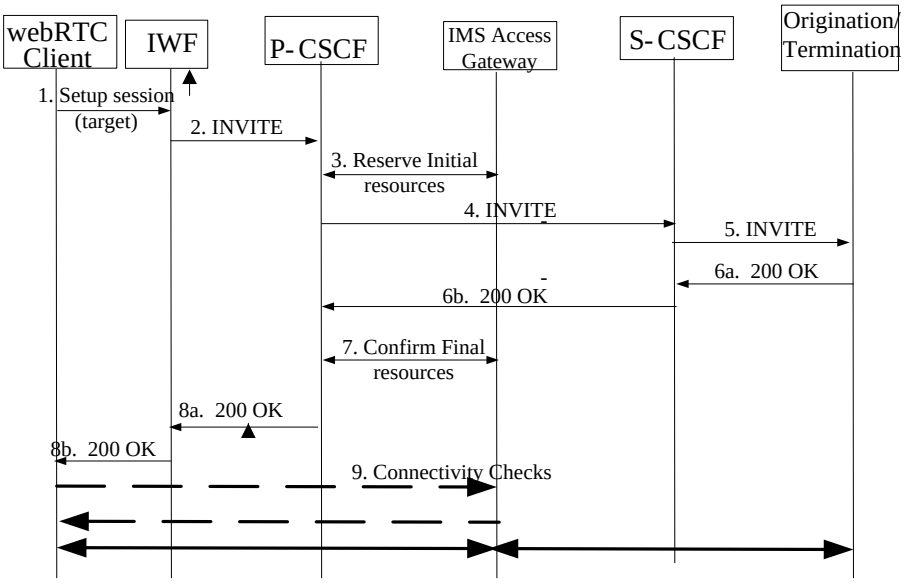


Figure 5.1.2.2.1-1: WebRTC client-outgoing session

The following is a brief description of the steps in the call flow:

- In step 1, the WebRTC client initiates an IMS session by sending a Setup Session request to the IWF that includes the target user.
- Steps 2 to 8 follow regular IMS session setup procedures according to TS 24.229 [9].
- In step8b, the WebRTC client receives a confirmation that session has been accepted. ACK is not shown for brevity.
- In step 9, ICE connectivity checks are being performed.
- Following a successful connectivity check, media can start flowing.

5.1.2.2.2 Handling of incoming sessions

The call flow depicted in Figure 5.1.2.2.1-2 illustrates this case.

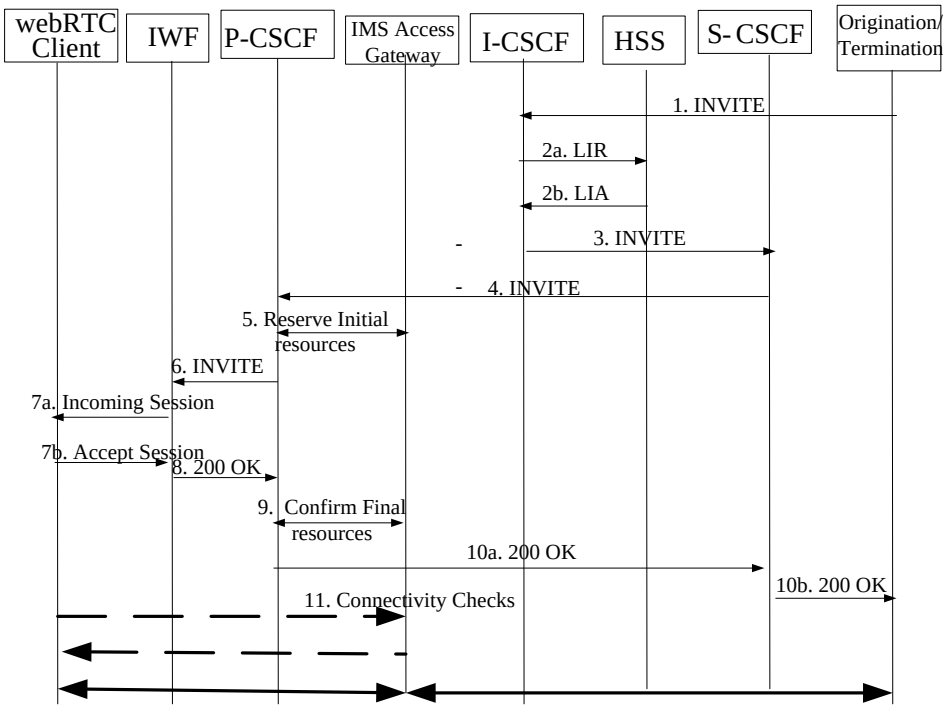


Figure 5.1.2.2.1-2: Incoming session to WebRTC client

The following is a brief description of the steps in the call flow:

- Steps 1 to 6 represent an incoming IMS session to a WebRTC client according to TS 24.229 [9].
- In step 7, the IWF sends an Incoming Session Request to the WebRTC client.
- In step 7b, the WebRTC client accepts the session.
- Steps 9 to 10b follow regular IMS session setup procedure according to TS 24.229 [9].
- In step 11, ICE connectivity checks are being performed.
- Following a successful connectivity check, media can start flowing.

5.1.2.3 Extended role of the P-CSCF to handle interoperability between a WebRTC client and an existing 3GPP UE

To enable the P-CSCF to handle the necessary media adaptation related to WebRTC media traffic to enable interoperability between a WebRTC client and a 3GPP UE, the P-CSCF role has to be extended with the following additional capabilities:

- At reception of an offer from IWF/WebRTC client that includes information that the offerer prefers multiplexing an RTP stream and its related RTCP stream if the answerer also can do this, then the P-CSCF shall downgrade the offer to not indicate preference for such multiplexing.
- At reception of an offer from IWF/WebRTC client that includes information that the offerer prefers multiplexing the offered RTP streams if the answerer also can do this, then the P-CSCF shall downgrade the offer to not indicate preference for such multiplexing.
- The support for DTLS/SRTP.
- The P-CSCF additionally will handle all necessary changes to the SDP offer received from the WebRTC client, if applicable, in accordance with operator policies and supported codecs.

5.1.3 Impact on existing entities and interfaces

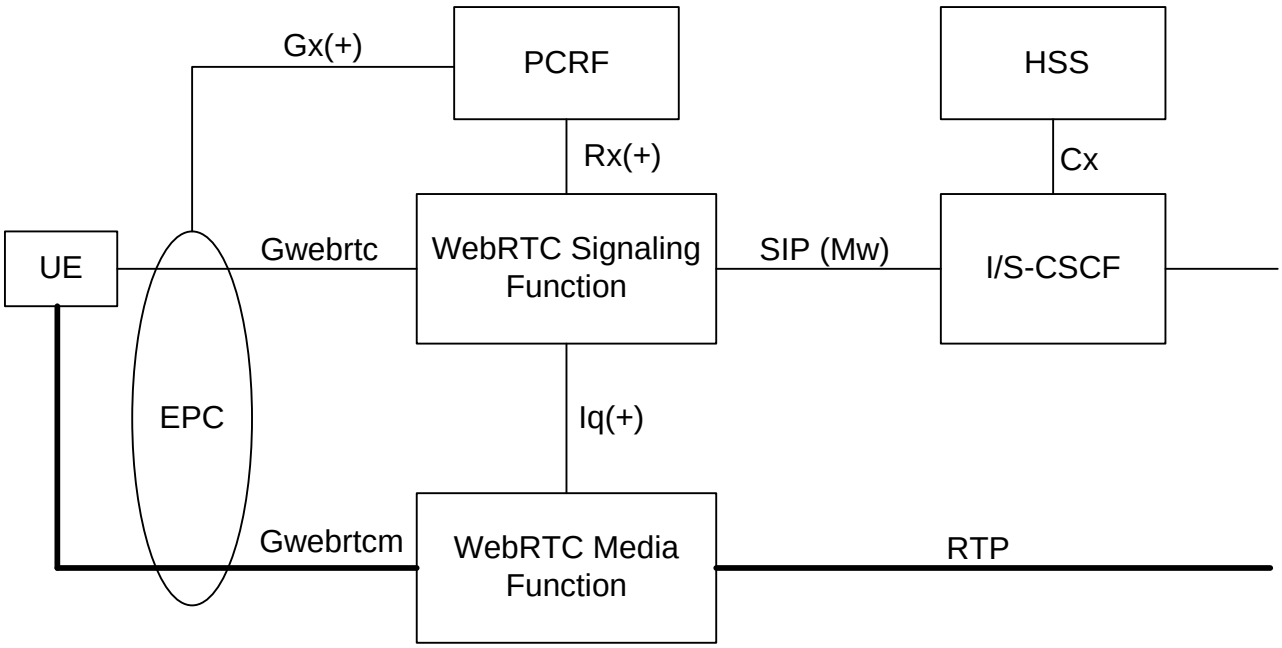
This solution limits the changes to the P-CSCF, in terms of the processing of the offer/answer, and the IMS access media gateway for supporting STUN consent procedures as well as DTLS/SRTP.

5.1.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.2 Solution 2

5.2.1 Overview



NOTE 1: Over the Gwebrtc interface several protocol options are possible, e.g. SIPoWebSockets, REST.
NOTE 2: It is an implementation decision whether to implement the WebRTC Signalling Function as a standalone entity or collocated with an existing entity such as the P-CSCF.
NOTE 3: It is an implementation decision whether to implement the WebRTC Media Function as a standalone entity or collocated with an existing entity such as the IMS-AGW.
NOTE 4: Enhancements to Rx, Gx and Iq interfaces may be required, which is why the figure 5.2.1-2 shows Rx(+), Gx(+) and Iq(+).
NOTE 5: The architecture the uses 3GPP access via EPC, but in principle the architecture supports any IP-CAN. Gx(+) might not be applicably for all IP-CANs.

Figure 5.2.1-1: WebRTC to access IMS services via Mw using EPC

Editor's note: The usage of an I2 interface instead of Mw is FFS.

5.2.2 Description of the solution - Procedures

5.2.2.1 Functions of the WebRTC Signalling Function

The WebRTC Signalling Function provides the following functions:

1. The WebRTC Signalling Function shall perform interworking between the protocol used on the Gwebrtc interface and SIP used on the Mw interface.

NOTE 1: WebRTC does not define a signalling protocol; it just defines that SDP and offer/answer exchanges must be used, such that the endpoints can agree on the actual media flows to be exchanged (see draft-ietf-rtcweb-jsep-03 [3]).

2. SDP mediation

   a. Signalling of RTP multiplexing [6]. The WebRTC Signalling Function shall either negotiate with the UE that RTP multiplexing is not used or shall negotiate RTP multiplexing towards the UE, but not towards the IMS.

   b. Use of the SDP extension for signalling of RTP and RTCP multiplexing [7]. The WebRTC Signalling Function may either negotiate with the UE that RTP and RTCP multiplexing is not used or may negotiate RTP and RTCP multiplexing towards the UE, but not towards the IMS UE.

   c. ICE handling: The WebRTC Signalling Function shall negotiate the usage of ICE with the UE. It is anticipated that procedures similar to those described in TS 24.229 [9] clause 5.7 can be used.

   d. Possible support of trickle ICE signalling [8]. The WebRTC Signalling Function shall either negotiate with the UE that trickle ICE is not used or shall negotiate that trickle ICE is used towards the UE, but not towards the IMS.

Editor's note: The support for trickle ICE (which is not mandatory but speeds up session set-up) is FFS.

   e. Transcoding: The WebRTC Signalling Function may offer transcoding between audio codecs used in the UE and used by the IMS.

NOTE 2: It is up to the operator to offer transcoding in other IMS nodes.

   f. The WebRTC Signalling Function shall configure the WebRTC Media Function according to the negotiated capabilities.

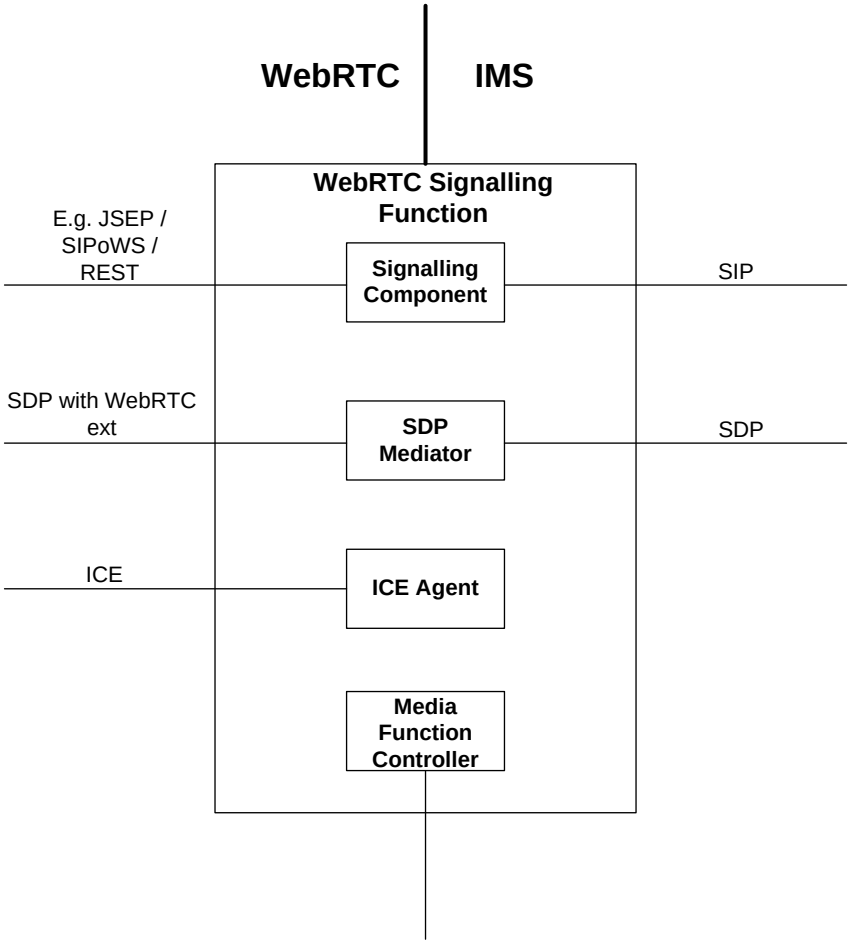


Figure 5.2.2.1-1: WebRTC Signalling Function

NOTE 3: References for JSEP in draft-ietf-rtcweb-jsep-03 [3], SIPoWS in draft-ietf-sipcore-sip-websocket-09 [4], REST in OMA Work Item 0284 [5].

5.2.2.2 Functions of the WebRTC Media Function

The WebRTC Media Function provides the following functions:

1. The WebRTC Media Function may provide transcoding capabilities.

NOTE 1: It is up to the operator to provide transcoding capabilities in other IMS nodes.

2. The WebRTC Media Function may perform RTP multiplexing/de-multiplexing.
3. The WebRTC Media Function shall terminate DTLS-SRTP and mediate towards the RTP variant used in the IMS.
4. The WebRTC Media Function may perform congestion control towards the UE as defined in draft-ietf-avtcore-rtp-circuit-breakers-02 [10] (using "RTP circuit breakers").
5. The WebRTC Media Function shall support STUN usage to signal consent to keep receiving media streams from the remote peer (see draft-muthu-behave-consent-freshness-03 [11]).
6. The WebRTC Media Function shall support STUN connectivity checks.

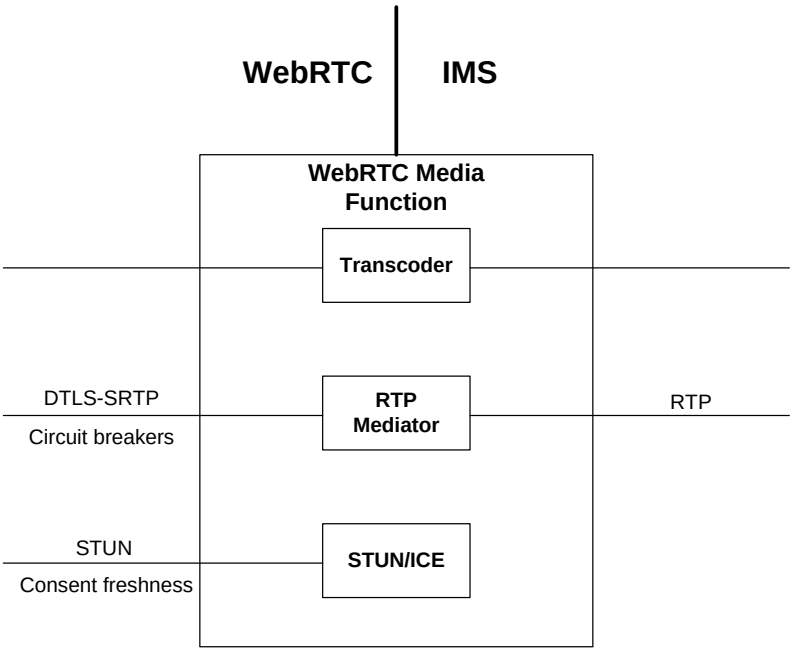


Figure 5.2.2.2-1: WebRTC Media Function

NOTE 2: References for DTLS-SRTP in IETF RFC 5763 [12], Circuit breakers in draft-ietf-avtcore-rtp-circuit-breakers-02 [10], STUN consent freshness in draft-muthu-behave-consent-freshness-03 [11].

5.2.2.3 Functions of the PCC framework

The PCC integration is shown in figure 5.2.1-1 above and following functions are required:

1. The PCC system is used to support the establishment of bearers for real-time media of WebRTC users.
2. The PCC system requires the WebRTC Signalling GW to act as an AF in the sense of the 3GPP PCC architecture and support the Rx interface - or a variant of the Rx interface.

5.2.2.4 IMS registration and authentication

5.2.2.4.0 General

The role of the WebRTC Signalling Function is similar to a P-CSCF. The WebRTC Signalling Function uses the Mw interface towards the IMS.

Editor's note: Third Party WebRTC Signalling Function support needs further study.

Editor's note: The WebRTC Signalling Function needs to be renamed to avoid ambiguity with other solutions.

Two different approaches are described below:

- The WebRTC client uses SIP over WebSockets to register with the IMS.
- The WebRTC client performs authentication with the WebRTC Signalling function and the WebRTC Signalling function performs registration with the IMS.

5.2.2.4.1 Registration: WebRTC client uses SIP over WebSockets

Figure 5.2.2.4.1-1 shows the registration flow where the WebRTC Signalling Function performs message interworking for IMS registration and WebSockets are used between the UE and the WebRTC Signalling Function.

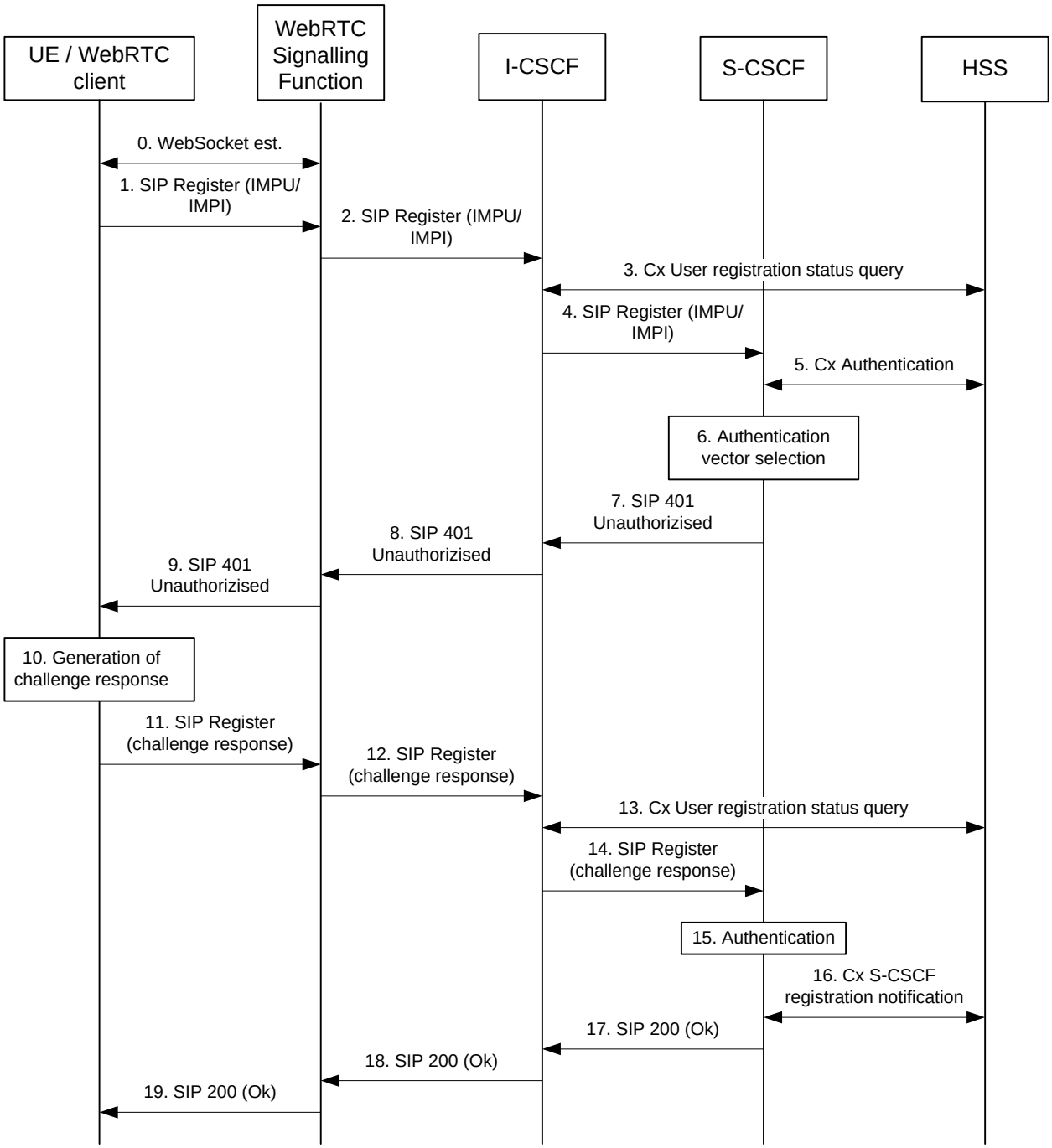


Figure 5.2.2.4.1-1: Registration using SIP over WebSockets (S-CSCF performs authentication)

0. The WebRTC client establishes a secure WebSocket connection with the WebRTC Signalling Function as described in draft-ietf-sipcore-sip-websocket-09 [4].

1. The UE sends REGISTER, containing the IMPI or IMPU towards the WebRTC Signalling Function.

NOTE 1: The browser needs to know the IMPI/IMPU.

Editor's note: Whether the same or a different IMPI/IMPU is used as for regular IMS registration is FFS.

2. The request is being forward from the WebRTC Signalling Function to the I-CSCF in the home domain via Mw. The request requires that sufficient information for authentication in IMS is provided.

NOTE 2: Network specific information that the S-CSCF expects in the REGISTER is the same as for P-CSCF, e.g. visited network identifier, and can be configured.

3. The I-CSCF requests the HSS for information related to the Subscriber registration status. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

4. The I-CSCF forwards the REGISTER request to the selected S-CSCF.

5. As the REGISTER request was sent without integrity protection to the WebRTC Signalling Function, the S-CSCF shall challenge the request and requires the necessary information from the HSS.

6. The S-CSCF selects an authentication vector for use in the authentication challenge according TS 33.203 [14].

7-8. The authentication challenge is sent in the 401 Unauthorized responses towards the WebRTC Signalling Function.

9. The WebRTC Signalling Functions sends the authentication challenge to the UE.

10. Upon receiving the Unauthorized response, the UE extracts the relevant information and calculates the authentication challenge response.

11. The authentication challenge response is sent to the WebRTC Signalling Function.

12. The authentication challenge response is put into the Authorization header and sent back towards the registrar in the REGISTER request.

14. The I-CSCF requests information related to the Subscriber registration status and the HSS returns the S-CSCF name which was previously selected in step 3.

15. The S-CSCF checks the received challenge response. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.

16. The S-CSCF informs the HSS that the user has been registered at this instance.

17-18. The S-CSCF sends a 200 (OK) response to the I-CSCF and the WebRTC Signalling Function indicating that registration was successful.

19. The WebRTC Signalling Function informs the UE that registration was successful.

5.2.2.4.2 Registration: WebRTC client uses Web Authentication

Figure 5.2.2.4.2-1 shows the registration flow where the WebRTC Signalling Function performs message interworking for IMS registration and HTTP is used between the UE and the WebRTC Signalling Function.

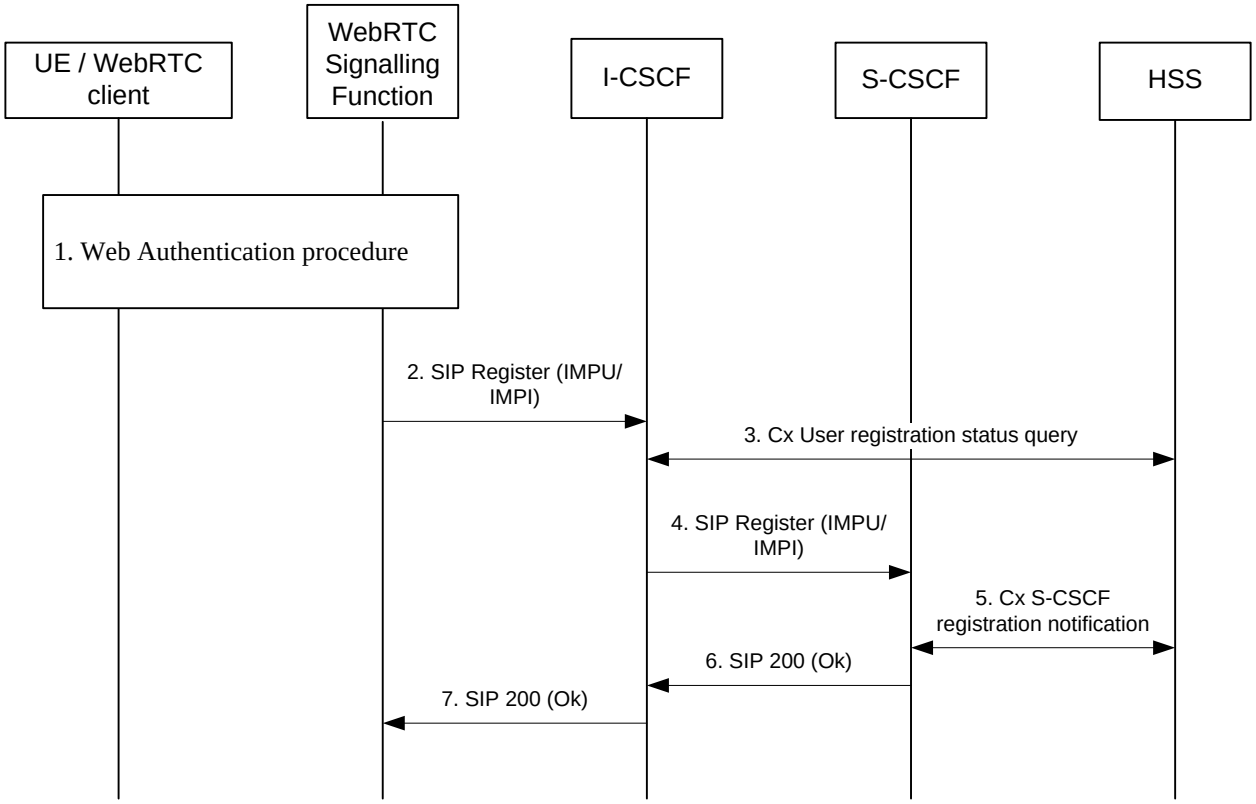


Figure 5.2.2.4.2-1: Registration using Web Authentication (WebRTC Signalling Function performs authentication)

1. The UE starts the web authentication procedure with WebRTC Signalling Function for requesting registration with the IMS (e.g. using HTTP Digest). The UE provides a username/password or an access token; the WebRTC Signalling Function validates them and authenticates the user by means outside the scope of this specification. It maps the user identity obtained during authentication to the corresponding IMS credentials.
2. The WebRTC Signalling Function provides the UA role for SIP REGISTER and determines the IMPI and IMPU assigned to the user (e.g. via a data base query) before sending the REGISTER towards the I-CSCF in the home domain via Mw. In addition the WebRTC Signalling Function indicates that no authentication of the user by the IMS is required as the WebRTC Signalling Function is part of the trust domain.
3. The I-CSCF requests the HSS for information related to the subscriber registration status. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.
4. The I-CSCF forwards the REGISTER request to the selected S-CSCF.
5. As the REGISTER request indicates that the user has already been authenticated the S-CSCF informs the HSS that the user has been registered at this instance.
6. The S-CSCF sends a 200 (OK) response to the I-CSCF.
7. The I-CSCF forwards the response to the WebRTC Signalling Function.

5.2.2.5 Origination and termination

Origination and termination flows for WebRTC IMS clients follow standard IMS procedures with the exception that routing of all messages between the WebRTC IMS client and the S-CSCF traverses the WebRTC Signalling Function instead of the P-CSCF. No further details needs to be described in this clause.

5.2.3 Impact on existing entities and interfaces

Editor's note: Impacts on existing nodes or functionality will be added.

5.2.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.3 Solution 3

5.3.1 Overview

5.3.1.1 Assumptions

In clause 5.3, the word " UE" may correspond to a non-3GPP terminal.

This clause include assumptions specific to this solution and are in addition to those listed in clause 4.1.

- The UE architecture includes a JS execution environment (typically a browser) that supports the WebRTC APIs. The WebRTC IMS client is a JS application that is downloaded from the network as needed.
- For session signalling between the UE and the network, only the information exchange needed to enable the supported options for user identification, authentication and registration in IMS will be standardized.

  Other aspects of the signalling protocol between the UE and the network will not be standardized in Release 12. For example, SIP over WebSockets and RESTful HTTP are two possible options.

NOTE 1: For ease of specification and similarity to Gm, the call flows associated with the architecture assume the use of SIP over WebSockets as the signalling protocol between the client and the network. This does not preclude the use of signalling protocol alternatives.

- The web server hosting and downloading the WebRTC client resides within the home IMS or a supported third party network.

NOTE 2: This restriction is due to the need for a business relationship between the home IMS operator and the third party to ensure use of a compatible client application and to establish the necessary security relationships.

5.3.1.2 Requirements

5.3.1.2.0 Introduction

The following clauses include requirements specific to this solution and are in addition to those listed in clause 4.2. Only the solution requirements in clause 5.3.1.2.4 on user identity and authentication are crucial to the basic architecture. All other solution requirements describe additional capabilities/characteristics of the architecture that can be modified without significantly impacting the basic architecture.

5.3.1.2.1 Supported access networks

- The architecture shall support WebRTC IMS client access from the following access networks:
  - 3GPP access with 3GPP core (EPC or legacy);
  - Non-3GPP access with EPC;
  - Non-3GPP access without EPC (e.g., NSWO).
- For signalling and media via 3GPP or EPC access, the WebRTC IMS client shall be able to use the ("default") APN for "internet".
- The WebRTC IMS client shall be able to function regardless of breakout location (i.e., location of PGW/GGSN) in HPLMN or VPLMN.

5.3.1.2.2 Media processing

- All media plane flows for WebRTC IMS clients shall be anchored in the home IMS for Release 12 to enable e2ae termination of media plane protocols not supported in IMS.

- The architecture shall support the WebRTC IMS client use of the following protocols over DataChannels (as defined for WebRTC) and shall support interworking at the access edge with the transport options supported for these protocols by IMS: MSRP, BFCP and T.140.

5.3.1.2.3 QoS

- The WebRTC IMS architecture shall allow for PCC access and control for the provision of appropriate QoS to WebRTC media flows using the internet APN via 3GPP access networks.

NOTE: Media flows using the internet APN can only receive priority treatment within the access network and not in the internet. While the access network without QoS is usually the largest potential contributor to service problems for media flows, lack of QoS in the internet remains an issue.

5.3.1.2.4 User identity and authentication

- The architecture shall support the option for the WebRTC IMS client to use SIP digest for IMS registration and authentication.

- The architecture shall support the option for the WebRTC IMS client to use a standard web identity/authentication mechanism for IMS registration, with the following characteristics:

  - The architecture shall allow either the IMS operator or an authorized third party to identify and authenticate the user of a WebRTC IMS client for access to IMS.

  - The architecture shall support use of any standard web identity/authentication mechanism that satisfies the security requirements of the IMS operator and/or third party. No particular mechanism will be specified.

  - The architecture shall support assignment of IMS identities to a WebRTC IMS client based on the corresponding authenticated web identity. The assigning entity shall only be able to assign valid IMS identities allocated to it by the IMS. The method of assigning IMS identities is a matter of local policy for the assigning entity.

5.3.1.2.5 Service architecture

- In addition to the support of services provided by IMS, the architecture shall allow for a third party to optionally provide communication services that do not require third party bearer plane processing.

5.3.1.2.6 Subscriber data management

NOTE: No special provisions are needed for WebRTC IMS client subscriber data management since the client can use HTML-based Ut procedures.

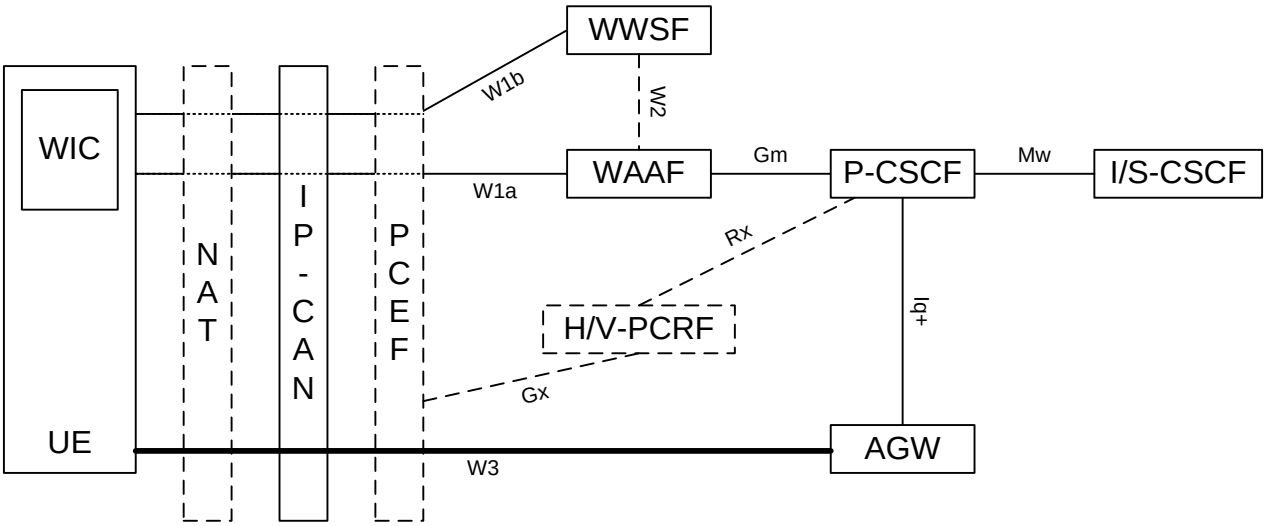
5.3.1.3 Signalling architecture

Figure 5.3.1.3-1 shows the WebRTC IMS signalling architecture. The WWSF (WebRTC web server function) is located either within the home IMS or within a third party network and is the first web server contacted by the user (generally by clicking on a link or entering a URL into the browser). The WAAF (WebRTC Access Aggregator Function) is the endpoint for the signalling connection from the client and is usually located in the home IMS but can also be located in the third party network if the WWSF is also located in the third party network.

NOTE 1: All network entities shown are functional entities and are not intended to suggest any physical realization. Individual functional entities (e.g., WWSF, WAAF, and existing IMS functions) may be co-located in any reasonable combination depending on the absence/presence of a third party.

NOTE 2: The presence of dashed elements in the figure depends on the configuration. The W2 reference point is only applicable to the web identity/authentication scenario in scenario 3 of clause 5.3.2.1.1.
PCC functional elements are present only for 3GPP access with QoS.

The corresponding PCC elements for fixed access are also optionally supported but not shown.
The NAT in figure 5.3.1.3-1 is meant for the access to IMS over a Wireline Access.



NOTE: W1a and W1b are not meant to be specified.
W3 corresponds to the output of the IETF RTCWEB discussions.
Whether W2 will be subject to specifications is still FFS.

Figure 5.3.1.3-1: WebRTC IMS signalling architecture

Editor's note: It is FFS if Gm as shown in the figure conforms to current specifications.

5.3.1.4 Functional entities

5.3.1.4.1 WIC (WebRTC IMS Client)

A WebRTC IMS Client (WIC) is a WebRTC JS application capable of interoperating with the WebRTC IMS access architecture defined herein. The WIC application is downloaded from a web server within the home IMS or a third party network and provides access to the communications services of the IMS. The WIC shall function on any device supporting a browser (or equivalent JS execution environment) with WebRTC extensions via any IP access network with internet access, subject to the QoS and reachability limitations of the access network.

5.3.1.4.2 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 user. The WWSF has the following characteristics and functions:

- The WWSF is located either in the home IMS or a third party network authorized by the home IMS;
- The WWSF provides the web page presenting the user interface to the user for IMS access;
- The WWSF provides for the downloading of the JS WIC application to the browser on the UE;
- If the WIC does not enforce the use of IMS digest authentication for the user, the WWSF arranges for identification and authentication of the user using web procedures;
- The WWSF manages the correct and consistent allocation of authorized IMS identities to WICs associated with authenticated web identities;

5.3.1.4.3 WAAF (WebRTC Access Aggregator Function)

The WebRTC Access Aggregator Function (WAAF) is the network server terminating the signalling protocol (e.g., SIP over WSS) from the WIC. The WAAF has the following characteristics and functions:

- The WAAF is usually located in the home IMS but can be located in an authorized third party network if the WWSF is also in the third party network;
- The WAAF aggregates signalling traffic (e.g. SIP over WSS) from multiple WICs towards the P-CSCF (e.g. in scenario 3 of clause 5.3.2.1.1);
- The WAAF can act as the SIP registrar for WICs that are allocated IMS identities by a third party from wildcard identities assigned to the third party;
- The WAAF verifies the correct allocation of IMS identities by a third party;
- When located in a third party network, the WAAF can optionally provide communication services to the WIC in addition to those provided by IMS.

5.3.1.4.4 P-CSCF

The P-CSCF is enhanced to control the AGW functions needed to adapt the WIC bearer flows for IMS.

The P-CSCF is enhanced with the following characteristics and functions to support WICs:

- The P-CSCF resides in the home IMS;
- The P-CSCF maintains secure transport connections to known WAAF entities in the home and third party networks;
- The P-CSCF controls the media plane interworking functions provided by the AGW, including those additional media plane functions specific to WebRTC.

5.3.1.4.5 AGW (Access GateWay)

The AGW is enhanced to provide media plane interworking as needed for WICs.

The AGW has the following additional characteristics and functions:

NOTE 1: WebRTC only supports audio and video media using RTP transport, and data media using WebRTC DataChannels. Hence any media plane protocol other than audio and video must use WebRTC DataChannels or HTTP for transport.

- The AGW resides in the home IMS.
- The AGW performs e2ae procedures for media protocols specific to WebRTC, including ICE, media consent, and DTLS-SRTP.
- The AGW performs any transcoding needed for audio and video codecs supported by the browser.
- When GTT service is requested, the AGW performs transport level interworking between T.140 over DataChannels and other T.140 transport options supported by IMS.
- When MSRP is requested, the AGW performs as an MSRP B2BUA between MSRP over DataChannels and the other MSRP transport options supported by IMS.

NOTE 2: IETF RFC 6714 [15] describes the CEMA (Connection Establishment for Media Anchoring) MSRP extension to enable the use of transport-only relays between MSRP endpoints. Without the CEMA extension, an MSRP endpoint shall signal an URI or path of URIs through which it is reachable. As described in IETF RFC 6714 [15], since IMS does not require support of CEMA for MSRP nodes, the architecture requires an MSRP B2BUA to interwork an endpoint using MSRP over DataChannels with endpoints using other MSRP transport options.

- When BFCP service is requested for conference floor control, the AGW performs transport level interworking between BFCP over DataChannels and other BFCP transport options supported by IMS.

5.3.1.5 Reference points

5.3.1.5.1 W1a (UE to WAAF)

The W1a reference point is between the UE (with a browser running a WIC application) and the WAAF. Across this reference point, only the information exchanges required for user identification, authentication and IMS registration are specified. The signalling protocols on this interface are otherwise not specified in Release 12 but all procedures shown are based on the use of SIP over WSS.

5.3.1.5.2 W1b (UE to WWSF)

The W1b reference point is between the UE and the WWSF. HTTPS is normally used to access the web page providing the UI for the WIC and to download the WIC JS application to the browser. Across this reference point, only the information exchanges required for user identification, authentication and IMS registration are specified.

5.3.1.5.3 W2 (WWSF to WAAF)

The W2 reference point is between the WWSF and WAAF. W2 is only used in support of third party web identity and authentication, as described in scenario 3 of clause 5.3.2.1.1. W2 provides for the WWSF to register its presence with a WAAF so that the WWSF can authorize WICs to contact the WAAF. W2 is expected to be based on HTTPS.

5.3.1.5.4 Gm (WAAF to P-CSCF)

The Gm reference point is enhanced for application to WebRTC IMS access between the WAAF and the P-CSCF.

Gm provides for transport of SIP messages between a WAAF and a P-CSCF for all WICs managed by the WAAF.

Gm is secured using network domain security procedures using IPSEC or TLS.

5.3.1.5.5 Iq+ (P-CSCF to AGW)

The Iq reference point is between the P-CSCF and AGW and is enhanced to control the additional bearer plane functions specific to WebRTC clients.

5.3.1.5.6 W3 (UE to AGW)

The W3 reference point is between the UE and AGW.

W3 carries the user plane between the UE and the network (see clause 5.3.1.6).

5.3.1.6 Media plane protocol architecture

5.3.1.6.0 General

The AGW is the media plane interworking element with the functions described in clause 5.3.1.4.5.

The AGW provides e2ae media procedures for ICE, periodic consent, DTLS-SRTP, transcoding, and DataChannels as needed in support of MSRP, BFCP and T.140.

DataChannel transport is selected over other available HTTP-based options for transport of all non-audio and non-video media plane protocols to avoid one or more of the following limitations:

- HTTP transport options typically will not allow setup of direct transport connections between peers due to possible presence of NAT/firewall and probable lack of DNS entries for the endpoints.
- The forced insertion of an intermediary removes the option of providing end-to-end media security.
- Since HTTP transport options are typically not signalled using SDP, a gateway will need to provide in-band to out-of-band signalling interworking for interoperation with legacy servers and endpoints that do not support the transport option.

- Some HTTP transport options have functional restrictions compared to the standard end-to-end media transport options. For example, MSRP file transfer using Restful APIs requires temporary file storage at an intermediary rather than direct peer-to-peer file transfer.
- WebRTC mechanisms for ICE, media security, media endpoint identification and media multiplexing are only available for audio media, video media and DataChannels.

5.3.1.6.1 Protocol architecture for MSRP

Figure 5.3.1.6.1-1 shows the protocol architecture for support of MSRP from a WebRTC IMS client.

The AGW provides an MSRP B2BUA to allow interoperation with existing MSRP peer endpoints.

Use of TLS between the AGW and peer is optional, as indicated by an asterisk (*) in the figure.

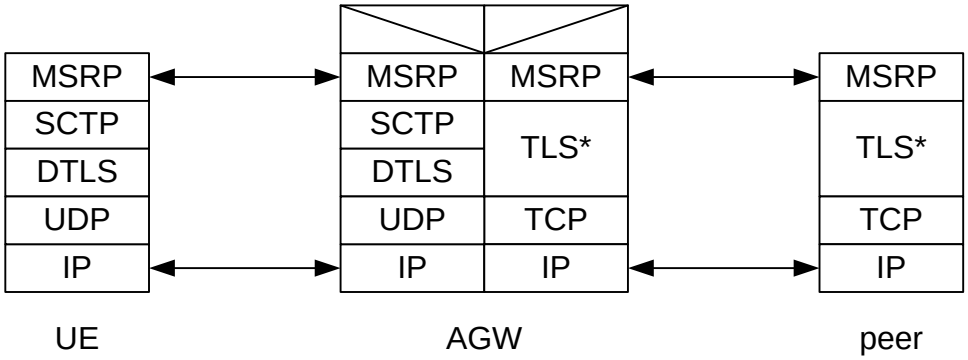


Figure 5.3.1.6.1-1: Protocol architecture for MSRP

5.3.1.6.2 Protocol architecture for BFCP

Figure 5.3.1.6.2-1 shows the protocol architecture for support of BFCP from a WebRTC IMS client.

The AGW provides a transport relay function from DataChannel to TLS/TCP to allow interoperation with existing BFCP peer endpoints. Use of TLS between the AGW and peer is optional, as indicated by an asterisk (*) in the figure.

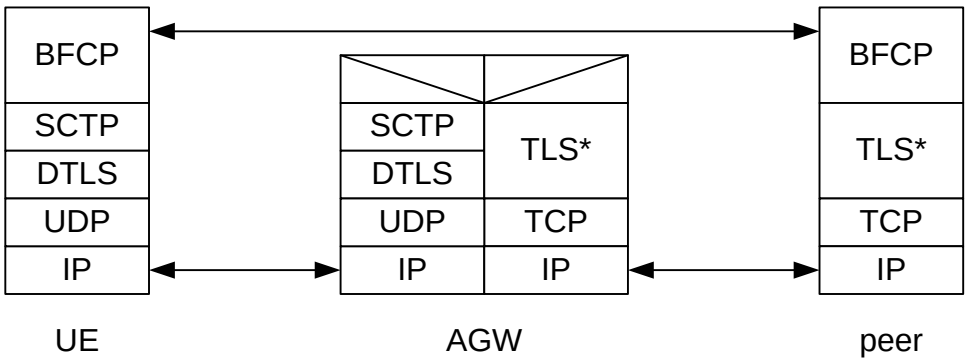


Figure 5.3.1.6.2-1: Protocol architecture for BFCP

5.3.1.6.3 Protocol architecture for T.140

Figure 5.3.1.6.3-1 shows the protocol architecture for support of T.140 from a WebRTC IMS client.

The AGW provides a transport relay function from DataChannel to RTP/SRTP to allow interoperation with existing T.140 peer endpoints. Use of SRTP between the AGW and peer is optional as an alternative to RTP.

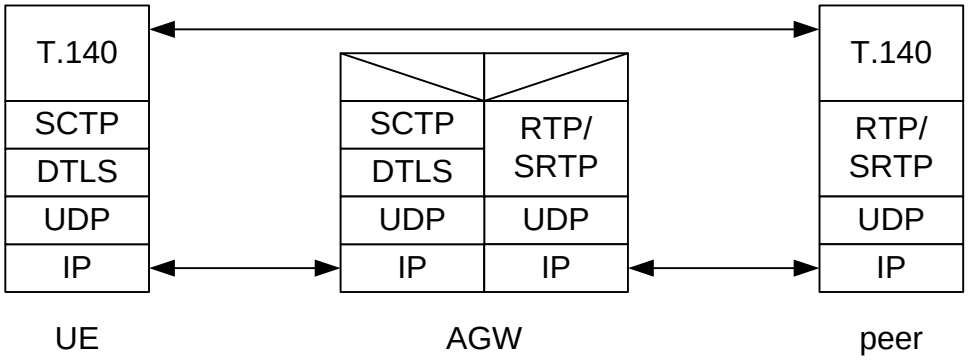


Figure 5.3.1.6.3-1: Protocol architecture for T.140

5.3.1.6.4 Protocol architecture for Voice and Video

Figure 5.3.1.6.4-1 shows the protocol architecture for support of Voice and Video from a WebRTC IMS client. Transcoding (whether codec1 is different from codec2) is optional.

SRTP between the UE and the AGW relies on keying material negotiated via DTLS.

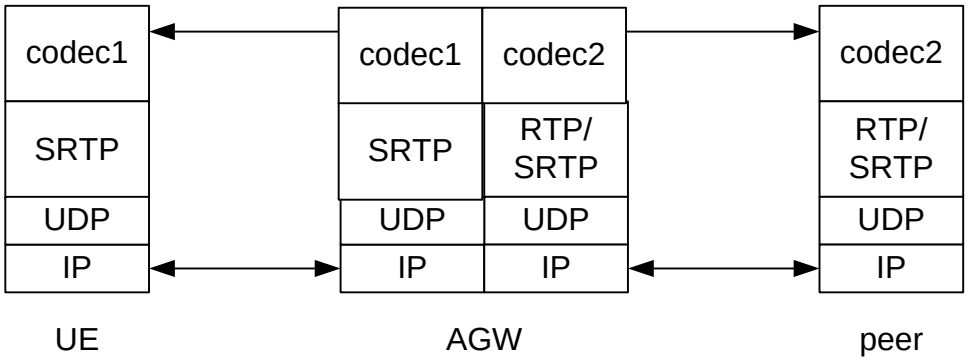


Figure 5.3.1.6.1-1: Protocol architecture for Voice and Video

5.3.2 Description of the solution - Procedures

5.3.2.1 Registration

5.3.2.1.1 Introduction

The WebRTC IMS architecture supports three different IMS registration scenarios that differ in the authentication method, type of IMPU being registered (i.e., with separate HSS entry or as a member of a wildcard IMPU range), and ownership of the WWSF and WAAF (i.e. home IMS or third party).

Scenario 1: The user has a subscription with an individual IMPU and uses IMS digest to authenticate with IMS. The WAAF is located within the home IMS and the home IMS trusts the WWSF to perform its services. Clause 5.3.2.1.2 provides detailed procedures for scenario 1.

Scenario 2: The user has a subscription with an individual IMPU but uses a web identity and authentication scheme to authenticate with the WWSF. The WWSF assigns IMS identities to the user based on the user's web identity (e.g., via database lookup or other translation). The WAAF is located within the home IMS and the home IMS trusts the WWSF to perform its services. Clause 5.3.2.1.3 provides detailed procedures for scenario 2.

Scenario 3: The user uses a web identity and authentication scheme to authenticate with the WWSF. The WWSF is located in a third party network and has a subscription with IMS for a wildcard IMPU. The WAAF registers the wildcard IMPU with IMS on behalf of the WWSF. The WWSF assigns an IMS identity to each individual user from its assigned wildcard IMPU. The WAAF acts as the SIP registrar for WICs assigned individual IMPUs from the wildcard IMPU range. The WAAF can be located either in the home IMS or a third party network. Clauses 5.3.2.1.4 and 5.3.2.1.5 provide detailed procedures for scenario 3.

5.3.2.1.2 WIC registration of individual IMPU with IMS using IMS digest

To support WIC registration using IMS digest, the WAAF must be located in the home IMS.

The home IMS trusts the WWSF to provide the WIC application and redirect the WIC to the WAAF for service.

The user enters information needed for IMS registration (e.g. IMPI and IMPU) to the WIC via unspecified means.

For example, this information might be stored in cookies or local browser storage after visiting a secure web site provided by the IMS operator.

NOTE: The WAAF is restricted to being located in the home IMS for this scenario to avoid the potential for a man-in-the-middle attack via a compromised third party WAAF.

Figure 5.3.2.1.2-1 shows a registration call flow where IMS digest is used to register the WIC.

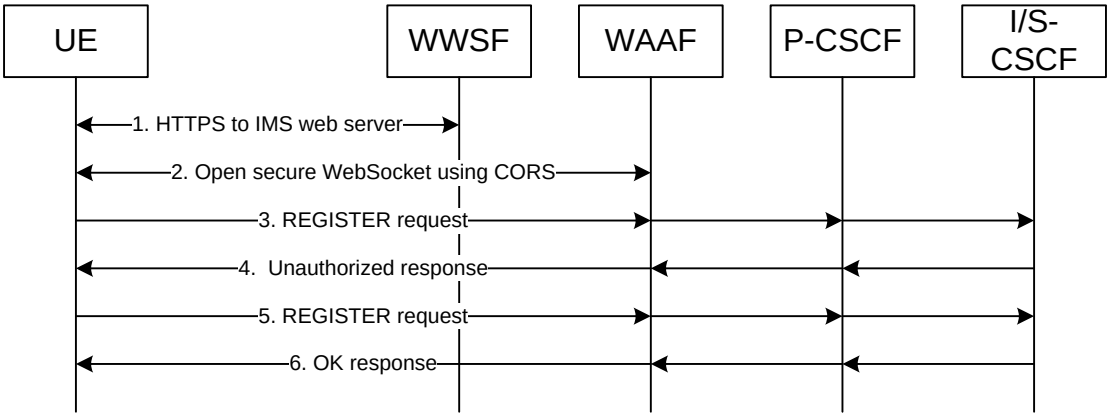


Figure 5.3.2.1.2-1: WIC registration of individual IMPU with IMS using IMS digest

1. From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF.

2. The WIC opens a WSS connection to the WAAF using standard cross-origin resource sharing (CORS) procedures to ensure that the WIC originated from a WWSF authorized to access this WAAF.

3-6. The WIC initiates a registration transaction with IMS via the WAAF by sending a REGISTER request to the WAAF via the WSS connection. The REGISTER request includes IMS Digest authentication parameters, IMPI, IMPU and other information as needed for proper IMS registration. This request is translated in the IMS Core into an IMS registration process. This process leverages user credentials in HSS.

5.3.2.1.3 WIC registration of individual IMPU with IMS based on web authentication

To support WIC registration based on web authentication, the WAAF located in the home IMS trusts the WWSF to authenticate and assign IMS identities to the WIC. The WWSF belongs to the operator or to a trusted Third party

NOTE: The WAAF is restricted to being located in the home IMS for this scenario since IMS must trust the authentication-less REGISTER requests from the WAAF in step 4 below.

Figure 5.3.2.1.3-1 shows a registration call flow where the WIC registers with IMS based on web authentication with the WWSF.

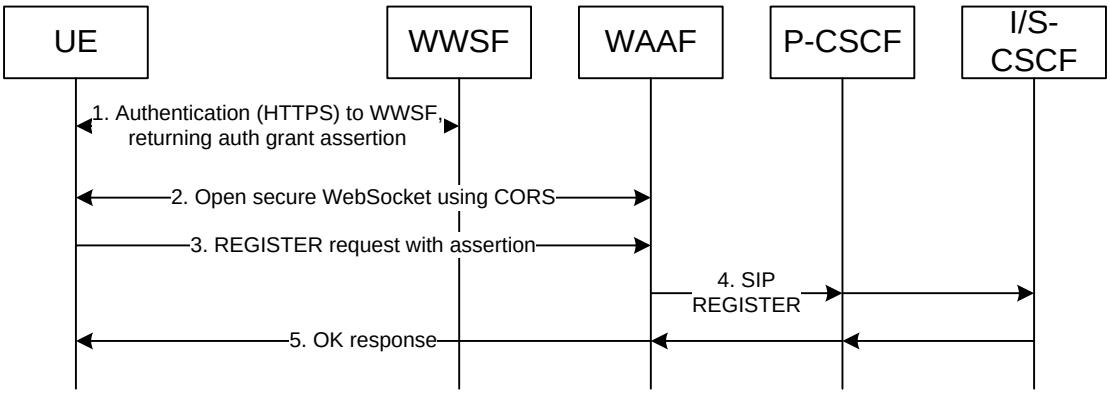


Figure 5.3.2.1.3-1: WIC registration of individual IMPU based on web authentication

1. From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF. The WWSF authenticates the user using a common web authentication procedure, determines the IMPI and IMPU assigned to the user (e.g. via an LDAP query to an identity database {not shown} using the authenticated identity as key), issues a security token for the user (e.g. where the security token is a JSON Web Token) and returns the IMS identities as claims within the security token to the WIC.

2. The WIC opens a WSS connection to the WAAF using CORS procedures (http://www.w3.org/TR/cors/, http://www.w3.org/wiki/CORS_Enabled#What_is_CORS_about.3F) to ensure that the WIC originated from a WWSF authorized to access this WAAF.

3. The WIC sends a REGISTER request to the WAAF via the WSS connection. The request includes the user identity extracted from the claims in the security token, as well as the security token received from the WWSF as an attachment to the request.

4. The WAAF validates the contents of the security token and confirms that the IMS identities being registered are authorized by the security token. The WAAF then forwards the authorized REGISTER request to IMS via the P-CSCF to initiate authentication-less IMS registration. As the P-CSCF trusts the WAAF, it forwards the registration with an indication that the authentication has already been carried out

5. IMS returns a OK response to the WIC to confirm the successful IMS registration.

5.3.2.1.4 WAAF registration of wildcard IMPU with IMS on behalf of WWSF

In scenario 3, the WWSF obtains control of a wildcard IMPU range from which it can assign individual IMPUs to WICs. The WWSF is usually located within a third party network authorized by the IMS operator to grant WICs access to IMS using the allocated IMS identities. The WAAF acts as the SIP registrar for all WICs using IMS identities from the assigned wildcard IMPU range. The WAAF registers each wildcard IMPU range with IMS using either static mode or registration mode (a la IMS business trunking) so that individual WICs can receive service based on the registration of the wildcard IMPU. The WAAF can be located in either the IMS operator network or a third party network as long as access to service based on the assigned identities is appropriately verified and restricted.

NOTE: WAAF location in a third party network can enable the third party network to offer communications services in addition to those offered by the IMS. Extra security precautions are needed to ensure proper assignment of identities to WICs and proper IMS service authorization. The definition of third party services that a WAAF might offer is out of scope.

Figure 5.3.2.1.4-1 shows a registration flow where the WWSF requests the WAAF to register a wildcard IMPU range on its behalf with IMS.

2 modes are described:

- A static mode where the IMS identities (wildcard IMPU range) associated with the WWSF are pre- registered (on IMS) by configuration and the WAAF interfaces an IBCF;

- A registration mode where the IMS identities (wildcard IMPU range) associated with the WWSF are dynamically registered on IMS and the WAAF interfaces a P-CSCF.

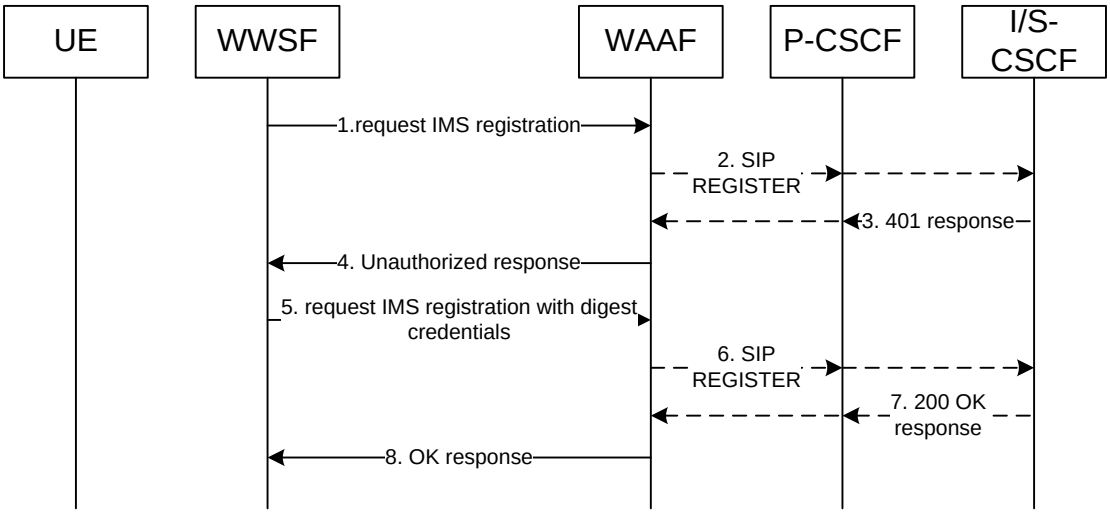


Figure 5.3.2.1.4-1: WAAF registration of wildcard IMPU on behalf of WWSF

1. The third party WWSF establishes a TLS connection to the WAAF with bilateral authentication based on server certificates. The WWSF sends a message to the WAAF requesting that the WAAF register on its behalf with IMS. The message includes the block of IMS identities associated with the WWSF that are to be delegated to the WAAF and IMS digest authentication parameters.

2. In the static mode case, the associated IMS identities are already registered with IMS by configuration, so the WAAF bypasses steps 2 and 3, and continues with step 4. In registration mode, the WAAF initiates an IMS registration transaction by sending a SIP REGISTER request to the P-CSCF and S-CSCF to register the block of IMS identities asserted by the WWSF.

3. In registration mode, the S-CSCF returns a digest challenge to the WAAF.

4. In static mode, the WAAF directly challenges the request in step 1. In registration mode, the WAAF forwards the challenge received from the S-CSCF in step 3.

5. The WWSF resends the IMS registration request to the WAAF with the IMS digest credentials.

6. In registration mode, the WAAF sends another SIP REGISTER request to the P-CSCF and S-CSCF that includes the IMS digest credentials from the WWSF.

7. In registration mode, the S-CSCF responds with a SIP 200 OK response if the credentials are accepted.

8. In static mode, the WAAF verifies the credentials from the WWSF directly. In registration mode, the WAAF waits for successful IMS registration. After success in either case, the WAAF sends an OK response to the WWSF to confirm that the WAAF has successfully registered the block of IMS identities with IMS on behalf of the WWSF.

5.3.2.1.5 WIC registration of individual IMPU from wildcard IMPU range

The WWSF that obtains control of a wildcard IMPU according to the procedure in clause 5.3.2.1.4 can assign individual IMPUs from the wildcard range to WICs under its control. This scenario takes place after the scenario of clause 5.3.2.1.4 and corresponds to the same business arrangement.

Figure 5.3.2.1.5-1 shows the registration flow for a WIC being assigned an individual IMPU from a wildcard IMPU range assigned to the WWSF.

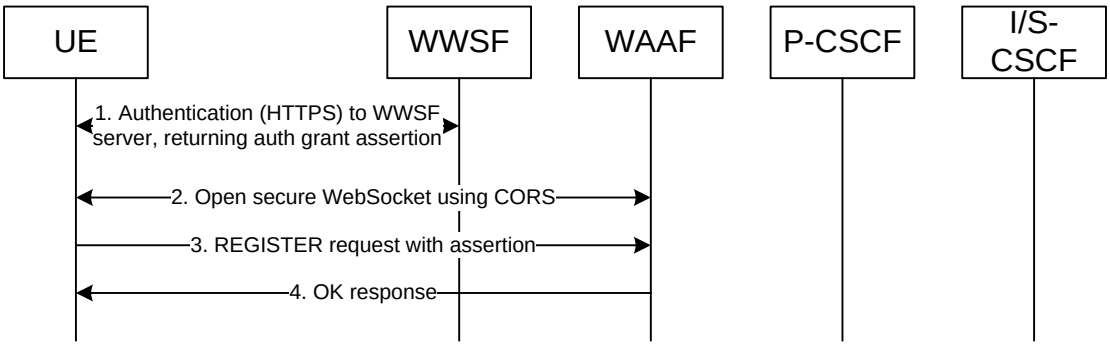


Figure 5.3.2.1.5-1: WIC registration of individual IMPU from wildcard IMPU range

1. From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the third party server based on the server certificate. The browser downloads and initializes the WIC from the WWSF. The WWSF may authenticate the user via unspecified means, assigns IMPI and IMPU to the user from those identities that the IMS operator has assigned to the WWSF, issues a security token for the user (e.g., where the security token is a JSON Web Token) and returns the IMS identities as claims within the security token to the WIC. Unauthenticated users are anonymous to the third party but may still be authorized for IMS service.

2. The WIC opens a WSS connection to the WAAF using CORS procedures to ensure that the WIC originated from a WWSF authorized to access this WAAF.

3. The WIC sends a REGISTER request to the WAAF via the WSS connection. The request includes the IMPI and IMPU in the security token, received from the WWSF as an attachment to the request.

4. The WAAF validates the contents of the security token and confirms that the IMS identities being registered are authorized by the security token. The WAAF also verifies that the IMS identities being registered are assigned to the third party based either on 1) configuration data identifying the IMPUs associated with the third party that the WWSF is allowed to assign to users accessing IMS via the WAAF (e.g., static mode operation) or 2) explicit prior WWSF request for the WAAF to perform IMS registration of a block of IMPUs on behalf of the third party (i.e., registration mode operation). The WAAF then returns a OK response to the WIC to confirm successful registration.

5.3.2.2 Origination and termination

Origination and termination flows for WebRTC IMS clients follow standard IMS procedures with the exception that routing of all messages between the WIC, P-CSCF and S-CSCF also traverse the WAAF and that parameters of Iq procedures take into account the specificities of the procedures used by the WIC to send media. No further details are necessary.

5.3.3 Impact on existing entities and interfaces

The primary functions impacted are the P-CSCF and AGW, as described in clause 5.3.1.4.4 and 5.3.1.4.5, respectively. The primary reference points impacted are Gm and Iq, as described in clause 5.3.1.5.4 and 5.3.1.5.5, respectively. Authentication-less IMS registration as described in clause 5.3.2.1.1 scenario 2 should be able to re-use signalling already defined for registration in the I2 case (see Trusted Node Authentication (TNA) in TS 33.203 [14]). Small changes might be needed in the S-CSCF and related reference points to support the new WebRTC access type.

5.3.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.4 Solution 4

5.4.1 Overview

5.4.1.1 Reference architecture model

Figure 5.4.1.1-1 represents the IMS_WebRTC reference architecture including interfaces between entities. Detail description of the roles of these nodes can be found in subsequent clauses.

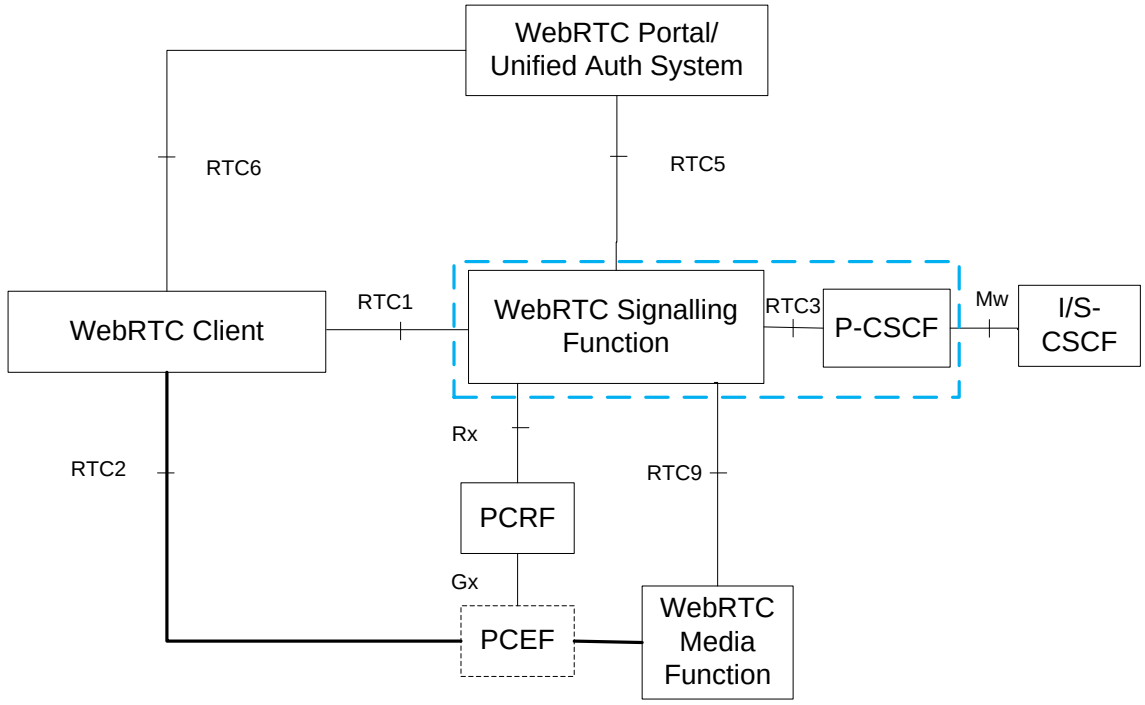


Figure 5.4.4.1-1 High level architecture for IMS_WebRTC

NOTE: The WebRTC Client can be co-located with an IMS client (i.e. on an IMS UE) or standalone on a device that does not support IMS UE functionality.

5.4.1.2 Reference points

RTC1 Reference point between a WebRTC client and a WebRTC Signalling Function. It is used to define the signalling plane interaction between WebRTC client and WebRTC Signalling Function.

RTC2 Reference point between a WebRTC client and a WebRTC Media Function. It is used to define the Media plane interaction between WebRTC client and WebRTC Media Function.

RTC3 Reference point between a WebRTC Signalling Function and a P-CSCF. It is used to define the interactions between a WebRTC Signalling Function and the IMS.

NOTE: RTC3 is not required if the WebRTC Signalling Function is incorporated with P-CSCF functionality.

RTC5 Reference point between a WebRTC Signalling Function and a WebRTC Portal/Unified Auth System. It conveys the user information stored in WebRTC portal/Unified Auth System to WebRTC Signalling Function .

RTC6 Reference point between a WebRTC client and a WebRTC portal/Unified Auth System. It is used to support the authentication of user identity provided by the WebRTC Client.

RTC9 Reference point between a WebRTC Signalling Function and a WebRTC Media Function. It is used by WebRTC Signalling Function to control WebRTC Media Function.

5.4.1.3 Functional entities

5.4.1.3.1 WebRTC Signalling Function

The WebRTC Signalling Function resides in the IMS operator network, as IMS interfacing functionality to the WebRTC client, has a reference point towards I-CSCF/S-CSCF (WebRTC Signalling Function is incorporated with P-CSCF) or P-CSCF (WebRTC Signalling Function is a standalone entity), and the WebRTC client.

The functionality includes but is not restricted to:

- Convert the signalling received from WebRTC client (e.g. HTTP/HTTPS/Websocket signalling) to SIP signalling, and then forward the SIP request towards the IMS.
- Support ICE procedures on SDP offer/answer negotiation.
- Implement a limited STUN server functionality to support the STUN keep-alive usage as defined in IETF RFC 5389 [16] which is used by the UE to maintain the NAT bindings. (Similar to the STUN function provided by P-CSCF).
- Communicate with Policy and Charging Rules Function (PCRF) by Rx interface to authorize the bearer resources and manage QoS.
- Communicate with Web portal/Unified Auth System to verify user authorization and retrieve IMS identities (e.g. IMPU that stored in Web portal/Unified Auth System).
- Support of forwarding the message to UE in terminating case.
- Support existing P-CSCF functionality when RTC3 is removed (i.e. when WebRTC Signalling Function is incorporated with P-CSCF).
- Support the registration with IMS on behalf of the user.

5.4.1.3.2 WebRTC Media Function

The functionality of WebRTC Media Function includes but is not restricted to:

- Convert the voice and video media between SRTP and RTP.
- Convert non-voice/video media between data channel/WebSocket and MSRP.
- Support codec transcoding.
- Support ICE procedures on connectivity check.

5.4.1.3.3 WebRTC portal/Unified Auth System

The WebRTC portal/Unified Auth System is functionality that may be provided by the IMS network operator or alternatively by a Third party service provider. The WebRTC portal/Unified Auth System in the network has reference points towards the WebRTC Signalling Function and the WebRTC client. The functionality includes but is not restricted to:

- Authenticate the user identification and then generate user security information (e.g. Token) for access control.
- Validate user security information sent from the WebRTC Signalling Function. The WebRTC portal/Unified Auth System provides the WebRTC Signalling Function with additional user information (e.g. IMPU) to map to the user identity used by the WebRTC client in the case where the WebRTC client uses an identity different from IMPU.
- Provide the UE with Web-based application JavaScript library and WebRTC Signalling Function IP address.

5.4.2 Description of the solution - Procedures

Editor's note: Describes the high-level operation, procedures and information flows for the solution.

5.4.3 Impact on existing entities and interfaces

Editor's note: Impacts on existing nodes or functionality will be added.

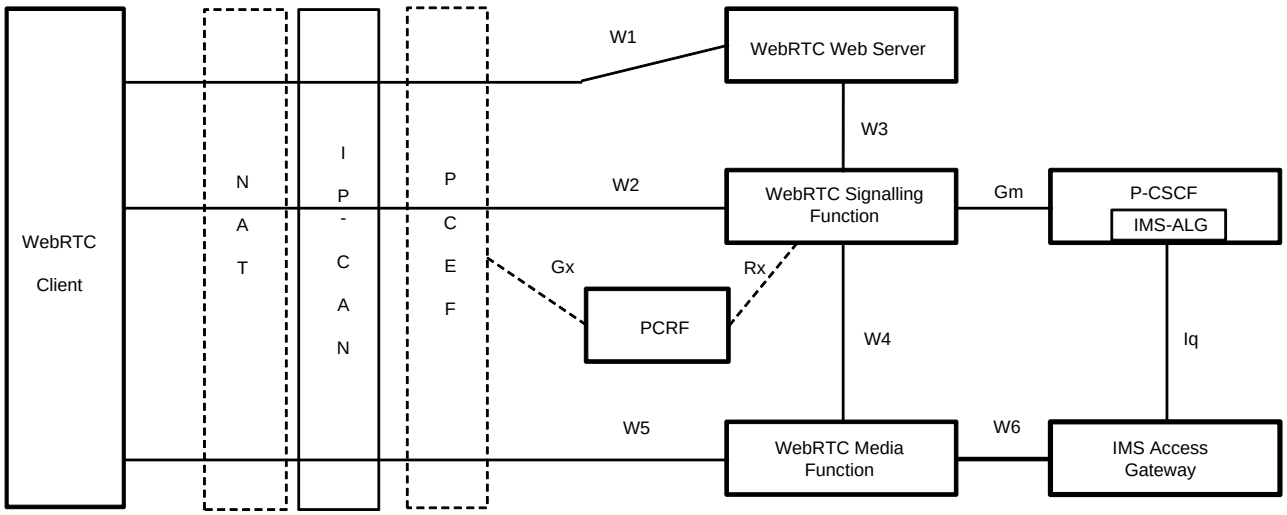
5.4.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.5 Solution 5

5.5.1 Overview

5.5.1.1 Reference architecture model



NOTE 1: In the above WebRTC architecture, the WSF acts as an Application Function to perform the Rx session with the PCRF, and the existing Rx interface between P-CSCF and PCRF is not used for the WebRTC session.

NOTE 2: In the above architecture it is assumed there exists a trust relationship between the WSF and IMS core network entities.

Figure 5.5.1.1 High level architecture for IMS_WebRTC

5.5.1.2 Reference points

W1 Reference point between a WebRTC client and a WebRTC Web Server Function.
It is used to download JavaScript and support the authentication of user identity provided by the WebRTC Client.

W2 Reference point between a WebRTC client and a WebRTC Signalling Function.
It is used to define the signalling plane interaction between WebRTC client and WebRTC Signalling Function.

W3 Reference point between a WebRTC Signalling Function and a WebRTC Web Server Function.
It conveys the user information stored in WebRTC Web Server Function to WebRTC Signalling Function and verifies the security info (e.g. Token) from WSF and WWS.

W4 Reference point between a WebRTC Signalling Function and a WebRTC Media Function.
It is used by WebRTC Signalling Function to control WebRTC Media Function.

W5 Reference point between a WebRTC client and a WebRTC Media Function. It is used to define the media plane interaction between WebRTC client and WebRTC Media Function.

W6 Reference point between WebRTC Media Function and IMS Access Gateway.

NOTE: W1 is provided here for information only and is considered out of scope of the later normative work.

Editor's note: Whether the W2, W3, W5 interfaces need to be specified is FFS.

5.5.1.3 Functional entities

5.5.1.3.1 WebRTC Signalling Function

The WebRTC Signalling Function resides in the home IMS network, acting as the signalling mediation function between the WebRTC client and P-CSCF.

The functionality of the WebRTC Signalling Function includes but is not restricted to:

- Perform conversion between WebRTC signalling (e.g. HTTP/HTTPS/Websocket signalling) and SIP signalling.
- Support ICE procedures on SDP offer/answer negotiation.
- Implement a limited STUN server functionality to support the STUN keep-alive usage as defined in IETF RFC 5389 [16] which is used by the UE to maintain the NAT bindings. (similar to the STUN function provided by P-CSCF).
- Communicate with Policy and Charging Rules Function (PCRF) by Rx interface to authorize the bearer resources and manage QoS.
- Communicate with WebRTC Web Server Function to verify user authorization and retrieve IMS identities (e.g. IMPU that stored in WebRTC Web Server Function).
- Support the registration with IMS on behalf of the user.
- Support forwarding the message to UE in terminating case.
- Detect if there is NAT between the WebRTC client and WSF and perform the necessary procedures for NAT traversal (e.g. the P-CSCF procedures related for NAT traversal according to Annex G of TS 23.228 [2]).
- Generation of CDRs.

5.5.1.3.2 WebRTC Media Function

The WebRTC Media Function resides in the home IMS network, acting as the media mediation function between the WebRTC client and IMS Access Gateway.

The functionality of the WebRTC Media Function includes but is not restricted to:

- Convert the voice and video media between SRTP and RTP.
- Convert non-voice/video media between data channel/WebSocket and MSRP.
- Support codec transcoding.
- Support ICE procedures on connectivity check.

5.5.1.3.3 WebRTC Web Server Function

The WebRTC Web Server Function may be provided by the home IMS operator or alternatively by a Third party service provider that is trusted and authorised by the home IMS operator to provide users with the service of WebRTC accessing IMS.

The functionality of the WebRTC Web Server Function includes but is not restricted to:

- Authenticate the user identification and then generate user security information (e.g. Token) for access control.
- Validate user security information sent from the WebRTC Signalling Function. The WebRTC Web Server Function provides the WebRTC Signalling Function with additional user information (e.g. IMPU) to map to the

user identity used by the WebRTC client in the case where the WebRTC client uses an identity different from IMPU.

- Provide the UE with Web-based application JavaScript library and WebRTC Signalling Function IP address.

5.5.2 Description of the solution - Procedures

5.5.2.0 General

The following clauses describe the high-level operation, procedures and information flows for the solution described above in clause 5.5.1.

5.5.2.1 Registration

5.5.2.1.1 Introduction

The scenarios of this solution are depicted as follows, mainly categorized by the type of identities used to access to IMS.

Scenario 1: The WebRTC client is an IMS subscriber, and uses operator provided credentials:

- Using web identities to access to WebRTC service. In this scenario, the authentication of username is done in the operator provided WWS and also the mapping between IMS identities and Web identities are stored in operator provided WWS. Clause 5.5.2.1.2.1 provides detailed procedure to this scenario.
- Using IMS credential to access to WebRTC service. In this scenario, the authentication of username is done in the IMS network. Clause 5.5.2.1.2.2 provides detailed procedure to this scenario.

Scenario 2: The WebRTC client uses a web identity. The WebRTC Web Server belongs to the enterprise domain. The operator assigns a range of IMPUs to the WWS and the registration will be done by the WWS on behalf of its users. Clause 5.5.2.1.3 provides detailed procedure to this scenario.

5.5.2.1.2 Registration procedures using operator provided credentials

5.5.2.1.2.0 General

In this scenario, the user uses operator provided credentials to login to the WebRTC server. The operator provided credentials can be either operator provided Web identities or IMS credentials.

5.5.2.1.2.1 Registration using operator provided Web identification

Figure 5.5.2.1.2.1.1 shows the registration flow when a WebRTC client registers with operator provided Web identification based on web authentication.

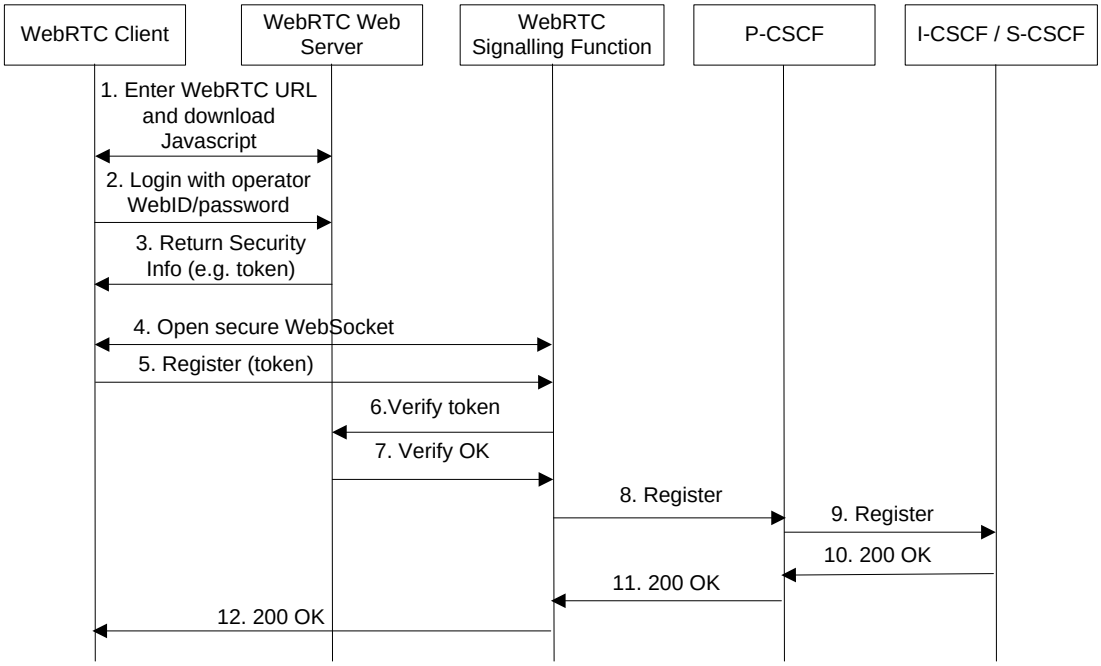


Figure 5.5.2.1.2.1-1 Registration using Operator provided Web ID

1-3. The user inputs the WebRTC Web Server URL to the WebRTC-capable browser, and downloads the WebRTC JavaScript from the WebRTC Web Server. Then the User login with the operator provided Web ID and password, the WebRTC Web Server authenticates the Web ID according to existing web authentication procedures, returns the security information (e.g. token) to the WebRTC client.

4. The WebRTC client opens the security WebSocket between the WebRTC client and the WebRTC signalling function.

NOTE 1: The WebSocket can be opened after successful completion of registration procedures if the signalling protocol between the WebRTC client and WSF is not dependent on WebSocketS.
Step 4 is necessary when for example SIP over WebSocketS is used to send a SIP request from the WebRTC client to the WSF.

5. The WebRTC client sends the Register request to the WebRTC Signalling Function via WebSoceketS, including the token received from WWS.

6-7. Upon receipt of the Register request, the WSF sends a message to WWS to verify the token. After validating the token, the WWS determines the IMPU/IMPI assigned to the user by querying a database (e.g. the WWS or a standalone entity {not shown}) which the mapping of Web identities and IMPUs/IMPIs are stored, returns the IMPU and IMPI mapped to the operator provided Web ID. As an alternative to the message flow in steps 6-7, token verification can occur via other methods, for example, an encryption method.

NOTE 2: The WWS doesn't need to return IMPU and IMPI in step 7, if the WWS returns the IMS identities as claims within the security information (e.g. token) in step 3 and the Register request in step 5 includes IMPU and IMPI extracted from the token.

8-9. The WSF forwards the Register request to IMS via the P-CSCF to initiate IMS registration after the validation from the WWS.

Editor's note: The authentication mechanism between the WSF and S-CSCF used in steps 8-9 is for FFS.

10-12. The S-CSCF returns 200 OK to the WebRTC client to confirm successful IMS registration.

5.5.2.1.2.2 Registration using IMS credential

Figure 5.5.2.1.2.2-1 shows the registration flow when a WebRTC client registers with IMS credential. In the below call flow, it is assumed that the WebRTC Web Server belongs to the IMS operator or a trusted entity.

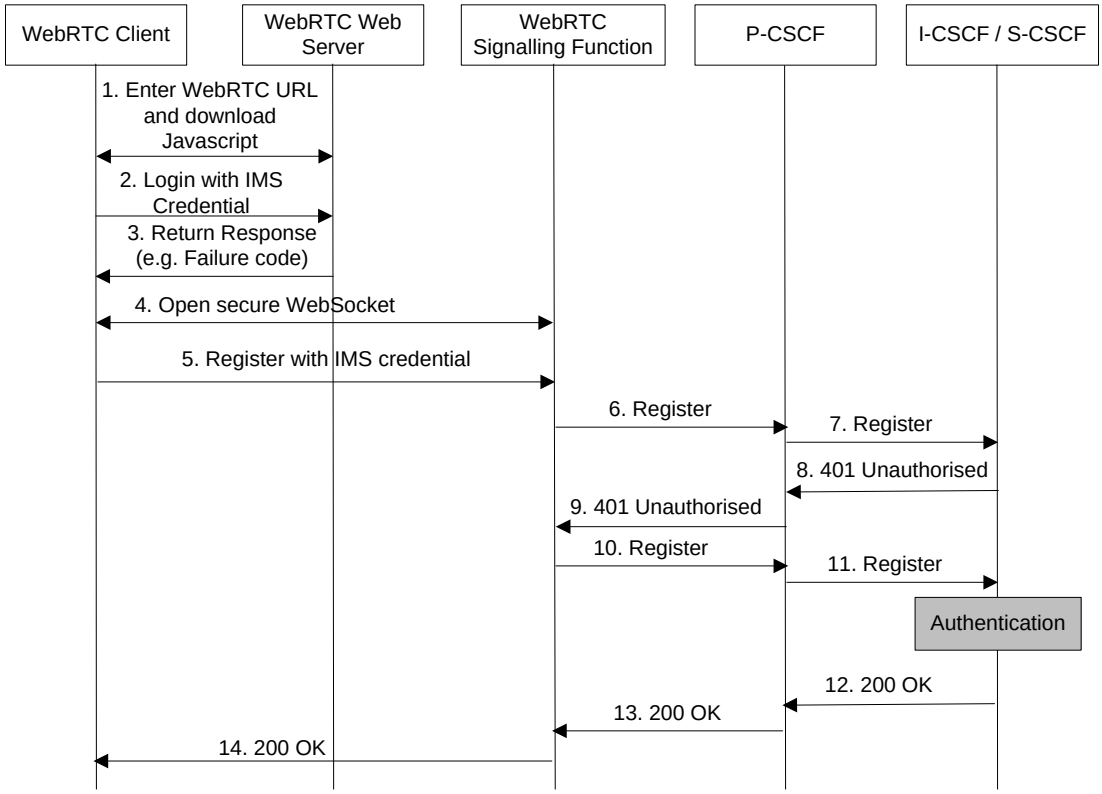


Figure 5.5.2.1.2.2-1 Registration using IMS credential

1-3. The user inputs the WebRTC Web Server URL to the WebRTC-capable browser, and downloads the WebRTC JavaScript from the WebRTC Web Server. Then the User login with IMS credential and password. The WebRTC Web Server checks that it cannot authenticate the IMS credential for the reason that there is no authentication information and returns response to the WebRTC client to indicate that the authentication needs to be done in IMS core.

NOTE 1: If the WebRTC client differentiates between Web ID and IMPU (for example different input fields), steps 2 and 3 can be omitted and IMS credentials are included in the Register request of step 5.

4. The WebRTC client opens the security WebSocket between the WebRTC client and the WebRTC signalling function.

NOTE 2: The WebSocket can be opened after successful completion of registration procedures if the signalling protocol between the WebRTC client and WSF is not dependent on WebSocketS. Step 4 is necessary when for example SIP over WebSocketS is used to send a SIP request from the WebRTC client to the WSF.

5-7. The WebRTC client sends the Register request to IMS via the WebRTC Signalling Function via WebSoceketS. The Register request includes IMS Digest authentication parameters, IMPI, IMPU and other information as needed to access IMS.

8-11. The S-CSCF initiates normal authentication procedure and send a 401 message towards WSF. On receiving a 401 (Unauthorized) response to the REGISTER request, the WSF will behave according to existing UE procedures when UE receives a 401.

NOTE 3: The response of the 401 auth_challenge to the WSF makes the client simpler and removes the dependency on the client to support specific authentication mechanisms.

NOTE 4: If SIP (SIP over WebSocketS) is supported by the WebRTC client, the 401 auth_challenge can be sent towards the WebRTC client, else the WSF is required to store additional user credential information if the 401 auth_challenge is terminated by the WSF.

Editor's note: Whether or not the above procedure where the 401auth_ challenge is not sent to the WebRTC client causes a security issue is FFS.

12-14. The S-CSCF returns 200 OK to the WebRTC client to confirm successful IMS registration.

5.5.2.1.3 Registration of IMPU range by WWS

5.5.2.1.3.1 General

The following clauses describe the scenario where the WebRTC Web Server belongs to the enterprise domain.

The operator assigns a range of IMPUs to the WWS and the registration will be done by the WWS on behalf of its users. WebRTC client uses a web identity.

5.5.2.1.3.2 Registration of IMPU range when WWS registers on behalf of its users

The WWS obtains a block of IMS identities which will be assigned to individual client. The WWS is usually located in third party network authorized by the IMS operator.

Figure 5.5.2.1.3.2-1 shows the registration flow when the IMS identities are managed by WWS and the WWS registers on behalf of its users. These steps are for the WWS to register a set of identities with the IMS and that this can happen at any time before the user registration, i.e. when the WWS is deployed for example.

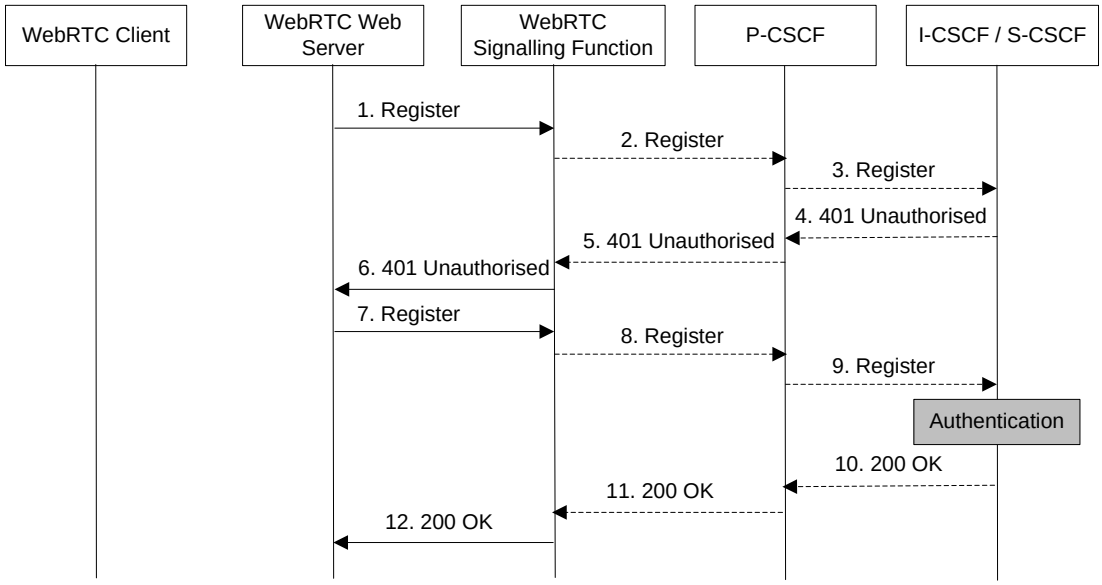


Figure 5.5.2.1.3.2-1 Registration of IMPU range Web ID when WWS registers on behalf of its users

1. The WWS initiates an IMS registration procedure by sending a Register request to the WSF requesting that the WSF register on its behalf with IMS. The message includes the block of IMS identities associated with the WWS and IMS digest authentication parameters.

2-3. In the static mode, the associated IMS identities are already registered with IMS by configuration, so the WSF bypasses steps 2 to 5, and continues with step 6. In registration mode, the WSF initiates an IMS registration transaction by sending a Register request to the P-CSCF and S-CSCF to register the block of IMS identities asserted by the WWS.

4. In registration mode, the S-CSCF returns a 401 Auth_Challenge to the WSF.

5-6. In static mode, the WSF directly challenges the request in step 1. In registration mode, the WSF forwards the challenge received from the S-CSCF.

7. The third party WWS resends the Register request to the WSF with the IMS digest credentials.

8-9. In registration mode, the WSF sends another Register request to the P-CSCF and S-CSCF that includes the IMS credentials from the WWS. And the S-CSCF authenticates as normal procedure.

10-11. In registration mode, the S-CSCF responds with a 200 OK message if the credentials are accepted.

12. In static mode, the WSF verifies the credentials from the WWS directly. In registration mode, the WSF waits for successful IMS registration. After success in either case, the WSF sends a 200 OK response to the WWS to confirm that the block of IMS identities has successfully registered.

5.5.2.1.3.3 WebRTC Client registration of individual IMPU from wildcard IMPU range

Based on the procedure in clause 5.5.2.1.3.2, the WWS can assign individual IMPUs from the block of IMPUs to WebRTC clients under its control.

Figure 5.5.2.1.3.3-1 shows the registration flow for a WebRTC client being assigned an individual IMPU from a block of IMPU range assigned to the WWS.

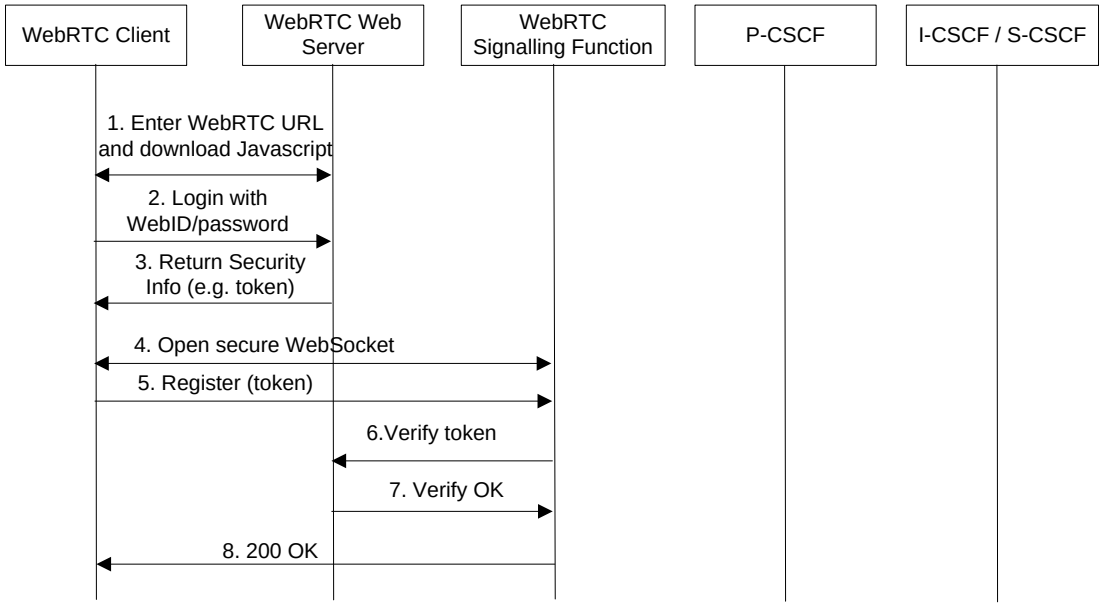


Figure 5.5.2.1.3.3-1 WebRTC Client registration of individual IMPU from wildcard IMPU range

1-3. The user inputs the third party WebRTC Web Server URL to the WebRTC-capable browser, and downloads the WebRTC JavaScript from the WebRTC Web Server. Then the user login with the third party provided Web ID and password. The WWS authenticates the Web ID according to existing web authentication procedures and returns the security information (e.g. token) to the WebRTC client.

4. The WebRTC client opens the security WebSocket between the WebRTC client and the WebRTC signalling function.

NOTE 1: The WebSocket can be opened after successful completion of registration procedures if the signalling protocol between the WebRTC client and WSF is not dependent on WebSocketS. Step 4 is necessary when for example SIP over WebSocketS is used to send a SIP request from the WebRTC client to the WSF.

5. The WebRTC client sends the Register request to the WebRTC Signalling Function via WebSoceketS, including the token received from WWS.

6-7. Upon receipt of the Register request, the WSF sends a message to the WWS to check if the token is valid. After validating the token, the WWS determines the IMPU/IMPI assigned to the user by querying a database (e.g. the WWS or a standalone entity {not shown}) which the mapping of Web identities and IMPUs/IMPIs are stored, returns the IMPU and IMPI mapped to the operator provided Web ID. The WSF also verifies that the IMS identities being registered are assigned to the third party based on the procedure depicted in clause 5.5.2.1.3.2 either in static mode operation or in registration mode operation. As an alternative to the message flow in steps 6-7, token verification can occur via other methods, for example, an encryption method.

NOTE 2: The WWS doesn't need to return IMPU and IMPI in step 7, if the WWS returns the IMS identities as claims within the security information (e.g. token) in step 3 and the Register request in step 5 includes IMPU and IMPI extracted from the token.

8. The WebRTC Signalling Function sends 200 OK to the WebRTC client to confirm successful IMS registration.

5.5.3 Impact on existing entities and interfaces

Editor's note: Impacts on existing nodes or functionality will be added.

5.5.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.6 Solution 6

5.6.1 Overview

Figure 5.6.1-1 shows an IP PBX emulation architecture with standard IMS business trunking interfaces. The WebRTC signalling and media mediation functions provide interworking between the WebRTC client and standard IMS signalling and media protocols. The UE can be of any type, supporting any IP-CAN(s), including EPC roaming options. The WebRTC client on the UE, the PBX emulation functions, and the interfaces between the UE and the PBX emulation functions are unspecified by 3GPP except for the signalling and media interfaces to IMS functions shown in the figure.

The functions providing PBX emulation can be located anywhere within an enterprise, a third party network or within the operator network. Since the functions providing PBX emulation conform to standard IMS business trunking interfaces, there is no impact to IMS. In particular, the WebRTC signalling function ensures that SIP on Gm or Ici is conformant to IMS SIP for business trunking on these interfaces. Media extensions not supported by IMS (e.g. unsupported codecs, trickle ICE, consent signalling, DTLS-SRTP) are terminated by the WebRTC media function.

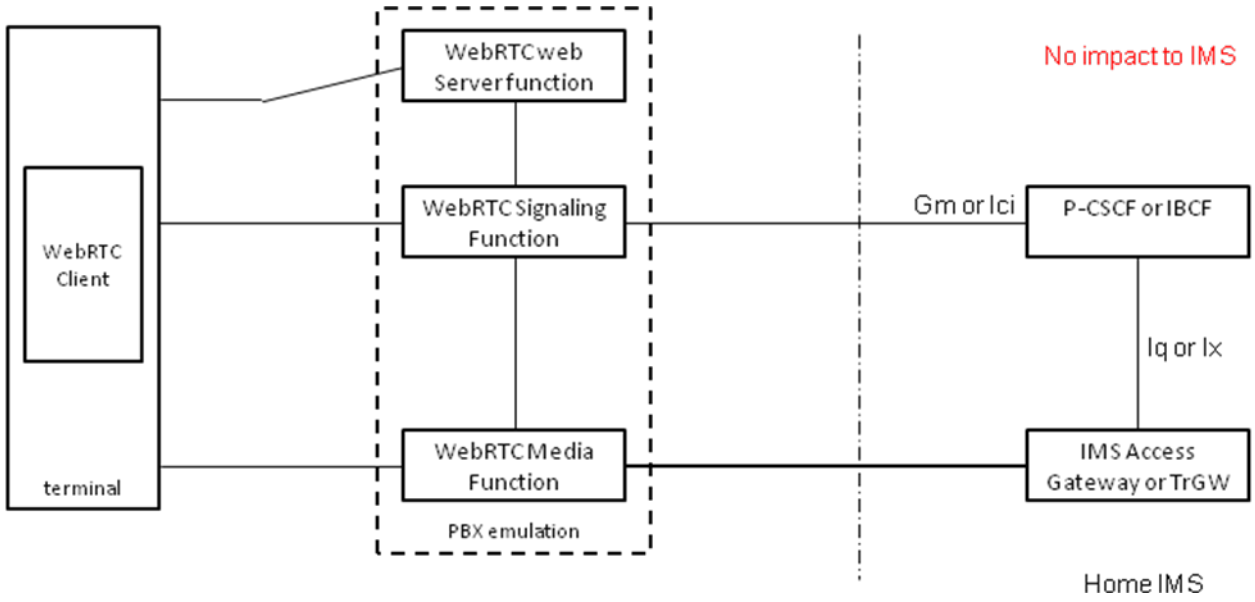
The media protocols seen at the AGW or TrGW need to be IMS compliant.

The functions providing PBX emulation register blocks of IMS user identities with IMS using either static mode or registration mode.

IMS has no knowledge of individual WebRTC clients and no responsibility to provide services such as security, identity, individual registration state, or QoS, directly to the clients. The clients are authenticated by the PBX emulation functions. The PBX emulation functions perform a role equivalent to a SIP registrar for individual clients.

The PBX might provide communication services to the clients before forwarding signalling associated with the clients to/from IMS.

Since the PBX emulation functions must anchor media to provide the necessary e2ae media procedures, IMS cannot provide QoS via Rx on the P-CSCF. The PBX emulation functions might directly use an OMA REST or XML interface to PCC for QoS, bypassing IMS, but the details are out of scope.



NOTE: The vertical line depicts the split between IMS and the non-IMS world and does not mean any ownership of the PBX emulation functions.

Figure 5.6.1-1: WebRTC PBX emulation architecture

5.6.2 Description of the solution - Procedures

The PBX emulation functions register blocks of IMS identities with IMS using either static mode or registration mode for business trunking.

The PBX emulation functions are responsible for all interaction with the WebRTC client, such as client download, authentication, location tracking for service terminations, and arranging for QoS, where possible. Detailed QoS procedures are out of scope.

The PBX emulation functions provide signalling and media interfaces that conform to standard IMS business trunking interfaces and procedures.

5.6.3 Impact on existing entities and interfaces

This solution re-uses the existing enterprise trunking solutions for IMS.

5.6.4 Solution evaluation

Editor's note: The fulfilment of requirements in clause 4.2 will be evaluated.

5.7 Solution 7

5.7.1 Overview

5.7.1.1 Assumptions

This clause include assumptions specific to this solution and are in addition to those listed in clause 4.1.

- The UE architecture includes a JS execution environment that supports the WebRTC APIs.
- The UE architecture includes an IMS client. The UE can register for IMS based services in the HPLMN. The solution requires neither modifications to IMS specification nor modifications to IMS functions deployed in the network.

- The browser may or may not support 3GPP codecs (AMR-WB/NB, H.264) in addition to those defined by IETF WebRTC. In case the browser does not support 3GPP codecs, the UE needs to implement transcoding from/to WebRTC codecs and 3GPP codecs.

- The web server providing the HTML and the WebRTC App resides in the HPLMN as an operator provided service.

- This UE based solution does not require browser customizations (beyond the support of 3GPP codecs, refer to clause 5.7.3), instead it keeps a generic Web Browser.

5.7.1.2 High level architecture

Figure 5.7.1.2-1 shows an architecture with WebRTC signalling and media mediation functions located within a custom application on the UE. These mediation functions provide interworking between the WebRTC client and standard IMS signalling and media protocols.

The UE can be of any type, supporting any IP-CAN(s), and the WebRTC client can have access to capabilities available to a native IMS client on the device, and has the same restrictions.

Since the UE configuration uses a standard IMS client on the device, there is no impact to the IMS network.

In particular, the UE provides Gm and media interfaces fully compliant to the standard IMS interfaces.

Since the WebRTC client has access to all of the functions of a native IMS client, webRTC services running on the UE benefit from the following characteristics:

- Access to a UICC that might be present in the device for IMS credentials.

- IMS can authenticate and register the WebRTC client using standard IMS registration procedures according to the IMS subscription information in the UICC, if present, or as otherwise presented depending on the type of UE.

- The UE can be configured for all IMS functions appropriate to a native IMS client, including APN selection (i.e. IMS APN), IMS roaming, Gm ciphering, SRVCC, QoS, etc.

Due to the above characteristics, this solution cannot address all of the use cases described for WebRTC IMS access in TS 22.228 [13]. The solution only provides WebRTC access for IMS subscribers using existing IMS procedures, in particular existing IMS authentication procedures. The solution cannot provide for web authentication options and cannot support allocation of IMS identities to WebRTC clients by a third party.

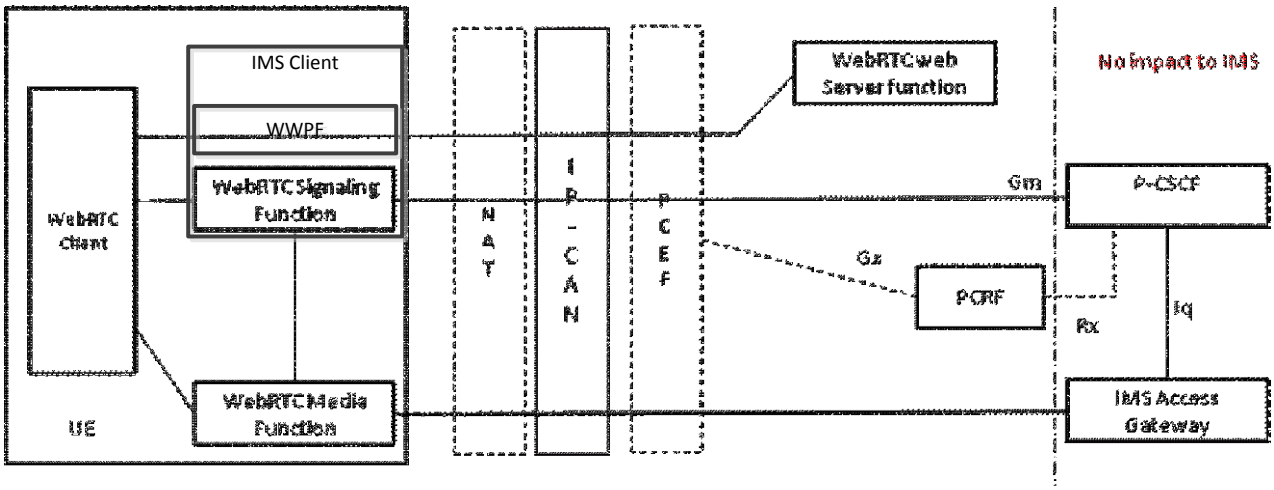


Figure 5.7.1.2-1 WebRTC IMS client emulation architecture

The following functions shall be supported on the device:

- WebRTC **Web Proxy (WWPF).**

There is no generic browser nowadays that has an interface through which it may access the IMS credentials on a UE. In order to allow a mechanism that permits a user to certify to a web server using IMS credentials and with no browser modifications, the solution proposes a two steps approach based on a new terminal component: WebRTC Web Proxy Function (WWPF). The role of the WWPF is to act as a middle layer between the WWSF component detailed in clause 5.3.1.3 and the local IMS client. It provides the IMS based credentials in the authentication exchange with the Web Server without requiring changes in the generic browser. WWPF implements basic web proxy functionalities and it interacts with the IMS client on the device as well as with the generic browser.

Editor's note: How the HTTP proxy can modify the HTTPS content when TLS is used is FFS.

- WebRTC **Signalling Function (SIF).**

In this approach, the key information that needs to be exchanged is the multimedia session description, which specifies the necessary transport and media configuration information necessary to establish the media plane.

Although JSEP allows a large flexibility regarding the signalling plane that may be used there are currently one signalling protocol that may be good contenders to be used in the context of WebRTC operator provided services: SIP. In the case of SIP, the SIF function is a simple pass-through, while if SIP is not used, SIF needs to do the conversion between the JSEP SDP offer/answer and the SIP SDP that is carried over the IMS infrastructure.

- **RTC Media Interworking Function (RMF).**

The media mediation on the UE must be treated based on two scenarios: a) operator controlled cases in which the web page is provided by the operator or is on a server under the operator control and b) Third party or OTT cases in which the operator does not have the control of the original JS download.

This solution addresses the Operator controlled cases and it may require either:

1. use UE-based DNS proxy to resolve TURN server to local UE-hosted instance or
2. use operator DNS to resolve TURN server to local UE-hosted instance.

The communication channel for WebRTC assumes SRTP to be used by each peer. In order to allow the operator to have control of the media that it is exchanged over the channel, the RMF function must be able to access the SRTP data and convert it into a format supported by the operator.

5.7.2 Description of the solution - Procedures

5.7.2.0 General

This clause describes the high-level operation, procedures and information flows for the solution.

The UE-resident functions providing IMS features authenticate and register IMS identities associated with an IMS subscription according to standard IMS UE procedures.

The UE-resident functions have access to all capabilities available to a native IMS client on the device, including APN selection (i.e. IMS APN), IMS roaming, Gm ciphering, SRVCC, QoS, etc.

The UE-resident functions provide signalling and media interfaces that conform to a standard native IMS client.

An example of how user registration onto IMS may work is shown in following figure:

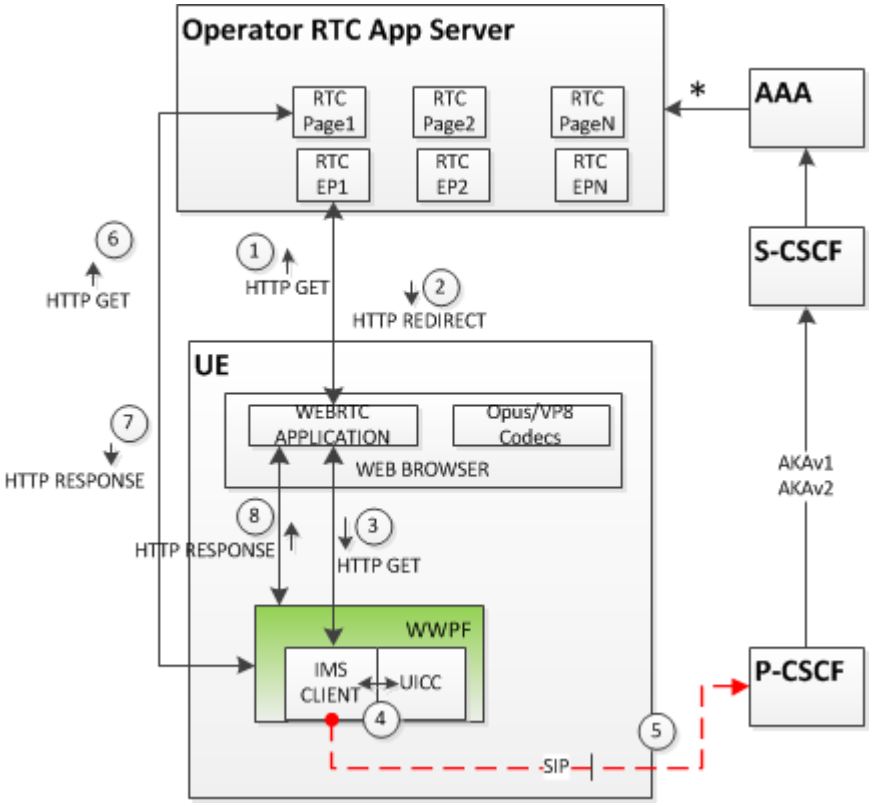


Figure 5.7.2-1: Web RTC authentication using IMS credentials

The WebRTC client in this scenario uses its IMS credentials to authenticate itself although the Web browser on the device does not have an interface to the IMS credentials. The following steps are followed in the interaction between the WebRTC client when accesses a web page as it is shown in Figure 5.7.2-1.

1. The JS above the Generic Web Browser initiates WebRTC app access to HTTP Operator Server ; the request is redirected to the local HTTP proxy.
2. HTTP Redirection to local HTTP proxy/client (in the WebRTC Signalling Function).
3. Request made to local HTTP proxy/client (in the WebRTC Signalling Function) as a result of HTTP Redirect.
4. Authentication follows: AKAv1, AKAv2 over the IMS network.
5. IMS client retrieves UICC credentials : CK, IK.
6. Once client is authenticated, the local HTTP proxy/client (in the WebRTC Signalling Function) request for RTC Page.
7. RTC Page delivered over HTTP.
8. RTC Page is delivered to the Generic Web Browser on the UE device.

5.7.2.1 ICE procedure and candidate list buildup

The JavaScript in the RTC Page provided at Step 8 of the Procedure detailed in Figure 5.7.2-1 shall contain at least the address of a STUN proxy or TURN proxy. The address of the STUN or TURN proxy, or both must be solved to a local IP address or to an IP alias that may be associated in all cases for this type of functionality. In a first step the webRTC application tries to identify using the STUN proxy the type of connectivity available for each local IP interface. If the only available connectivity is through a symmetric NAT then the WebRTC application is using TURN proxy for an allocation. In operator controlled cases the traffic is redirected through TURN proxy. The detailed steps are shown below:

Step 0: Load UE STUN/TURN/DNS Proxy. Load WebRTC application and Initiate ICE candidate gathering.

Step 1: Solve the STUN and/or TURN FQDN to a local STUN and/or TURN proxy IP.

Step 2: On STUN UE proxy for operator controlled cases the ICE initiates TURN allocation TURN allocation.

Step 3: In operator controlled case, authenticate UE against UE TURN proxy; in OTT case with IMS peer, skip TURN authentication. Allocate media resources on TURN server.

Step 4: On UE TURN proxy: on ICE connectivity checks, use IMS network to check availability on TURN peer proxy.

5.7.2.2 WebRTC call flow

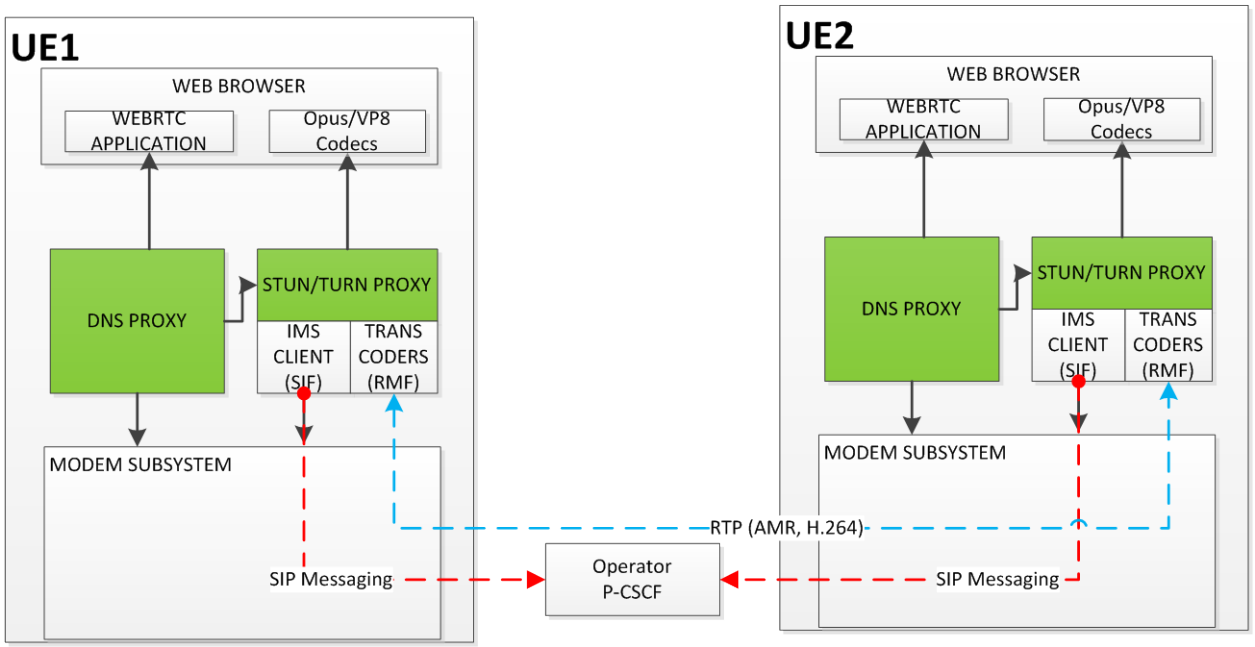


Figure 5.7.2.2-1: End to end connectivity on operator controlled WebRTC

Each of the terminal devices creates the candidate build up list as described in clause5.7.2.1. The two peers use SDP attributes to exchange the candidates on each part of the connection through a sequence of INVITE/183Session In Progress/PRACK/200OK/ messages. At the end of the exchange the media transmission path is established between the peers. An example of this exchanged is detailed in Figure 5.7.2.2-2.

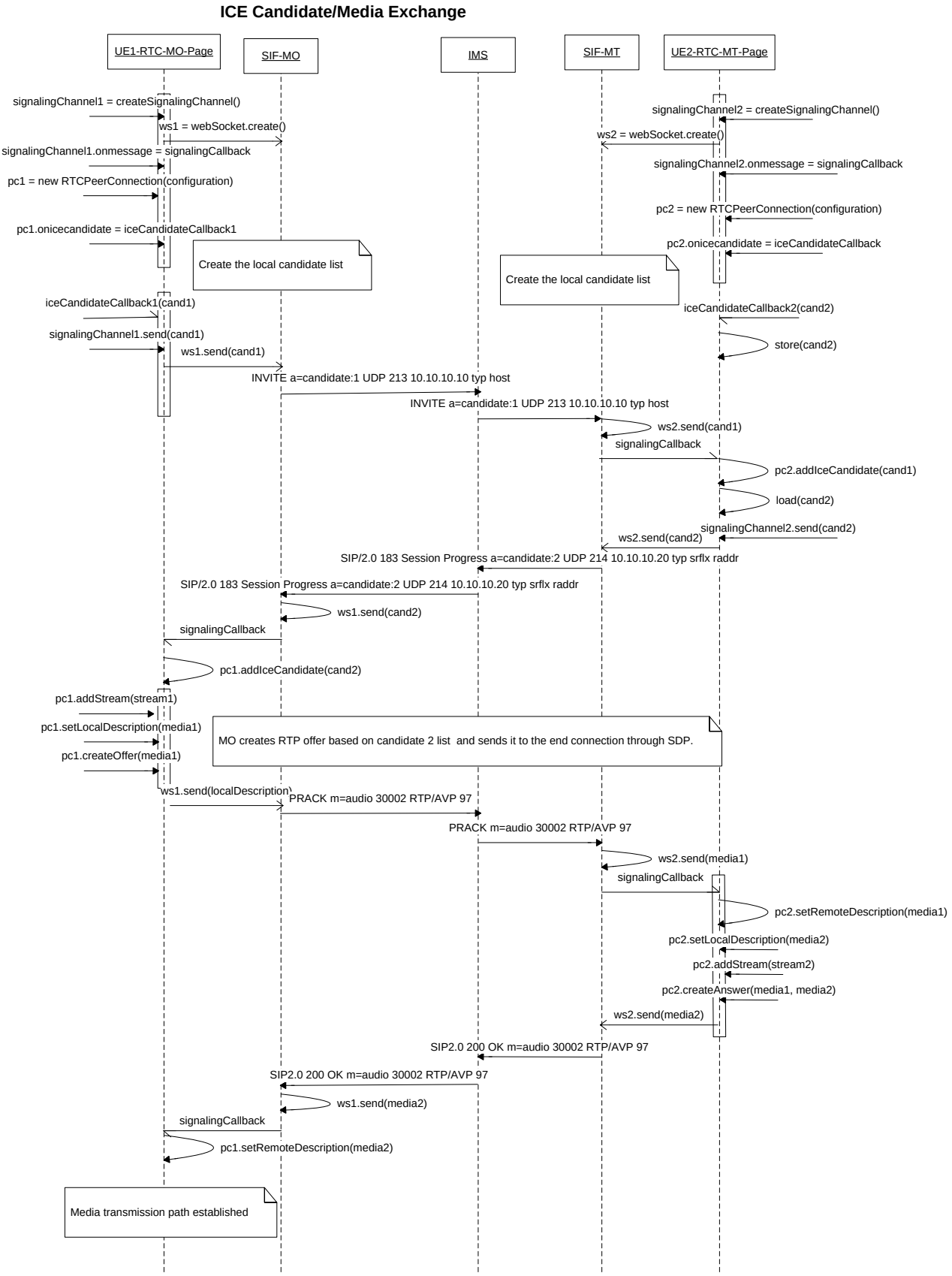


Figure 5.7.2.2-2: ICE Candidate and Media exchange between peers

5.7.2.3 Media Interworking Function – Transcoding free operation

Many of the 3GPP terminal devices have built-in support for audio/video encoding/decoding functionalities, A web browser should support 3GPP codecs.

If the browser does not support 3GPP codecs the MIF function provides the conversion functionality.

5.7.3 Impact on existing entities and interfaces

The impact on the existing nodes is discussed in clause 5.7.4.

5.7.4 Solution evaluation

The proposed solution does not require changes either in ICE procedure, WebRTC app or web browser capabilities.

The proposed solution shows one mechanism of implementing signalling and media interworking of WebRTC traffic within a device. There could be other implementation specific architectures to achieve similar interworking.

The solution allows the reuse of IMS credentials and IMS authentication mechanisms already standardized in the 3GPP.

The solution does not require any changes to the operators IMS Core Network.

It uses UE STUN proxy and/or TURN proxy. It requires a local DNS proxy or DNS custom function in the operator network.

It forces ICE to use UE internal TURN server to achieve direct UDP connectivity over IMS . The UE-based STUN/TURN proxy embeds IMS client signalling functionality. The TURN component acts as a redirection mechanism of the WebRTC traffic toward the IMS connectivity.

In operator controlled cases, if IMS infrastructure is being used peers may be able to control the use of SRTP. The DNS proxy resolves the operator provided STUN/TURN server to local UE-hosted instance.

On the media path this Solution proposes that the browser should support all the 3GPP codecs available on the device. If there is no browser support for this codecs this Solution uses MIF.

6 Evaluation

Editor's note: This clause contains the overall evaluation of various solutions.

7 Conclusions

Annex A captures the decisions reached in Release 12 as a result of the study with regard to network-based solutions, and provides source text that can be used for CRs to TS 23.228 [2] for Release 12 to populate it with normative text for the WebRTC access to IMS feature. This annex is comprised of elements of all network-based solutions in the TR and supersedes them in Release 12.

It is also concluded that UE-based solutions do not have any standard impact.

Annex A:
WebRTC access to IMS - network-based architecture

A.1 Overview

A.1.1 Assumptions

- In this annex, the word "UE" can correspond to either a 3GPP or a non-3GPP terminal.
- The JS execution environment that executes the WIC has no standardized way to access an ISIM/USIM on any terminal.
- This Release specifies an option to use a signalling interface from the UE to the network based on SIP over WebSocket, which is used as the information model on which other options are expected to be based. Options other than SIP over WebSocket are allowed in this Release, such as a REST based interface, JSON over WebSocket, XMPP, but are not described in this document. Any enhancements required to accommodate an unspecified signalling interface are considered compliant to the Release as long as other defined interfaces in the architecture are not impacted.
- At the discretion of the CT groups, it is recommended that stage 3 documentation include information describing the elements of the message sequences and information model for SIP over WebSocket that need to be present for any alternative signalling interface.
- SDP offer/answer exchange is the mechanism used for media plane feature negotiation.
- In this Release, the architecture does not support media multiplexing that is defined for WebRTC clients.

NOTE 1: A JS downloaded in a WIC accessing IMS services is not expected to allow usage of media multiplexing in the browser. If an SDP offer with media multiplexing was nevertheless sent to the network the part of the SDP offer associated with media multiplexing would be removed at the entry of the IMS network.

- In this Release, WebRTC specific media plane extensions will be handled at the access edge and will not be propagated to other IMS functions.
- This Release specifies DataChannel transport options for MSRP, BFCP and T.140. Other options are allowed in this Release, but are not described in this document.
- In this Release, in case of a network based interworking between WebRTC and IMS, for 3GPP and EPC access from a WebRTC client:
  - Use of available techniques to select preferred access technologies and APNs, and to provide IP address continuity, are allowed but not described.
  - When the WebRTC client is served by an IP-CAN in a configuration that supports PCC, it is possible to request QoS within the IP-CAN for WebRTC media.

NOTE 2: To ensure full end to end QoS support, proper IP forwarding policies should be set in the path between the PGW and the Functions supporting media interworking to the IMS.

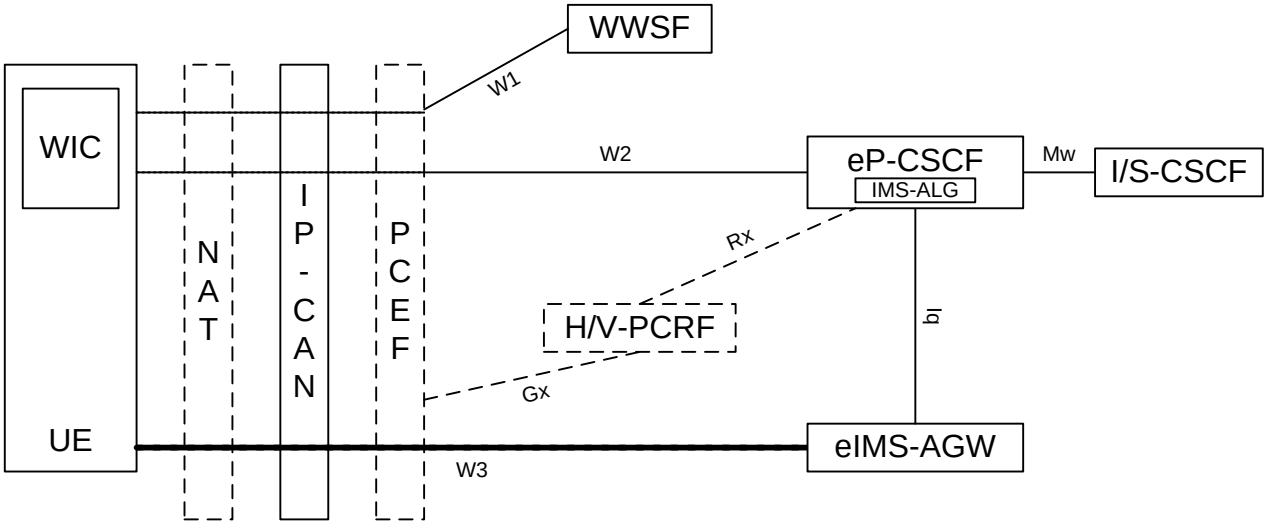
- QoS can be provided in configurations where the IMS can identify the transport (TCP-UDP/IP) addresses handled by the PCEF and where based on this information PCC functions can identify the UE media flows to prioritize.

A.1.2 Signalling architecture

Figure A.1.2-1 shows the WebRTC IMS signalling architecture. The WWSF (WebRTC web server function) is located either within the operator network or within a third party network and is the first web server contacted by the user

(generally by clicking on a link or entering a URL into the browser). The P-CSCF enhanced for WebRTC (eP-CSCF) is the endpoint for the signalling connection from the client and is located in the operator network.

NOTE 1: The presence of dashed elements in the figure depends on the configuration.
PCC functional elements are present only for 3GPP access with QoS.
The corresponding PCC elements for fixed access are also optionally supported but not shown.
The NAT in figure A.1.2-1 is meant for non-cellular access to IMS.



NOTE 2: A reference point between the WWSF and eP-CSCF might be considered in future Releases.
NOTE 3: W3 corresponds to the output of the IETF RTCWEB discussions.
NOTE 4: The enhanced network entities, such as the eP-CSCF, might be decomposed into multiple network elements (e.g., P-CSCF and WebRTC Signalling Function) in future Releases to address additional use cases and configurations.

Figure A.1.2-1: WebRTC IMS signalling architecture

A.1.3 Functional entities

A.1.3.1 WIC (WebRTC IMS Client)

A WebRTC IMS Client (WIC) is a WebRTC JS application capable of interoperating with the WebRTC IMS access architecture defined herein. The WIC application is downloaded from the WWSF within the operator network or a third party network and provides access to the communications services of the IMS. The WIC functions on any device supporting a browser (or equivalent JS execution environment) with WebRTC extensions via any IP access network with access to the internet, subject to the QoS and reachability limitations of the access network. The WIC places no other requirements on the UE on which it is executed.

A.1.3.2 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 user. The WWSF has the following characteristics and functions:

- The WWSF is located either in the operator network or a third party network authorized by the operator network.
- The WWSF provides the Web page presenting the user interface to the user for IMS access.
- The WWSF provides the JS WIC application for downloading to the browser on the UE.
- If the WIC does not enforce the use of IMS authentication for the user, the WWSF manages the correct and consistent allocation of authorized IMS identities to WICs associated with authenticated Web identities. The JS application downloaded from the WWSF controls which authentication mode applies.

NOTE: The WWSF represents a collection of functions that might be further split across servers or networks, so long as they behave in the aggregate as described.

A.1.3.3 eP-CSCF (P-CSCF enhanced for WebRTC)

The P-CSCF enhanced for WebRTC (eP-CSCF) is a standard P-CSCF with the IMS-ALG functionality and with the following additional conditionally mandatory characteristics and functions when enhanced to support WebRTC:

- The eP-CSCF supports at least one WebRTC UE-to-network signalling protocol, e.g. SIP over WebSocket, JSON over WebSocket, XMPP over WebSocket, HTTP/REST interface.
- The eP-CSCF is located in the operator network.
- The eP-CSCF verifies any UE authentication performed by the WWSF and performs Trusted Node Authentication (TNA), as defined in TS 33.203, in IMS for UEs already authenticated by the WWSF.
- For Web authentication scenarios, the eP-CSCF verifies that the WWSF is authorized to allocate IMS identities that it assigns to a WIC.
- The eP-CSCF performs IMS registration for WICs using either IMS or Web authentication schemes.
- The eP-CSCF controls the media plane interworking functions provided by the eIMS-AGW, including those additional media plane functions specific to WebRTC.
- The eP-CSCF ensures via signalling that RTP streams are not multiplexed onto the same port if entities anchoring the session media path in the IMS domain do not support that capability.
- The eP-CSCF ensures via signalling that RTP and RTCP flows of an RTP stream are not multiplexed onto the same port if entities anchoring the session media path in the IMS domain do not support that capability.

A.1.3.4 eIMS-AGW (IMS Access GateWay enhanced for WebRTC)

The IMS AGW enhanced for WebRTC (eIMS-AGW) is a standard IMS-AGW with the following additional conditionally mandatory characteristics and functions:

NOTE 1: WebRTC only supports audio including DTMF and video media using SRTP transport, and data media using WebRTC DataChannels. Hence any media plane protocol other than audio and video will use WebRTC DataChannels for transport.

- The eIMS-AGW supports the media plane interworking extensions as needed for WICs.
- The eIMS-AGW resides in the same network as the eP-CSCF.
- The eIMS-AGW performs e2ae procedures for media protocols specific to WebRTC, including ICE, media consent, and DTLS-SRTP.
- The eIMS-AGW performs any transcoding needed for audio and video codecs supported by the browser.
- When GTT service is requested, the eIMS-AGW performs transport level interworking between T.140 over DataChannels and other T.140 transport options supported by IMS.
- When MSRP is requested, the eIMS-AGW performs as an MSRP B2BUA between MSRP over DataChannels and the other MSRP transport options supported by IMS.

NOTE 2: If CEMA extensions for transport-level interworking for MSRP are supported in IMS, the eIMS-AGW will also support this option. In this case, clause A.1.5.1 will also include a protocol architecture showing transport-level interworking for MSRP based on CEMA.

- When BFCP service is requested for conference floor control, the eIMS-AGW performs transport level interworking between BFCP over DataChannels and other BFCP transport options supported by IMS.

A.1.4 Reference points

A.1.4.1 W1 (UE to WWSF)

The W1 reference point is between the UE and the WWSF. The HTTPS protocol is normally used to access the web page providing the UI for the WIC and to download the WIC JS application to the browser.

A.1.4.2 W2 (UE to eP-CSCF)

The W2 reference point is the signalling interface between the UE and the eP-CSCF. SIP over secure WebSocket is a non-mandatory option for W2 in Release 12, where the SIP/SDP procedures are based on Gm with enhancements to support extensions defined for WebRTC clients, and secure WebSocket is the supported transport protocol. Other protocols are allowed on W2 for WebRTC access but are not described in this document.

A.1.4.3 Iq (eP-CSCF to eIMS-AGW)

The Iq reference point is between the eP-CSCF and eIMS-AGW and is enhanced to control the additional bearer plane functions specific to WebRTC clients.

A.1.4.4 W3 (UE to eIMS-AGW)

The W3 reference point is between the UE and eIMS-AGW. W3 carries the user plane between the UE and the network (see clause A.1.5).

A.1.5 Media plane protocol architecture

A.1.5.0 General

The IMS AGW enhanced for WebRTC (eIMS-AGW) is the media plane interworking element with the functions described in clause A.1.3.4. The eIMS-AGW provides e2ae media procedures for ICE, periodic consent, DTLS-SRTP, transcoding, and DataChannels as needed in support of MSRP, BFCP and T.140.

A.1.5.1 Protocol architecture for MSRP

Figure A.1.5.1-1 shows the protocol architecture for support of MSRP from a WebRTC IMS client (WIC).

The eIMS-AGW provides an MSRP B2BUA to allow interoperation with existing MSRP peer endpoints.

Use of TLS between the eIMS-AGW and peer is optional, as indicated by an asterisk (*) in the figure.

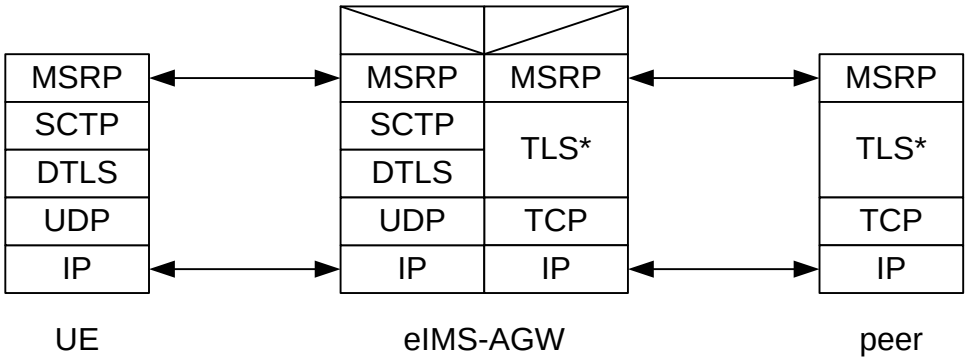


Figure A.1.5.1-1: Protocol architecture for MSRP

A.1.5.2 Protocol architecture for BFCP

Figure A.1.5.2-1 shows the protocol architecture for support of BFCP from a WebRTC IMS client (WIC).

The eIMS-AGW provides a transport relay function from DataChannel to TLS/TCP to allow interoperation with existing BFCP peer endpoints.

Use of TLS between the eIMS-AGW and peer is optional, as indicated by an asterisk (*) in the figure.

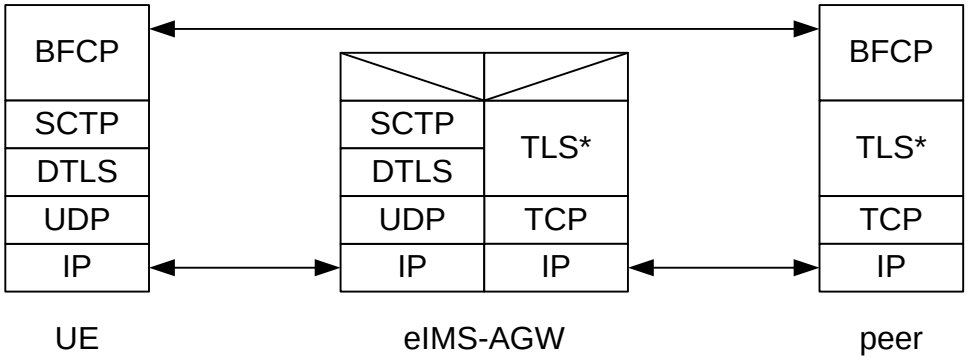


Figure A.1.5.2-1: Protocol architecture for BFCP

A.1.5.3 Protocol architecture for T.140

Figure A.1.5.3-1 shows the protocol architecture for support of T.140 from a WebRTC IMS client (WIC).

The eIMS-AGW provides a transport relay function from DataChannel to RTP/SRTP to allow interoperation with existing T.140 peer endpoints. Use of SRTP between the eIMS-AGW and peer is optional as an alternative to RTP.

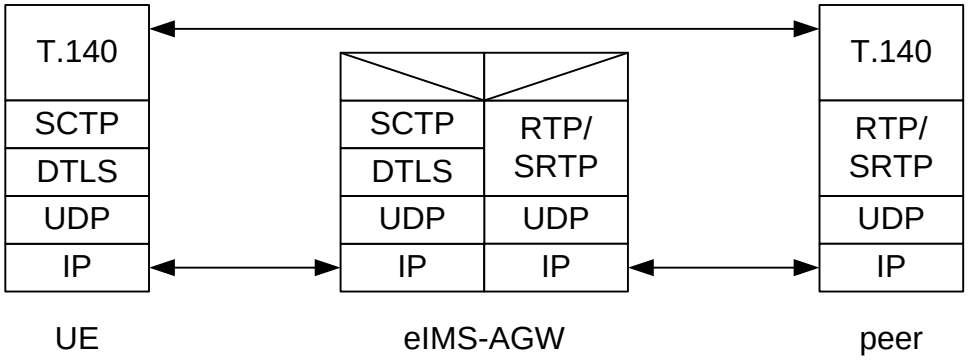


Figure A.1.5.3-1: Protocol architecture for T.140

A.1.5.4 Protocol architecture for Voice and Video

Figure A.1.5.4-1 shows the protocol architecture for support of Voice and Video from a WebRTC IMS client (WIC). Transcoding (whether codec1 is different from codec2) is optional. SRTP between the UE and the eIMS-AGW relies on keying material negotiated via DTLS.

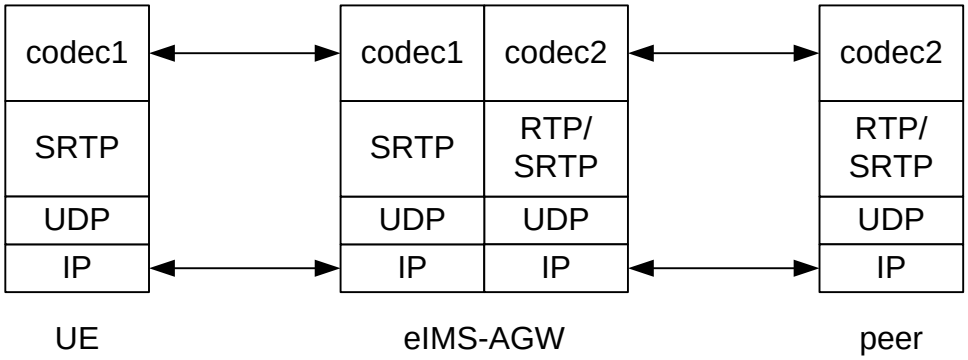


Figure A.1.5.4-1: Protocol architecture for Voice and Video

A.2 Procedures

A.2.1 Registration

A.2.1.1 Introduction

NOTE 1: SA WG3 must validate the registration scenarios and provide additional details related to security aspects of the architecture. In particular, SA WG3 should verify for all scenarios the security properties of at least the following aspects: the use of TLS, WSS and CORS at the relevant reference points; the use of IMS digest, TNA, and/or potentially other IMS authentication mechanisms; how to provide IMS digest authentication and registration information to the WIC; the potential use of a security token if the origin of the WWSF cannot be verified; the required trust relationships between functional entities for the scenarios; the mechanisms used to verify the required trust relationships between functional entities; and whether there are any constraints on network locations of the functional entities of the architecture in the scenarios.

The WebRTC IMS architecture supports two different IMS registration scenarios that differ in the authentication method, and ownership of the WWSF (i.e. operator network or third party). For these scenarios, the eP-CSCF verifies that the UE is executing a WIC from an authorized WWSF.

NOTE 2: The example procedures in the following clauses are intended to demonstrate a way of realizing the scenarios. These procedures are not intended to constrain the security solutions provided by SA WG3 within the context of the agreed architecture and use cases.

Scenario 1: The user has a subscription with an individual IMPU and uses an IMS authentication mechanism (e.g. IMS digest) to authenticate with IMS. Clause A.2.1.2 provides detailed procedures for scenario 1.

Scenario 2: The user has a subscription with an individual IMPU but uses a web identity and authentication scheme to authenticate with the WWSF. The WWSF assigns IMS identities to the user based on the user's web identity (e.g. via database lookup or other translation means). Clause A.2.1.3 provides detailed procedures for scenario 2.

NOTE 3: A third scenario described here is also under consideration for inclusion in the Release but details will be investigated during the normative work. In this scenario, the user uses a web identity and authentication scheme to authenticate with the WWSF. The WWSF is located in a third party network and has a subscription with IMS for a wildcard IMPU. The WWSF assigns an IMS identity to each individual user from its assigned wildcard IMPU. The WIC uses the assigned IMS identity to access IMS services.

NOTE 4: This Release does not include support for either of the following optional enhancements to the third scenario: dynamic WWSF configuration; and provision for the third party to offer its communication services in addition to IMS services.

A.2.1.2 WIC registration of individual IMPU with IMS using IMS digest

The WIC obtains information needed for IMS registration (e.g. IMPI and IMPU) via unspecified means. For example, some of this information might be stored in cookies or local browser storage after visiting a secure web site provided by the IMS operator.

Figure A.2.1.2-1 shows a registration call flow where IMS digest is used to register the WIC.

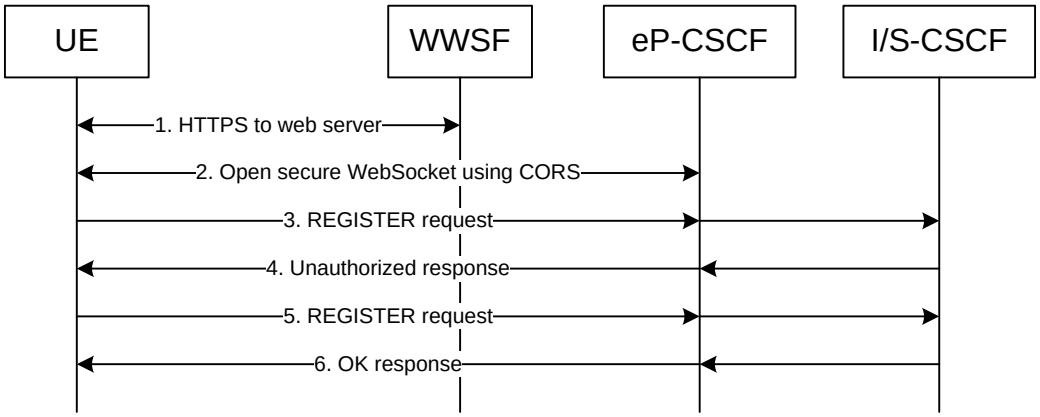


Figure A.2.1.2-1: WIC registration of individual IMPU with IMS using IMS digest

1. From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF.

2. The WIC opens a WSS connection to the eP-CSCF using standard cross-origin resource sharing (CORS, http://www.w3.org/TR/cors/) procedures to ensure that the WIC originated from a WWSF authorized to access this eP-CSCF.

3-6. The WIC initiates a registration transaction with IMS via the eP-CSCF by sending a REGISTER request to the eP-CSCF via the WSS connection. The REGISTER request includes IMS Digest authentication parameters, IMPI, IMPU and other information as needed for proper IMS registration. This request is translated in the IMS Core into an IMS registration process. This process leverages user credentials in HSS.

A.2.1.3 WIC registration of individual IMPU with IMS based on web authentication

Figure A.2.1.3-1 shows a registration call flow where the WIC registers with IMS based on web authentication with the WWSF.

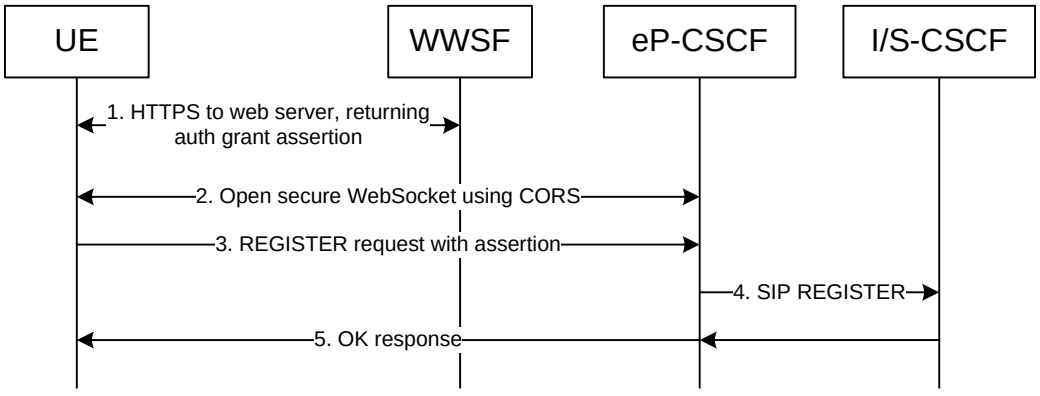


Figure A.2.1.3-1: WIC registration of individual IMPU based on web authentication

1. From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server

certificate. The browser downloads and initializes the WIC from the WWSF. The WWSF authenticates the user using a common web authentication procedure, determines the IMPI and IMPU assigned to the user (e.g., via an LDAP query to an identity database {not shown} using the authenticated identity as key), issues a security token for the user (e.g., where the security token is a JSON Web Token) and returns the IMS identities as claims within the security token to the WIC.

2. The WIC opens a WSS connection to the eP-CSCF using CORS procedures to ensure that the WIC originated from a WWSF authorized to access this eP-CSCF.

3. The WIC sends a REGISTER request to the eP-CSCF via the WSS connection. The request includes the user identity extracted from the claims in the security token, as well as the security token received from the WWSF as an attachment to the request.

4. The eP-CSCF validates the contents of the security token and confirms that the IMS identities being registered are authorized by the security token. The eP-CSCF then forwards the authorized REGISTER request to IMS to initiate authentication-less IMS registration using TNA procedures, with an indication that the authentication has already been carried out.

5. IMS returns a OK response to the WIC to confirm the successful IMS registration.

A.2.2 Origination and termination

Origination and termination flows for WebRTC IMS clients follow standard IMS procedures with the exception that routing of all messages between the WIC and S-CSCF traverse the eP-CSCF (rather than P-CSCF) and that parameters of Iq procedures take into account the WebRTC-specific extensions used by the WIC to send media. No further details are necessary.

Annex B:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2013-12	SP-62	SP-130543	-	-	MCC Editorial update for presentation to TSG SA for approval	0.3.0	1.0.0
2013-12	SP-62	SP-130706	-	-	Remove empty sections, renumber sections and update references; resolve hanging paragraphs.	1.0.0	1.0.1
2013-12	SP-62	-	-	-	MCC Editorial update to version 12.0.0 after TSG SA Approval.	1.0.1	12.0.0