**3GPP TSG-WG SA4 Meeting #124**

**Berlin, DE, 22nd – 26th May 2023 Revision of S4-230802**

|  |
| --- |
| *CR-Form-v12.2* |
| **PSEUDO CHANGE REQUEST** |
|  |
|  | **26.113** | **CR** |  | **rev** |  | **Current version:** | **0.5.5** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Updates to the SWAP protocol |
|  |  |
| ***Source to WG:*** | Qualcomm Inc. |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | iRTCW |  | ***Date:*** | 16th May 2023 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | This pCR fixes a few mistakes and describes the operation of the SWAP protocl. |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

|  |
| --- |
| **First Change** |

###### 6.2.4.4.3.2 Parameters

type: the type parameter may either be “ack” or “error”

source: the source identifier of the request message source that corresponds to this response message.

request: the message identifier of the request

description: in case of an error response, this field provides a description of the error message. In case of an acknowledgement, this description field is optional.

|  |
| --- |
| **Second Change** |

###### 6.2.4.4.4.2 Parameters

offer: a string that includes the SDP description for the offer.

matching\_criteria: an array that contains the matching criteria for the target endpoint. Each object shall comply with the definition of a matching criteria as described in clause 6.2.4.4.2.

|  |
| --- |
| **Third Change** |

##### 6.2.4.4.5 Accept message

###### 6.2.4.4.5.1 Description

If the connection request is accepted by the remote endpoint, it shall reply with an accept message. The accept message shall contain the answer SDP.

###### 6.2.4.4.5.2 Parameters

target\_id: this parameter represents the source id of the target endpoint.

answer: This parameter shall contain the answer SDP.

##### 6.2.4.4.6 Update message

###### 6.2.4.4.6.1 Description

The update message may be sent by any of the endpoints of a WebRTC session. It contains the updated SDP, which may add, update, or remove one or more local media streams. If accepted, the remote endpoint shall reply with an accept message.

###### 6.2.4.4.6.2 Parameters

target\_id: this parameter represents the source id of the target endpoint.

sdp: The updated local SDP that is transmitted to the remote endpoint.

##### 6.2.4.4.7 Reject message

###### 6.2.4.4.7.1 Description

In case the remote endpoint does not accept the offer or update message, it shall respond with the reject message. The message shall contain a reference to the corresponding offer or update message as well as a description of the reason why the message was rejected.

###### 6.2.4.4.7.2 Parameters

source

target\_id: this parameter represents the source id of the target endpoint.

request: the message identifier of the request

error\_id: an identifier of the error message

description: a description of the error message.

##### 6.2.4.4.8 Close message

###### 6.2.4.4.8.1 Description

The close message may be triggered by any of the two endpoints of a WebRTC session. Upon reception, the endpoint shall respond with an accept message, after which the WebRTC session is torn down and the resources associated with the WebRTC session are released.

###### 6.2.4.4.8.2 Parameters

target\_id: this parameter represents the source id of the target endpoint.

###### 6.2.4.4.9 Application message

###### 6.2.4.4.9.1 Description

Application-specific message may be defined by the application and exchanged between the endpoints of a WebRTC session. The message shall contain a type that uniquely identifies the type of the application message. If an application message type is not supported, it shall be rejected by the remote endpoint.

###### 6.2.4.4.9.2 Parameters

###### 6.2.4.4.6.2 Parameters

target\_id: this parameter represents the source id of the target endpoint.

type: the type of the application message shall be a URN that uniquely identifies the application message type.

value: an object that contains the application message content.

#### 6.2.4.7 Protocol Operation

SWAP is an acknowledged protocol for WebRTC. Each message that the WebRTC signaling server receives shall be acknowledged after proper processing. This is valid for the case where one of the endpoints acts as the signaling server. The Response message may also indicate an error, in case the received message cannot be processed and forwarded properly.

SWAP uses the following error messages:

|  |
| --- |
| **Description** |
| Message type unknown |
| Message malformatted |
| Target cannot be located |
| Unauthorized |

The WebRTC Signaling Function uses the (source id, target id) pairs of the communicating endpoints to identify the session and properly route the messages. Note that in the first connect message, the target id might not be known. In such a case, routing is done based on the matching criteria.