**3GPP TSG-SA WG4 Meeting #127S4-240327**

**Sophia-Antipolis, France, 29 January – 2 February 2024**

**Source: NTT**

**Title: [FS\_eiRTCW] Pseudo-CR on updating Key Issue #1 and Solution #1**

**Spec: 3GPP TR 26.930**

**Agenda item: 10.9**

**Document for: Agreement**

1. **Introduction**

The pCR proposes to update the description of Key Issue #1 and Solution #1 (i.e., Architecture for eiRTCW).

**2. Reason for Change**

The following editor’s notes need to be solved.

Editor’s Note: The description of this solution will be updated based on the study on Key Issue #5 as needed.

Editor’s Note: Terminologies in this document will be clarified and aligned (e.g., clarification of correspondence between Web APP and WebRTC browser type endpoint).

**3. Proposal**

It is proposed to agree on the following changes to 3GPP TR 26.930.

To solve the editor’s notes, the following modifications are deployed.

* + Refining the words
    - Clarifying the description based on the definitions studied in Key Issue #5 (service control API) e.g., RTC resource, RTC ID resource, content provider, service provider.
    - Replacing “eiRTCW architecture” with “RTC architecture” to align with the description of TS 26.506.
  + Adding the NOTE to explain the correspondence between Web APP and WebRTC browser type endpoint.
  + Reconstruct the TR structure for readability. (e.g., clause 6.2.8.2 move to after clause 6.2.8.3.)

In addition to Key Issue# 5, Key Issue #6 (WSF discovery mechanism) and has the functional enhancement on the RTC architecture. Then the functionality for WSF discovery mechanism described in Solution #6 is reflected in the enhancements on RTC architecture.

\* \* \* First Change \* \* \* \*

## 5.2 Key Issue #1: Enhancements on RTC architecture

As described in 3GPP TS 26.506 [10], the detailed scenario and the RTC architecture for collaboration scenario 4 is FFS. This key issue identifies the scenarios and the possible enhancements on RTC architecture to realize collaboration scenario 4 in addition to collaboration scenario 3, based on the high-level network model described in clause 4.2.

This key issue includes:

1) Possible enhancements on functional entities and RTC architecture

- Study possible enhancements on functional entities and enhanced RTC architecture for collaboration scenario 4 in addition to collaboration scenario 3 based on general WebRTC implementation viewpoint.

2) Interaction with 5GC

- To realize the QoS control, study the interaction between functional entities in the enhanced RTC architecture and those in 5GC.

3) Media connection model

- Study the target use cases (i.e., connection model) of user plane (U-Plane) and considerations of QoS-enabled end-to-end path.

4) IP addressing

- Study the considerations on IP addressing related issues and identify the possible additional enhancements of ICE functionality.

5) Alignment and gap analysis between the enhanced RTC architectures and the current RTC architecture.

- Study the alignment between the enhanced RTC architecture derived from 1) – 4) and the current RTC architecture defined in 3GPP TS 26.506 [10]. This also includes gap analysis of functionalities between the architectures.

6) Enhanced architecture for collaboration scenario 4

- Study the expected architecture variant for the collaboration scenario 4 and enhancements on the current RTC architecture defined in 3GPP TS 26.506 [10], based on the gap analysis studied in 5). This also includes the clarifications on the focused functions and interfaces in this document.

\* \* \* Next Change \* \* \* \*

## 6.2 Solution #1: Enhancements on RTC architecture

### 6.2.1 Solution description

This solution addresses Key Issue #1.

This clause identifies the enhancements on RTC architecture considering what functionalities, functional entities and reference points are needed for WebRTC-based immersibe RTC services in collaboraion scenario 4. This includes:

1) Possible enhancements on functional entities and RTC architecture based on WebRTC view point (see clause 6.2.2);

2) Interaction between fuctional entities in the enhanced RTC architecture and 5GC (see clause 6.2.3);

3) Media connnection model (see clause 6.2.4);

4) IP addressing (see clause 6.2.5);

5) Alignment and gap analysis between the enhanced RTC architecture and the current RTC architecture (see clause 6.2.6); and

6) Enhanced RTC architecture for collaboration scenario 4.

As a conclusion of 1) to 6), the derivative RTC architecture and enhancements on 3GPP TS 26.506 [10] are proposed as a solution for Key Issue #1 in clause 6.2.8.

### 6.2.2 Possible enhancements on functional entities and RTC architecture based on WebRTC viewpoint

#### 6.2.2.1 Overview

Figure 6.2.2.1-1 depicts a possible enhanced RTC architecture based on the WebRTC viewpoint. It contains the functional entities described in clause 6.2.2.2 and reference points described in clause 6.2.2.3. The names of functional entities and reference points described here are only for discussion of this solution and the alignment of these names with 3GPP TS 26.506 [10] are considered in clause 6.2.7.

Figure 6.2.2.1-1: Possible RTC architecture from WebRTC viewpoint

WebRTC Signalling Function (WSF) and Conference Supporting Function (CSF) could co-locate in a physical node. WebRTC NNI Signalling Gateway Function (WNSGF) and WebRTC NNI Media Gateway Function (WNMGF) are optional when gateway functions are not needed at the network boundary.

#### 6.2.2.2 Functional entities for WebRTC

##### 6.2.2.2.1 General

This clause enumerates functional entities in terms of 1) WebRTC-related standardized specifications, 2) WebRTC implementations, and 3) providing inter-operator services.

1) Functional entities that are essential for this document and those already defined in IETF RFCs or 3GPP specifications concerning WebRTC (see clause 6.2.2.2.2).

2) Functional entities that are not directly defined in WebRTC-related specifications of IETF RFCs or 3GPP specifications but considered to be widely implemented for realizing WebRTC services; they are essential for this document (see clause 6.2.2.2.3).

3) Functional entities that may be specifically required for inter-operator or third-party collaboration services if modification of signalling and termination of media at network boundaries are needed (see clause 6.2.2.2.4).

##### 6.2.2.2.2 Functional entities defined in WebRTC-related standardized specifications

###### 6.2.2.2.2.1 UE (User Equipment)

6.2.2.2.2.1.1 General

User Equipment (UE) contains a user agent function which is equivalent to "WebRTC Endpoint" as described below. For the purposes of the present document, the following terms and definitions given in IETF RFC 8825 [33] are applied:

**WebRTC Endpoint**

- Either a WebRTC browser or a WebRTC non-browser. It conforms to the protocol specification.

**WebRTC Browser (also called a "WebRTC User Agent" or "WebRTC UA")**

- Something that conforms to both the protocol specification and the JavaScript API specification (W3C WebRTC 1.0 [44]).

NOTE: WebRTC browser is also called a "web app" in this document.

**WebRTC Non-Browser**

- Something that conforms to the protocol specification but does not claim to implement the JavaScript API. This can also be called a "WebRTC device" or "WebRTC native application".

Both "WebRTC Browser" type endpoint and "WebRTC Non-Browser" type endpoint are supported on the enhanced RTC architecture proposed in this document, as same as the current RTC architecture defined in 3GPP TS 26.506 [10]).

6.2.2.2.2.1.2 Considerations specific to WebRTC endpoint types

There are two types of WebRTC Endpoint; one is "WebRTC Browser" type, and the other is "WebRTC Non-Browser" type. This clause shows possible functional model for each type of endpoints on enhanced RTC architecture for identifying the specific issues related to the WebRTC endpoint types. If the RTC application provider connects its server (e.g., media server, content server) to a WSF in an operator network without providing WSF functionality (i.e., connect to the operator's WebRTC DN via UNI not NNI), the server is treated as UE (WebRTC endpoint) for the operator's network.

Regarding the "WebRTC Browser" type WebRTC endpoint, a JavaScript application runs on a web browser that has capabilities of JavaScript APIs including WebRTC APIs defined by W3C (see Figure 6.2.2.2.2.1.2-1). According to the concept of WebRTC described in IETF RFC 8829 [34], the procedures and protocols stated in this document are expected to be fully writable only with JavaScript.



Figure 6.2.2.2.2.1.2-1: "WebRTC Browser" type endpoint

However, in the current situation, most of the OSS (e.g., android, iOS) and the web browsers (e.g., chrome, firefox) do not support/provide the enablers (provided by RTC MSH) for immersive RTC as JavaScript API. Therefore, to provide functionalities for realizing immersive RTC on "WebRTC Browser" type WebRTC endpoint, the mechanisms other than RTC MSH need to be supported. In order to support "WebRTC Browser" type endpoint, the protocols and procedures in this document can be implemented without RTC MSH.

Regarding the "WebRTC Non-Browser" type WebRTC endpoint, an application written in a programming language specific to the UE platform runs on UE using libraries and/or system call handlers. (See Figure 6.2.2.2.2.1.2-2)



Figure 6.2.2.2.2.1.2-2: "WebRTC Non-Browser" type endpoint

NOTE: The programming language and programming APIs used to write applications depend on the UE platform. For example, Java and Android API (SDK) will be selected for Android platform UEs, Swift and its libraries will be selected for iOS platform UEs, and C++ and Win64 API will be selected for Windows platform UEs.

The application can be realized in a way other than JavaScript running on a web browser. The application can support the functions provided by RTC MSH since the application can be developed proprietary.

In this document, the solution which realizes the immersive RTC services without using RTC MSH is addressed to support both "WebRTC Browser" type endpoint and "WebRTC Non-Browser" type endpoint.

This document does not state details of the application's implementation; but the network interfaces, which is applicable for both "Browser" and "Non-Browser" type UEs are mainly described.

###### 6.2.2.2.2.2 WSF (WebRTC Signalling Function)

The WebRTC Signalling Function (WSF) is a functional entity that is responsible for WebRTC signalling mechanism including capability exchange and management of media sessions between UEs and the network. This functional entity is described as "Servers" or "Web Server" in clause 3 of IETF RFC 8825 [33]. Each operator or third-party in this document is assumed to have their own WSF(s) in their network.

WSF also provides the following functionalities:

- Interaction with WMCF for media session (real-time streaming and data channel) control.

- Interaction with CSF for collaboration with web applications/services.

- Interaction with 5GC, using Network Support function AF's (NS-AF) functionality.

##### 6.2.2.2.3 Functional entities widely implemented for WebRTC

###### 6.2.2.2.3.1 WMCF (WebRTC Media Centre Function)

The WebRTC Media Centre Function (WMCF) is a functional entity that performs media processing. WMCF terminates media path (including audio/video stream and data channel) and performs media processing (e.g., mixing, selective forwarding, transcoding) which are required for immersive RTC applications. It may also perform decryption and encryption of media packets if DTLS, SRTP, or TLS is used for a transport layer. It also has the function of storing contents (including text or other static material as well as audio and video) and providing them to the UE. For media transport control, the WMCF interacts with WSF.

In the case that the WMCF acts as a simple media relay function, the WMCF simply relays media data packets and supports IP packet connectivity. When UE behaves as ICE Agents defined in IETF RFC 8445 [29] or IETF RFC 8838 [36], WMCF may be either STUN servers defined in IETF RFC 8489 [31] for connectivity check or TURN servers defined in IETF RFC 8656 [32] for relaying media data packets. This functional entity facilitates NAT traversal of UE and the connectivity between UE and other network functions.

This functional entity is generally implemented in WebRTC Multipoint Control Unit (MCU) or Selective Forwarding Unit (SFU).

###### 6.2.2.2.3.2 CSF (Conference Supporting Function)

The Conference Supporting Function (CSF) is a functional entity that provides various functionality to realize WebRTC based RTC services with operator assistance. The CSF is expected to provide the following functionalities:

- Conference session management, i.e., "CRUD" operation – create, read, update, delete of conference instances.

NOTE 1: CSF needs to support service control APIs. The details of these APIs are addressed in Key Issue #5 and Solution #5.

- Providing supplementary files (e.g., icon images of participants, and shared documents) via best-effort transport different from the channels for real-time media.

- Storage of user subscription data specific to MNO's WebRTC services.

NOTE 2: In this document, it is assumed that a single user (i.e., identity) and its subscription data (associated with the identity) are assigned, owned, and managed by both operator and RTC application provider independently. The two identities have a link with each other via some technique. User subscription data specific to RTC application provider's services are stored in their networks.

- Authorization endpoint and token endpoint of OAuth 2.0 described in IETF RFC 6749 [22] for establishing authentication linkage between MNO's ID and RTC application provider's ID.

NOTE 3: OAuth token will be used to C-Plane authentication at WSF and RTC application providers. STUN/TURN authentication with OAuth token is defined in IETF RFC 7635 [25]. Portal http(s) servers of WebRTC services provide this function in general implementations.

##### 6.2.2.2.4 Functional entities needed for inter-operator services

###### 6.2.2.2.4.1 WNSGF (WebRTC NNI Signalling Gateway Function)

The WebRTC NNI Signalling Gateway Function (WNSGF) is located at the boundary of the RTC networks where different operator's or third-party RTC network connects.

Each operator or third-party has its own WebRTC Signalling Functions (WSF) so that WSFs are connected to each other with border control functions such as security, policy management, charging, etc. WNSGF is inserted into "Signalling Path" in Figure 2 of IETF RFC 8825 [33] and responsible for border control functions and supports session establishment between disparate address realm's networks.

Also, WNSGF is able to support the functionality for interworking between WebRTC based signalling message and SIP message of IMS as a border control function.

NOTE: The details of interworking with IMS network are addressed in Key Issue #7 and Solution #7.

###### 6.2.2.2.4.2 WNMGF (WebRTC NNI Media Gateway Function)

The WebRTC NNI Media Gateway Function (WNMGF) is a media relay located at the boundary of the RTC networks where different operator's or third-party RTC network connects. WNMGF is responsible for the border control and transport of media data packets between different RTC networks. WNMGF may also transcode media data packets.

Also, WNMGF is able to support the functionality for interworking between WebRTC media and IMS media (e.g., transcoding of codec) as a border control function.

NOTE: The details of interworking with IMS network are addressed in Key Issue #7 and Solution #7.

#### 6.2.2.3 Reference Points

The reference points shown in Figure 6.2.2.1-1 are enumerated as follows.

Reference points for signalling are called as "control plane" or "C-Plane" in this document. Reference points for media are similarly called as "user plane" or "U-Plane" in this document.

Reference Points for C-Plane:

**Rs-u:** Reference Point between a WSF and a UE.

**Rs-i:** Reference Point between a WSF and another WSF in the same network (DN) or between a WSF and a WNSGF.

**Rs-a:** Reference Point between a WSF and a CSF.

**Rs-n:** Reference Point between a WNSGF and another WNSGF in an external network.

Reference Points for U-Plane:

**Rm-u:** Reference Point between a WMCF and a UE.

**Rm-i:** Reference Point between a WMCF and another WMCF in the same network (DN) or between a WMCF and a WNMGF.

**Rm-n:** Reference Point between a WNMGF and another WNMGF in an external network.

Reference Points for signalling nodes to control media nodes:

**Mc-i:** Reference Point between a WSF and a WMCF.

**Mc-r:** Reference Point between a WNSGF and a WNMGF.

Other Reference Points:

**Rh-u:** Reference Point between a CSF and UE. This reference point is used for providing CSF functionalities (e.g., application usage assistance such as downloading an application) to UE.

**Rh-n:** Reference Point between a CSF and RTC application provider. This reference point is used for interaction between CSF and RTC application provider for media session set up related interaction.

Detailed protocol for each reference point will be discussed in the dedicated key issue and solution.

### 6.2.3 Interaction between functional entities in the enhanced RTC architecture and 5GC

#### 6.2.3.1 Overview

This clause shows a solution for integrating the enhanced RTC architecture based on pure WebRTC with 5GC. In other words, this clause identifies the possible interaction between the functional entities of the enhanced RTC architecture and the functional entities of 5GC.

NOTE: "pure WebRTC" means the original WebRTC described in IETF work, which basically does not consider domain specific functions or features (e.g., mobile networks).

#### 6.2.3.2 Mapping of functional entities for interaction with 5GC

##### 6.2.3.2.1 General

This clause identifies the mapping of functional entities shown in Figure 6.2.2.1-1 into 5GC functional entities defined in 3GPP TS 23.501 [4].

In this document, the mapping of WSF and AF, and the mapping of WNSGF and 5GC functional entities are considered. Other functional entities (i.e., CSF, WMCF, WNMGF) are not considered since these functional entities are not expected to interact with 5GC.

##### 6.2.3.2.2 WSF and AF

WSF is connected from UE and is expected to process the following:

1) authenticate a UE.

2) setup a WebRTC media session required by a UE, which may be in another network.

3) manage QoS for the media path of a WebRTC session.

Then it is expected that the WSF interacts with functional entities of 5GC and UE to perform 1) and 3) as the following:

1) WSF can retrieve the identity of a UE from 5GC, then authenticates and authorizes the UE.

3) WSF can request PCF to enable QoS control for the media path through e.g., N5, N32 (specified in 3GPP TS 23.501 [4]) or CAPIF reference points (specified in 3GPP TS 23.222 [2]).

NOTE: These processes are close to the processes of IMS functional entities such as P-CSCF and S-CSCF defined in 3GPP TS 23.228 [3]. The process of 1) is similarly performed by S-CSCF and UDM, and 3) is similarly performed by P-CSCF and PCF.

WSF can be mapped into "AF (Application Function)" of 5GC according to the definition of AF in 3GPP TS 23.501 [4] clause 5.2.10 due to the following reasons:

- WSF interacts with the 3GPP core network to provide services.

- The interaction between 5GC (e.g., PCF/UDM) and WSF is close to the interaction between 5GC and IMS entities (e.g., P-CSCF) that are AFs.

##### 6.2.3.2.3 WNSGF

###### 6.2.3.2.3.1 Overview

This clause identifies the mapping of WNSGF to a 5GC functional entity. There are a couple of possibilities currently identified. The following two 5GC functional entities can be mapped from WNSGF:

- NEF (see clause 6.2.3.2.3.2)

- SEPP (see clause 6.2.3.2.3.3)

As another possibility, it may be appropriate that WNSGF is mapped to a new functional entity (like Interconnection Border Control Function (IBCF) in IMS). The exact mapping of WNSGF is clarified in the alignment with 3GPP TS 26.506 [10] (clause 6.2.6 of this document).

###### 6.2.3.2.3.2 WNSGF and NEF

When WSF is mapped into an AF and if WNSGF is deployed as 5GC functional entity, WNSGF can be mapped into an NEF due to the following reasons:

- When WSF processes 2) of clause 6.2.3.2.2 and the media session relates to other operator's network, WSF (mapped to an AF) of operator-A is requested to interact with WNSGF on the boundary of operator-B to communicate with WSF (mapped into an AF) in operator-B due to operator-B's policy. In this model, the relationship between WSF (in operator-A) and WNSGF (in operator-B) is close to the relationship between AF and NEF described in clause 6.2.10 of 3GPP TS 23.501 [4].

- The major function of WNSGF is close to the former three functionalities described in 3GPP TS 23.501 [4] clause 6.2.5.0; WNSGF exposes WSF's WebRTC signalling capability and events. WNSGF interworks with WebRTC C-Plane signalling between Rs-i and Rs-n reference points in terms of security and translation of internal-external information.

When WNSGF is mapped into an NEF, the definition of the NEF may need to be modified as follows:

- Descriptions for the exposure of WSF's WebRTC signalling capability and the events by WNSGF are added in 3GPP TS 23.501 [4] clause 7.2.8.

- Descriptions for the event exposure details are added in 3GPP TS 23.502 [5] clause 4.15.3.

- Descriptions for the capability exposure details are added in 3GPP TS 23.502 [5] clause 5.2.6.

###### 6.2.3.2.3.3 WNSGF and SEPP

Security Edge Protection Proxy (SEPP) is defined in 3GPP TS 33.501 [12] and 3GPP TS 23.501 [4]. The SEPP is an entity sitting at the perimeter of the PLMN for protecting control plane messages, hiding network topology. The SEPP enforces inter-PLMN security on the N32 interface that is a reference point between a SEPP in one PLMN and a SEPP in another PLMN.

If WNSGF is deployed as 5GC functional entity, WNSGF is also located at the perimeter of the PLMN and its function is protecting control plane messages and hiding network topology. The function of WNSGF is close to that of SEPP.

The difference between WNSGF and SEPP is the type of located PLMN. WNSGF is located at the edge of inter-HPLMN. On the other hand, SEPP is expected to be used for N32 that lies between HPLMN and VPLMN.

###### 6.2.3.2.3.4 New functional entity

WNSGF is a border control function over C-Plane signalling path and located at the boundary of the networks where different operators or third-party network connects, as described in clause 6.2.2.2.4.1. Then, WNSGF is not expected to interact with 5GC functional entities and act as the gateway function for SBI.

In this document, the C-Plane signalling messages are expected to be exchanged via a DN over N6 interfaces and WNSGF is located at the DN. Therefore, WNSGF needs to be treated as a new border control function for C-Plane signalling path in WebRTC domain.

#### 6.2.3.3 Possible architecture integrated with 5GC

The functional entities shown in Figure 6.2.2.1-1 can be connected to 5GC as described in Figure 6.2.3.3-1.

Figure 6.2.3.3-1: Possible architecture integrated with 5GC

WSF (with NS-AF functionality of RTC architecture) is mapped into an AF as the 5GC viewpoint.

WSF (with NS-AF functionality of RTC architecture) is interconnected with PCF via N5 interface. WSF manages QoS of real-time media packets and C-Plane signalling packets via N5 interface. WSF may interact with UDM to authenticate and to authorize the UE.

Both signalling packets and media packets between UE and the network are transmitted via N6 interface. Signalling packets (C-Plane packets) from UE are transmitted to WSF, and real-time media packets (U-Plane packets) from UE are transmitted to WMCF. C-Plane signals may travel to WNSGF via Rs-i, and may travel further to other operator's WNSGF via Rs-n. U-Plane signals may travel to WNMGF via Rm-i, and may travel further to other operator's WNMGF via Rm-n. (see Figure 6.2.3.3-2)

Figure 6.2.3.3-2: Possible architecture from 5GC viewpoint with data flows of C/U-Planes

#### 6.2.3.4 Mapping to RTC collaboration scenarios

The following table shows the mapping of functional entities in this document into the collaboration scenarios described in 3GPP TS 26.506 [10]. Each box shows the condition (required or not) for MNO. The targets of this document are collaboration scenarios 3 and 4.

Table 6.2.3.4-1: Functional entities required for each collaboration scenarios

|  |  |  |  |
| --- | --- | --- | --- |
| Functional Entity | Collaboration Scenario 3 | | Collaboration Scenario 4 |
| 3A / Service Provider provides WebRTC services and MNO assists the services | 3B / MNO provides WebRTC services only in the MNO's network | MNO's WebRTC service interconnects with other MNO's or Service Provider’s service |
| WSF | Required | Required | Required |
| WMCF | Required | Required | Required |
| CSF | Required | Required | Required |
| WNSGF | N/A (NOTE) | N/A | Required |
| WNMGF | N/A (NOTE) | N/A | Required |
| NOTE: Scenario 3A in this table assumes service provider’s WebRTC functions communicate with WSF and WMCF via UNI-like interface, i.e., WSF and WMCF work as a gateway by themselves. Further Operator-Assistance models may be introduced. | | | |

### 6.2.4 Media connection model

#### 6.2.4.1 General

In the original WebRTC design, the communication between UEs is thought to be peer-to-peer (P2P). In most of the existing WebRTC implementations, however, the media connection is not P2P. An intermediate server (or servers) between UEs is used. In the multi-party call, the intermediate server which performs media processing is helpful for a UE because, for a UE, decoding all media from other UEs is a heavy load. Direct full-mesh connections among multiple UEs consumes a lot of network resources. Additionally, such an intermediate server is useful even for a one-to-one communication for offloading immersive media processing which needs more computation power than conventional media. This leads to the discussion about split rendering.

This document mainly focuses on the media connection model with intermediate servers.

P2P connection has some benefit for one-to-one communication (i.e., no need for an intermediate server and less server-relayed delay). For that reason, P2P connection is also considered for some special cases.

#### 6.2.4.2 Target use cases from network view

Based on the high-level network model and target interfaces described in clause 4.2 and the enhanced RTC architecture described in clause 6.2.2, a signalling protocol which is called as "RESPECT" in this document supports the following use cases of media session set up from network view.

<Media session set up with RTC resource served in the operator network via UNI>

a. UE 🡪 RTC Resource (served by the same operator) 🡨 UE

b. UE 🡪 RTC Resource (served by the same operator) 🡨 UE (CP)

<Media session set up with RTC resource via NNI>

c. UE 🡪 RTC Resource (served by the other operator)

d UE 🡪 RTC Resource (served by an SP)

e. UE (served by the other operator) 🡪 RTC Resource 🡨 UE (CP)

f. UE 🡪 Transit network (served by the other operator) 🡪 RTC Resource (served by an SP)

<Media session set up between UEs>

g. UE 🡪 UE (served by the same operator) without media gateway

h. UE 🡪 UE (served by the other operator) without media gateway

i. UE 🡪 UE (CP) without media gateway

j. UE (served by the other operator) 🡪 UE (CP) without media gateway

The overviews of these use cases are described below.

NOTE 1: Content provider connected via UNI is treated as UE.

NOTE 2: CSF is not shown in the figures for simplicity.

1. **UE 🡪 RTC Resource (served by operator) 🡨 UE**

- UE establishes a media session destined for an RTC ID resource (e.g., immersive conference room) served by the same operator. Figure 6.2.4.2-1 shows an example that UE\_A and UE\_B establish media sessions destined for the same RTC ID resource (e.g., immersive conference room) to communicate with each other.



Figure 6.2.4.2-1: UE 🡪 RTC Resource (served by the same operator) 🡨 UE

1. **UE 🡪 RTC Resource (served by operator) 🡨 UE (CP)**

- UE\_A and UE (CP) establish a media session destined for a RTC ID resource served by an operator network which UE\_A and UE (CP) connected to.



Figure 6.2.4.2-2: UE 🡪 RTC Resource (served by the same operator) 🡨 UE (CP)

1. **UE 🡪 RTC Resource (served by the other operator)**

- UE\_A establishes a media session destined for a RTC ID resource (e.g., Immersive conference room) served by the operator that different from the network which the UE\_A is connected to. In this scenario, the C-Plane signalling messages and media/data are sent over the NNI. Other UEs can connect to the RTC ID resource as same as use case a.



Figure 6.2.4.2-3: UE 🡪 RTC Resource (served by the other operator)

1. **UE 🡪 RTC Resource (served by an SP)**

- UE\_A establishes a media session destined for a RTC ID resource (e.g., Immersive conference room) served by an SP. In this scenario, the C-Plane signalling messages and media/data are sent over the NNI.



Figure 6.2.4.2-4: UE 🡪 RTC Resource (served by an SP)

1. **UE (served by other operator) 🡪 RTC Resource 🡨 UE (CP)**

- UE\_C in the other operator network than an operator network serving a RTC ID resource (e.g., Immersive conference room) and UE (CP) in the operator network serving the RTC ID resource establish a media session destined for the RTC ID resource. In this scenario, the C-Plane signalling messages and media/media from UE are sent over the NNI.



Figure 6.2.4.2-5: UE (served by the other operator) 🡪 RTC Resource 🡨 UE (CP)

1. **UE 🡪 Transit NW (other operator) 🡪 RTC Resource (served by an SP)**

- UE\_A establishes a media session with a RTC ID resource (e.g., Immersive conference room) served by an SP via transit network served by the another operator. In this scenario, the C-Plane signalling messages and media/data are sent over the two different NNIs.



Figure 6.2.4.2-6: UE 🡪 Transit network (served by the other operator) 🡪 RTC Resource (served by an SP)

1. **UE - UE (served by the same operator) without WMCF**

- UE\_A establishes a media session (e.g., voice chat) with UE\_B served by the same operator, without using WMCF.



Figure 6.2.4.2-7: UE - UE (served by the same operator) without media gateway

1. **UE 🡪 UE (served by the other operator) without WMCF**

- UE\_A establishes a media session (e.g., voice chat) with UE\_C served by the different operator, without using WMCF. In this scenario, the C-Plane signalling messages and media/data are sent over the NNI.



Figure 6.2.4.2-8: UE 🡪 UE (served by the other operator) without media gateway

1. **UE 🡪 UE (CP) without WMCF**

- UE\_A establishes a media session with a UE (CP) which is connected to the same operator, without using WMCF.



Figure 6.2.4.2-9: UE 🡪 UE (CP) without media gateway

1. **UE (connected to the other operator) 🡪 UE (CP) without WMCF**

- UE\_C establishes a media session with a UE (CP) which is connected to the different operator, without using WMCF. In this scenario, the C-Plane signalling messages and media/data are sent over the NNI.



Figure 6.2.4.2-10: UE (connected to the other operator) 🡪 UE (CP) without media gateway

#### 6.2.4.3 QoS-enabled end-to-end path

In the collaboration scenario where the WebRTC functions in an operator's network assists an external provider (i.e., service provider, content provider, or another operator), setting up a QoS-enabled media path across different networks needs to be considered.

The media path from a UE to the external provider is roughly divided into the following four sections:

Section 1) Between a UE and the UPF (operator's CN section)

Section 2) Between the UPF and the operator's network edge (operator's DN section)

Section 3) Between the operator's network edge and the external provider network edge

Section 4) A network in the external provider

Section 4) is a matter of an external provider and out of scope of this document.

Regarding Section 1), this section includes the operator's core network. In this section, QoS is controlled by the PCF.

Regarding Section 2), operator's DN may have sufficient bandwidth or the other QoS mechanism may be adopted.

Regarding Section 3), this section's QoS control needs a bandwidth guaranteed path (i.e., a dedicated line). On the enhanced RTC architecture described in clause 6.2.2, when the media path is connected to a RTC resource in other operator's network or service provider's network, the media packets to be prioritized are transmitted to WNMGF placed in the operator's network and the WNMGF relays the media to the main media server in the other operator's network or service provider's network via guaranteed path as shown in Figure 6.2.4.3-1 (red-line). If the media path is connected to a WebRTC endpoint function in a content provider's network via WSF and WMCF (which work as a gateway) in the operator's network, this section is treated as UNI, as shown in Figure 6.2.4.3-1 (blue-line).



Figure 6.2.4.3-1: Sections of end-to-end media path

### 6.2.5 IP Addressing

#### 6.2.5.1 Overview

IP addressing for UE has some options: assigning IPv4 address only, IPv6 address only, or both.

In the operator deployment, the number of available IPv4 addresses would be insufficient for its subscribers. Generally, operators use IPv4 private address (and ISP shared address defined in IETF RFC 6598 [21]) with network address translation (NAT).

In clause 6.2.5, appropriate IP addressing is identified, discussing NAT-traversal in the WebRTC user plane and network verified ID retrieval.

#### 6.2.5.2 NAT

##### 6.2.5.2.1 Overview

NAT, including port translation as NAPT (Network Address and Port Translation), is a method of mapping an IP address space into another, which is mainly used to translate a private IP address into a global IP address, and vice versa, for communicating with external networks.

Generally, UE can be assigned with an IP address through a PDU session in operator networks. When an IPv4 address is allocated, as mentioned in clause 6.2.5.1, a private IP address or an ISP shared address is used. On the contrary, when an IPv6 address is allocated, a global unicast address is assigned.

NAT is essential for carrier-grade network deployment. Subscribers can be much more than usually available IPv4 global address space, and they are treated by using IPv4 private address and NAT. The same private address can be reused in each different domain behind NAT. Although NAT deployments have a wide variety, NAT is generally installed in a DN (data network) and often put in the middle between the UPF and other functional entities (see Figure 6.2.5.2-1).

On the other hand, IPv6 global unicast addresses basically do not require NAT, except for special security reasons or some transition method between IPv6 and IPv4 domains.



Figure 6.2.5.2-1: Possible NAT location

##### 6.2.5.2.2 NAT Variation

NAT is classified into some types by its address translation and packet filtering behavior.

The first version of STUN in IETF RFC 3489 [17] defines three types:

- Full Cone NAT,

- Restricted NAT (Restricted Cone NAT or Restricted Port Cone NAT), and

- Symmetric NAT.

Full cone NAT does not limit access to an internal UE from external network entities, which have not communicated with the internal UE. Any external entities can re-use the external IP address and port number mapped to a specific internal UE and can access to it (Figure 6.2.5.2.2-1). Full cone NAT is less restrictive than other NATs. Restricted NAT only permits external entities to access the internal UE if the NAT have received any packets from the internal UE directed to the external UE (Figure 6.2.5.2.2-2). Symmetric NAT uses a different pair of an external IP address and port, which are specific to each external entity and only the external entity can access to the internal UE through the IP address and port pair.



Figure 6.2.5.2.2-1: Full Cone NAT behaviour



Figure 6.2.5.2.2-2: Restricted or Symmetric NAT behaviour

##### 6.2.5.2.3 Existing NAT-traversal

###### 6.2.5.2.3.1 General

An effective NAT-traversal method is different depending on the NAT type described in clause 6.2.5.2.2.

In the original WebRTC design, STUN and TURN are listed, included as ICE, for major NAT-traversal methods. In addition, Hosted NAT Traversal (HNT, described in IETF RFC 7362 [24]) and its similar mechanism are frequently used in real implementations for conversational applications.

###### 6.2.5.2.3.2 STUN

STUN is the method for UE behind the NAT to discover its external IP address observed by external networks. This method supports P2P communications and only works for full-cone NAT.

This document excludes STUN because the main communication model is not P2P but with intermediate servers (as described in clause 6.2.5), and general NATs deployed in operator networks are not limited to full-cone type.

###### 6.2.5.2.3.3 TURN

TURN is the method for UE behind the NAT to communicate with external nodes via an intermediate server. TURN is a protocol for the session management and requires an intermediate server.

Generally, this method is regarded as the last resort for NAT-traversal for UDP-based conversational services. This method does not require the alignment with other control plane signalling, but is equipped as its own user plane connection management mechanism. This method needs additional message exchanges and has a protocol overhead.

The TURN server has its authentication mechanism for UEs and can be used for the purpose of traffic steering for an inter-operator communication scenario detailed in clause 4.2.4.3.

###### 6.2.5.2.2.4 HNT

HNT (Hosted NAT Traversal) is the mechanism that a session border controller (SBC) placed at the edge of networks intermediates the communication between UEs behind NAT.

The problem tackled by HNT is that a UE behind a NAT tries to set up a session with its private address and port number for media, which have no clue to the SBC for the real media which comes later.

Regarding the control plane signalling, the signalling part of the SBC modifies media-related information represented by the private IP address and port number set in the SDP offered by an originating node into a global IP address and a new port number. This modification enables a terminating node to target the accessible IP address and port pair provided by the SBC. In the signalling return path, the SBC also modifies the terminating node's IP address and port number set in the SDP answered by the terminating node into new ones, and forwards it to the originating node. This is to solicit the originating node to send media to the SBC. Once the SBC receives the first media packet from the originating node targeting at the solicitation, the SBC recognizes the real NAT-ed IP address and port pair of the originating node. The SBC captures that information and uses it for relaying packets from the terminating node to the originating node. This is called "latching".

This method is embedded in the control plane signalling and does not require extra message exchange. For that reason, it has no additional protocol overhead. It is a better feature than TURN in the same condition requiring an intermediate server.

Since this document focuses on the connection model with an intermediate server, the NAT issues can be argued differently. Let's assume that all communication services are provided by the intermediate server as a conference. UEs can just join the open channel provided by the server and receives media from the server. UEs can also send their media to the intermediate server and the server mixes the media and distributes to other UEs. In this model, the first join packet from a UE to the NAT and the NAT to the server creates an address mapping at the NAT. The server simply sends packets to the source address of the join packet from the UE.

This mechanism does not need the dedicated protocol and there is no additional protocol overhead for NAT-traversal by sending media to the specific IP address and port pair exposed by WMCF. That points are analogous to HNT (Figure 6.2.5.2.2.4-1).



Figure 6.2.5.2.2.4-1: HNT like NAT-traversal

##### 6.2.5.2.4 Conclusion of NAT handling

NAT-traversal problems have been discussed and several solutions have been proposed as described above. However, if equipment for NAT-traversal is not required, certainly less server resources would be needed.

In short, it is preferable that only IPv6 global unicast address be assigned to UE and no dedicated NAT-traversal equipment be used. Intermediate servers are used mainly for media processing and for the media relay when there is no direct IP reachability (e.g., across inter-operator connection).

#### 6.2.5.3 IP Address and Trustable Subscriber Identifier

The operator uses subscription identifiers (e.g., GPSI (Generic Public Subscription Identifier) in 5GC) for managing its customer's service subscription and charging. In WebRTC support, the operator needs to check customer's service requests by checking against operator's subscriber database organized with the subscription identifier. An OTT-specific ID and password may be insufficient even in the collaboration scenario with external service providers because they cannot be securely linked with subscriber information in the viewpoint of the operator. The issue is how the MNO deduces (or retrieves) the trustable subscriber identifier from customer's requests, which are carried by IP packets.

Trustable subscriber identifiers in the MNO network are required for certain validity check, since a UE's self-claimed GPSI and source IP address are untrusted.

The EDGEAPP architecture specifies the method how the EAS function block retrieves the GPSI from terminal's source IP address. The AF regarded as an EAS can retrieve the GPSI bound to the UE by Eees\_UEIdentifier API in EDGEAPP. This mechanism and its flow contain authentications conducted at the related network functions (i.e., EES and NEF), which enable the EAS to acquire the valid GPSI in the operator network as a trustable subscriber identifier.

Validity of the terminal's source IP address needs consideration. UE's self-claimed IP address, especially presented in an application level, is not trustable. The source IP address presented in an IP header can be relatively trustable when the IP packet is transmitted through a connection with some handshake procedures.

The IP address linkage with a subscriber identifier also has an issue when NAT is deployed. In release 18, the method with which the AF can identify the trustable subscriber identifier (e.g., GPSI) to invoke the 3GPP network service API for the UE (Application client) remains to be investigated in eEDGEAPP. In VoLTE, this linkage with NAT can be achieved with the help of additional operator-specific information (e.g., PDN session related value). In the AF for WebRTC, it depends on which additional information element can be acquired by the AF. There is no clear answer for the ID linkage between the NAT-ed IP address and the subscriber identifier.

Contrarily, the UE IP address without translated by NAT can be linked with GPSI by Eees\_UEIdentifier API (though detailed specification is needed).

In terms of ID linkage, using IPv6 global unicast address for UE is reasonable.

Using IPv4 private address will be studied further when NAT-ed ID linkage issue is solved.

#### 6.2.5.4 Conclusion of IP Addressing

In terms of the required server resources for NAT-traversal and unclear retrieval of the trustable subscriber identifier, using IPv6 global unicast address for UE is reasonable. NAT deployments have a wide variety of behaviors and cannot be treated straightforward (refer to clause 6.2.5.2). Using media relay servers that act as either TURN or HNT covers most cases with NAT-traversal. However, there are still issues using IPv4 private address with NAT, such as ID linkage (refer to clause 6.2.5.3). For the sake of simplicity and to concentrate on identifying signalling requirements, this document considers IPv6-only use.

Then the use of ICE Function and the enhancements of ICE function are excluded from the scope of this document.

NOTE 1: As specified in 3GPP TS 26.506 [10], the use of ICE Function is optional and is not restricted.

NOTE 2: IPv6-only use is acceptable for future services because IPv6 address allocation to UEs is now widely available among operators. Also, IPv6-only deployment leads to efficient system development and equipment utilization.

### 6.2.6 Alignment and gap analysis between the enhanced RTC architecture and the current RTC architecture

#### 6.2.6.1 General

This clause identifies the architectural and functional mapping between enhanced RTC architecture described in clause 6.2.2 of this document and the current RTC architecture defined in 3GPP TS 26.506 [10]. Figure 6.2.6.1-1 shows the RTC general architecture specified in 3GPP TS 26.506 [10].



Figure 6.2.6.1-1: RTC General Architecture

#### 6.2.6.2 WebRTC endpoint and RTC endpoint on UE

WebRTC endpoint on the UE is expected to be mapped to RTC endpoint on the UE on the RTC architecture with the following consideration.

- An WebRTC endpoint includes signalling related aspects of applications on the UE, however, an RTC endpoint does not include applications on the UE. To support the signalling protocol for media session setup, the signalling related functionality of application needs to be included in the scope of the RTC endpoint. Note that application itself is not included in this scope.

#### 6.2.6.3 WSF and (RTC) WSF

WSF is expected to be mapped to WSF (integrated with NS-AF) on RTC architecture with the following considerations.

- WSF needs to support the functionality for interaction with Application Supporting Web Function (ASWF) for collaboration with web applications/services.

- WSF needs to support the functionality for interaction with 5GC, using network Support function (NS-AF) functionality.

- WSF needs to support the functionality for retrieval of the identity of a UE from 5GC, and authentication of the UE.

Regarding the retrieval of the identity of a UE from 5GC, as described in clause 6.2.5.4, the WSF is not able to retrieve the identity from 5GC in the case that the UE is assigned an IPv4 private address behind NAT in the current release. In that case, the authentication mechanism in commercial use such as SMS OTP (One Time Password) is possibly applicable for enhancement of authentication of the UE.

#### 6.2.6.4 WNSGF and Inter-working Function

Inter-working Function (IWF) is specified in 3GPP TS 26.506 [10] as an inter-working functionality to enable MNO-facilitated WebRTC sessions that involve endpoints across different MNOs (e.g., providing cross-network signalling functionality). This is the expected functionality for WNSGF, since WNSGF is a gateway function for signalling messages between MNOs. Then, WNSGF is expected to be mapped to IWF on RTC architecture.

No gap is found between WNSGF and IWF.

#### 6.2.6.5 CSF and Application Supporting Web Function

CSF is expected to be mapped to ASWF on RTC architecture. Also, the ASWF is expected to support the additional functionalities described in clause 6.2.2.2.3.2 in addition to the current functionality defined in 3GPP TS 26.506 [10].

#### 6.2.6.6 WMCF and Media Function

WMCF is expected to be mapped to Media Function (MF) on RTC architecture. Also, the MF is expected to support the following functionalities.

- Performing decryption and encryption of media packets if DTLS, SRTP, or TLS is used for a transport layer.

- Storing contents (including text or other static material as well as audio and video) and providing them to the UE.

#### 6.2.6.7 WNMGF and Transport Gateway Function

WNMGF is expected to be mapped to Transport Gateway Function (TGF) on RTC architecture.

No gap is found between WNMGF and TGF.

### 6.2.7 Enhanced RTC Architecture for collaboration scenario 4

This clause identifies the enhanced architecture for collaboration scenario 4 specified in 3GPP TS 26.506 [10] based on the consideration in above clauses. Figure 6.2.7-1 shows the derivative RTC architecture for collaboration scenario 4.



Figure 6.2.7-1: Possible derivative RTC architecture for collaboration scenario 4

NOTE 1: Other network includes RTC ASs in different MNO and service provider.

NOTE 2: If RTC AF and RTC AS are controlled by a single operator and located in the same operator network, these functions are trusted. Inter-working Function and Transport Gateway Function act as a border controller function at the boundary of the network.

The following interfaces are expected to be introduced for collaboration scenario 4.

- **RTC-Y**: This reference point is for C-Plane signalling and U-Plane media transport between RTC AS (Inter-working Function) and other RTC network or service provider network. This interface is necessary for inter-connect RTC-AS with other RTC network or service provider network to realize collaboration scenario 4. RTC-Y may further be grouped into two sub-interfaces as follows.

i) **RTC-Ys**: This interface is for C-Plane signalling between Inter-working Function and other RTC network or service provider network.

ii) **RTC-Ym**: This interface is for U-Plane media transport between Transport Gateway Function and other RTC network or service provider network.

The following interfaces are expected to be introduced/extended for collaboration scenario 3 and collaboration scenario 4. These interfaces are to enable operator assistance for RTC application providers and UEs, then these interfaces are used not only for inter-MNO scenario (Collaboration scenario 4) but also single MNO assistance scenario (Collaboration scenario 3).

- **RTC-X**: This interface is application interface between RTC AS and content provider, a form of RTC application provider. The interface is used for providing RTC AS functionalities via ASWF. (e.g., subscription of RTC resource in RTC-AS.). This interface is necessary for real-time interaction between RTC-AS and content provider for service control.

- **RTC-4m**: This interface needs to be extended for providing ASWF functionalities (e.g., application usage assistance such as downloading an application) to UE. This extension is necessary for providing RTC AS functionalities to UE as operator assistance.

The functional entities in Figure 6.2.2.1-1 correspond to the functions defined in 3GPP TS 26.506 [10] as follows:

- **WSF (WebRTC Signalling Function)**: WebRTC Signalling Function

- **WMCF (WebRTC Media Centre Function)**: Media Function

- **CSF (Conference Supporting Function)**: Application Supporting Web Function

- **WNSGF (WebRTC NNI Signalling Gateway Function)**: Inter-working Function

- **WNMGF (WebRTC NNI Media Gateway Function)**: Transport Gateway Function

NOTE 3: As described in 3GPP TS 26.506 [10], the integration/collocation of RTC AF and WebRTC signalling server is possible. Co-located WebRTC signalling server is able to act as a RTC AF which is accessible to 5GC, and replace some of this RTC AF's interfaces and APIs with WebRTC signalling. For example, interfaces and APIs between this RTC AF and UE will be replaced to avoid concurrent/redundant requests from UE.

The reference points in Figure 6.2.2.1-1 correspond to those defined in TS 26.506 [10] as follows:

- **Rs-u**: RTC-4s

- **Rs-n**: RTC-Ys

- **Rm-u**: RTC-4m

- **Rm-n**: RTC-Ym

- **Rh-u**: RTC-4m

- **Rh-n**: RTC-X

In the C-Plane signalling aspects, this document focuses on RTC-4 based solutions as shown in Figure 6.2.7-2 to support the collaboration scenario 4 and the case for the application which is not able to use MSH (e.g., Web App).

- RTC AF functionalities are integrated in WebRTC signalling function, since MSH is not used. Then, MSH related interfaces are omitted in Figure 6.2.7-2.

- Functions of RTC AF are integrated within WebRTC Signalling Function, then RTC-3 is out of the scope.

- The use and usage of ICE Function is optional functionality and is not used for non- NAT case. Then the extension of ICE functionality and its usage are outside the scope of this document, since no further extension is not identified in this document.

- The representation of RTC-4s and RTC-4m are simplified. Web App and Native WebRTC App are expected to use these interfaces as follows:

\* Web App utilizes the web browser's JS API (including WebRTC API) to send/receive signalling message on RTC-4s and media/data on RTC-4m.

\* Native WebRTC App utilizes the SDK provided by the OS of the UE to send/receive signalling message on RTC-4s and media/data on RTC-4m.



Figure 6.2.7-2: The focused interface of C-Plane signalling protocol

NOTE 4: RTC-4m is connected to ICE function when TURN server needs to be used. Otherwise, RTC-4m is connected to Media Function (MF) or Application Supporting Web Function (ASWF).

NOTE 5: The interfaces and the functionalities related to MSH, NS-AF, configuration function and provisioning function are not in the focus.

### 6.2.8 Proposed enhancements on RTC architecture

#### 6.2.8.1 General

In this clause, the followings are described as proposed enhancements on RTC architecture.

1) The derivative RTC architecture supporting collaboration scenario 3 and 4 (see clause 6.2.8.2)

2) Enhancements on functionality in RTC AS functional entities (see clause 6.2.8.3)

3) Enhancements on reference points (see clause 6.2.8.4)

4) Enhancements on architecture diagrams in 3GPP TS 26.506 (see clause 6.2.8.5)

#### 6.2.8.2 Derivative RTC architecture supporting collaboration scenario 3 and 4

This clause describes the derivative RTC architecture for collaboration scenario 3 and 4 according to the previous considerations. Figure 6.2.8.2-1 shows the derivative RTC architecture and reference points between RTC AS functions and other entities.



Figure 6.2.8.2-1: Derivative RTC architecture diagram

NOTE 1: WebRTC endpoint function of content provider connects to RTC AS via RTC-4s/RTC-4m (UNI). For simplicity, this line is snipped in this figure.

NOTE 2: NAT functionality and ICE functionality can be applied. However, these are snipped in this figure.

The derivative RTC architecture for collaboration scenario 3 and 4 with 5GC interaction viewpoint is shown in Figure 6.2.8.2-2. Network Support function (NS-AF) defined in 3GPP TS 26.506 [10] is integrated in the WSF to interact with 5GC via N5 interface.



Figure 6.2.8.2-2: Derivative RTC architecture diagram with 5GC interaction viewpoint

#### 6.2.8.3 Enhancements on functionality in RTC AS functional entities

##### 6.2.8.3.1 General

This clause describes the functionalities needed for the functional entities in the derivative RTC architecture, which are identified in this document.

##### 6.2.8.3.2 User Equipment

The User Equipment (UE) contains a user agent function for WebRTC. The user agent function is equivalent to "WebRTC Endpoint", which is either a WebRTC browser or a WebRTC non-browser as defined in IETF RFC 8825 [33]. The definitions of Web Browser and WebRTC Non-Browser in IETF RFC 8825 [33] are given below. WebRTC endpoint is the RTC endpoint supporting signalling related functionality of the application. Application itself is not scope of this document.

**WebRTC Browser (also called a "WebRTC User Agent" or "WebRTC UA")**: Something that conforms to both the protocol specification and the JavaScript API specification (W3C WebRTC 1.0 [44]).

NOTE 1: WebRTC browser is also called "web app" in this document.

**WebRTC Non-Browser**: Something that conforms to the protocol specification but does not claim to implement the JavaScript API. This can also be called a "WebRTC device" or "WebRTC native application".

When a content provider provides a service via UNI, the content provider acts as UE (i.e., WebRTC endpoint). Since this is not considered in the current versions of 3GPP TS 26.506 [10], a certain clarification on "content provider" in 3GPP TS 26.506 [10] is expected.

This document identifies the following functionality needed for the UE. Since these functionalities are not defined in the current versions of 3GPP TS 26.506 [10], the enhancement on the functional definition in 3GPP TS 26.506 [10] is expected.

- Support of WSF discovery mechanism (NOTE 2)

NOTE 2: This solution does not address the details of WSF discovery mechanism since this is addressed in Key Issue #6 and Solution #6.

##### 6.2.8.3.3 WebRTC Signalling Function

The WebRTC Signalling Function (WSF) is one of the RTC AS functional entities defined in 3GPP TS 26.506 [10]. The WSF is responsible for WebRTC signalling including capability exchange and management of media sessions between UEs and the RTC network. This functional entity is described as "Servers" or "Web Server" in clause 3 of IETF RFC 8825 [33]. Each operator or third-party in this document is assumed to have their own WSF in their RTC network.

This document identifies the following functionalities needed for the WSF. Since these functionalities are not defined in the current versions of 3GPP TS 26.506 [10], the enhancements on the functional definition in 3GPP TS 26.506 [10] are expected.

- Interaction with MF for media session control

- Interaction with ASWF for collaboration with web applications/services.

- Interaction with 5GC, using network Support function (NS-AF).

- Authentication/authorization of the UE.

- Functionalities derived from service control API (i.e., connection control enforcer and RTC ID resource handling enforcer). (NOTE 1)

- Signing and verification of network-asserted UE's ID. (NOTE 2)

NOTE 1: This solution does not address the details of service control API since this is addressed in Key Issue #5 and Solution #5.

NOTE 2: This solution does not address the details of signing and verification of network-asserted UE’s ID since this is addressed in Key Issue #10 and Solution #10.

NOTE 3: Regarding the retrieval of the identity of a UE from 5GC for authentication of UE, the WSF is not able to retrieve the identity from 5GC in the case that the UE is assigned an IPv4 private address behind NAT in the current release. In that case, the authentication mechanism in commercial use such as SMS OTP (One Time Password) is possibly applicable for enhancement of authentication of the UE.

##### 6.2.8.3.4 Media Function

The Media Function (MF) is one of the RTC-AS functional entity defined in 3GPP TS 26.506 [10]. The MF performs media processing. MF terminates media path (including data channel path) and performs media processing (e.g., mixing, selective forwarding, transcoding) which are required for immersive RTC applications. The MF is able to perform decryption and encryption of media packets if DTLS, SRTP, or TLS is used for a transport layer. The MF has the function of storing contents (including text or other static material as well as audio and video) and providing them to the UE. For Media transport control, the MF is able to interact with WSF.

In cases where an MF performs as a simple media relay function, the MF simply relays media data packets and supports IP packet connectivity. When a UE behave as ICE agents defined in IETF RFC 8445 [29] or IETF RFC 8838 [36], the MF may be either STUN servers defined in IETF RFC 8489 [31] for connectivity check or TURN servers defined in IETF RFC 8656 [32] for relaying media data packets. This functional entity facilitates NAT traversal of UE and the connectivity between UE and other network functions.

This functional entity is generally implemented in WebRTC Multipoint Control Unit (MCU) or Selective Forwarding Unit (SFU).

This document identifies the following functionality needed for the MF. Since the functionality is not defined in the current versions of 3GPP TS 26.506 [10], the enhancement on the functional definition in 3GPP TS 26.506 [10] is expected.

- Functionalities derived from service control API (i.e., media data forwarding control enforcer and RTC exchange resource handling enforcer for service control).

NOTE: This solution does not address the details of service control API since this is addressed in Key Issue #5 and Solution #5.

##### 6.2.8.3.5 Application Supporting Web Function

The Application Supporting Web Function (ASWF) is one of the RTC AS functional entities defined in 3GPP TS 26.506 [10]. This document identifies the following functionalities needed for the ASWF. Since these functionalities are not clearly defined in the current versions of 3GPP TS 26.506 [10], the enhancements on the functional definition in 3GPP TS 26.506 [10] are expected.

- Exposing the service control APIs. (NOTE 1)

- Storage of user subscription data specific to MNO's WebRTC services. (NOTE 2)

- Authorization endpoint and token endpoint of OAuth 2.0 described in IETF RFC 6749 [22] for establishing authentication linkage between MNO's ID and RTC application provider's ID. (NOTE 3)

- Providing supplementary files (e.g., icon images of participants, and shared documents) via best-effort transport different from the channels for real-time media.

- Providing WSF discovery functionality (NOTE 4).

NOTE 1: This solution does not address the details of service control APIs since this is addressed in Key Issue #5 and Solution #5.

NOTE 2: In this document, it is assumed that a single user (i.e., identity) and its subscription data (associated with the identity) are assigned, owned, and managed by both MNO and application provider independently. The two identities have a link with each other via some technique. User subscription data specific to application provider's services are stored in their networks.

NOTE 3: OAuth token will be used to C-Plane authentication at WSF and RTC application providers. STUN/TURN authentication with OAuth token is defined in IETF RFC 7635 [25]. Portal http(s) servers of WebRTC services provide this function in general implementations.

NOTE 4: This solution does not address the details of WSF discovery functionality since this is addressed in Key Issue #6 and Solution #6.

##### 6.2.8.3.6 Inter-working Function

The Inter-working Function (IWF) is one of RTC AS functional entity defined in 3GPP TS 26.506 [10]. The IWF is located at the boundary of the RTC network where different operator or third-party network inter-connects.

The IWF is inserted into "Signalling Path" in Figure 2 of IETF RFC 8825 [33] and responsible for border control functions and supports session establishment between disparate address realm's networks. By inserting the IWF into "Signalling Path", each operator or 3rd-party network can securely inter-connect with the other network.

This document identifies the following functionalities needed for the IWF. Since these functionalities are not defined in the current versions of 3GPP TS 26.506 [10], the enhancements on the functional definition in 3GPP TS 26.506 [10] are expected.

- C-plane signalling protocol interworking between RTC network and IMS network. (NOTE 1)

- Signing and verification of network-asserted UE's ID. (NOTE 2)

NOTE 1: This solution does not address the details of interworking with IMS network since this is addressed in Key Issue #7 and Solution #7.

NOTE 2: This solution does not address the details of signing and verification of network-asserted UE’s ID since this is addressed in Key Issue #10 and Solution #10.

##### 6.2.8.3.7 Transport Gateway Function

The Transport Gateway Function (TGF) is one of RTC AS function entity defined in 3GPP TS 26.506 [10]. The TGF is a media relay located at the boundary of the RTC network where different operator or third-party inter-network connects. The TGF is the function responsible for the border control and transport of media data packets between different networks. The TGF is responsible for the border control and transport of media data packets between different networks.

This document identifies the following functionality needed for the TGF. Since the functionality is not defined in the current versions of 3GPP TS 26.506 [10], the enhancement on the functional definition in 3GPP TS 26.506 [10] is expected.

- U-Plane protocol interworking between RTC network and IMS network.

NOTE: This solution does not address the details of interworking with IMS network since this is addressed in Key Issue #7 and Solution #7.

#### 6.2.8.4 Enhancements on reference points

The reference points shown in Figure 6.2.8.2-1 (Derivative RTC architecture diagram) are listed in Table 6.2.8.4-1.

The reference points marked as "No" in the 3rd column of Table 6.2.8.4-1 are expected to be introduced in 3GPP TS 26.506 [10].

Table 6.2.8.4-1: Reference points used for derivative RTC architecture

|  |  |  |
| --- | --- | --- |
| Reference point  (NOTE) | Descriptions | 3GPP TS 26.506 [10] already define? |
| RTC-4 | Reference Point between an RTC network and a UE for C/U-Plane. | Yes |
| RTC-4s | Reference Point between a WSF and a UE for C-Plane signalling. | Yes |
| RTC-4m | Reference Point between a MF and a UE or between an ASWF and a UE for U-Plane. | Yes |
| RTC-X | Reference Point between a ASWF and a content provider network for service control. | No |
| RTC-Y | Reference Point between an RTC network and another network (i.e., other operator network or service provider network) for C/U-Plane. | No |
| RTC-Ys | Reference Point between a IWF and another network (i.e., other operator network or service provider network) for C-Plane signalling. | No |
| RTC-Ym | Reference Point between a TGF and another network (i.e., other operator network or service provider network) for U-Plane. | No |
| N5 | Reference Point between a WSF and PCF in 5GC. | Yes |
| NOTE: RTC-X/Y reference points need to be assigned/defined considering the common architecture for 5GMS and RTC. | | |

#### 6.2.8.5 Enhancements on architecture diagrams in 3GPP TS 26.506

This clause describes the expected enhancements on architecture diagrams in 3GPP TS 26.506 [10].

The expected enhancements on RTC general architecture are shown in Figure 6.2.8.5-1. RTC-4 reference point is connected to UE rather than WebRTC Framework since the interface is used for C-Plane signalling between application in the UE and RTC AS in addition to U-Plane media (audio/video stream) and data between RTC endpoint and RTC AS. RTC-X reference point and RTC-Y reference point are newly introduced.

NOTE 1: RTC-X is applicable between the RTC AS (ASWF) and the content provider in Figure 6.2.8.5-1.



Figure 6.2.8.5-1: Expected enhancements on RTC General Architecture

Figure 6.2.8.5-2 shows the expected enhancements on derivative RTC architecture for collaboration scenario 3 defined in 3GPP TS 26.506 [10]. RTC-4m reference point is clarified that this interface is used for providing ASWF functionality to UE, and RTC-X reference point is newly introduced to provide the service control API for content provider, a form of RTC application provider, from ASWF.

NOTE 2: RTC-X is applicable between the RTC AS (ASWF) and the content provider in Figure 6.2.8.5-2.



Figure 6.2.8.5-2: Expected enhancements on derivative architecture for collaboration scenario 3

Figure 6.2.8.5-3 shows the expected derivative RTC architecture for collaboration scenario 4. Collaboration scenario 4 supports inter-operable WebRTC services. Then collaboration scenario 3 is extended with functions and interfaces to support MNO to MNO inter-operability. RTC-Y (RTC-Ys and RTC-Ym) reference point is introduced to support the inter-connection between MNO's RTC ASs.

NOTE 3: RTC-X is applicable between the RTC AS (ASWF) and the content provider in Figure 6.2.8.5-3.

NOTE 4: Other RTC network in Figure 6.2.8.5-3 includes other operator's network and service provider's network.

Figure 6.2.8.5-3: Expected derivative architecture for collaboration scenario 4

### 6.2.9 Solution evaluation

The proposed architecture in clause 6.2.8 supports the functionalities and capabilities to support immersive RTC services for collaboration scenario 4 (also applicable for collaboration scenario 3) and the architecture is consistent with RTC architecture in 3GPP TS 26.506 [10]. Then it is proposed to;

- reflect the architectural enhancements on functional entities, reference point described in clause 6.2.8 into the stage 2 specification of RTC (i.e., 3GPP TS 26.506 [10]) and

- based on the above enhancements, update the architecture diagrams (RTC general architecture, derivative architectures for collaboration scenario 3 and 4.

\* \* \* End of Changes \* \* \* \*