**3GPP TSG-SA3 Meeting #95-LIs3i240725**

**Las Vegas, United States, 29th Oct 2024 - 1st Nov 2024**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **33.127** | **CR** | **0252** | **rev** | **2** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  | Web RTC Access to IMS  |
|  |  |
| ***Source to WG:*** | SA3LI (Ministère Economie et Finances) |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | LI19 |  | ***Date:*** | 2024-10-30 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-19 |
|  | *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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | Lack of Web RTC Access to IMS architecture for LI (It has been already defined in TS 33.107) |
|  |  |
| ***Summary of change:*** | Define as IRI-POI the WWSF and eP-CSCF WWSF and eP-CSCF shall provide the IRI-POI |
|  |  |
| ***Consequences if not approved:*** | Regulatory issue |
|  |  |
| ***Clauses affected:*** | 3.3; 7.X;  |
|  |  |
|  | **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:*** | s3i240645,s3i240677 |

**\*\*\* Start of First Change \*\*\***

## 3.3 Abbreviations

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

5GC 5G Core Network

5GMS 5G Media Streaming

5GS 5G System

AAnF AKMA Anchor Function

AC Application Client

ACR Application Context Relocation

ADMF LI Administration Function

AF Application Function

AF\_ID Application Function Identity

AKA Authentication and Key Agreement

A-KID AKMA Key IDentifier

AKMA Authentication and Key Management for Applications

AMF Access and Mobility Management Function

AS Application Server

AUSF Authentication Server Function

BBIFF Bearer Binding Intercept and Forward Function

BSS Business Support System

CAG Closed Access Group

CC Content of Communication

CP Control Plane

CP NF Control Plane Network Function

CPIM Common Presence and Instant Messaging

CPS Call Placement Service

CSI Cell Supplemental Information

CSP Communication Service Provider

CSR Cell Site Report

CUPS Control and User Plane Separation

DN Data Network

DNAI Data Network Access Identifier

DoNAS Data over NAS

EAP Extensible Authentication Protocol

EAS Edge Application Server

ECGI E-UTRAN Cell Global Identifier

eCNAM Enhanced Calling Name

ECSP Edge Computing Service Provider

E-CSCF Emergency – Call Session Control Function

EDN Edge Data Network

EEC Edge Enabler Client

EECID Edge Enabler Client IDentifier

EES Edge Enabler Server

eIMS-AGW enhanced IMS-AGW

eP-CSCF enhanced P-CSCF

GPSI Generic Public Subscription Identifier

HMEE Hardware Mediated Execution Enclave

HR Home Routed

IBCF Interconnection Border Control Functions

ICF Identity Caching Function

IEF Identity Event Function

IMS-AGW IMS Access Gateway

IM-MGW IM Media Gateway

IP Interception Product

IQF Identity Query Function

IRI Intercept Related Information

KAF AKMA Application Key

KAKMA AKMA Anchor Key

KID Key IDentifier

KLI Decryption key(s) for services encrypted by CSP-provided keys

KSF Key Server Function

LAF Location Acquisition Function

LALS Lawful Access Location Services

LARF Location Acquisition Requesting Function

LBO Local Break Out

LEA Law Enforcement Agency

LEMF Law Enforcement Monitoring Facility

LI Lawful Interception

LI CA Lawful Interception Certificate Authority

LICF Lawful Interception Control Function

LI\_HI1 Lawful Interception Handover Interface 1

LI\_HI2 Lawful Interception Handover Interface 2

LI\_HI3 Lawful Interception Handover Interface 3

LI\_HI4 Lawful Interception Handover Interface 4

LI\_HILA Lawful Interception Handover Interface Location Acquisition

LI\_HIQR Lawful Interception Handover Interface Query Response

LIID Lawful Interception Identifier

LIPF Lawful Interception Provisioning Function

LIR Location Immediate Request

LI\_SI Lawful Interception System Information Interface

LISSF Lawful Interception State Storage Function

LI\_ST Lawful Interception State Transfer Interface

LI\_T1 Lawful Interception Internal Triggering Interface 1

LI\_T2 Lawful Interception Internal Triggering Interface 2

LI\_T3 Lawful Interception Internal Triggering Interface 3

LI\_X0 Lawful Interception Internal Interface 0

LI\_X1 Lawful Interception Internal Interface 1

LI\_X2 Lawful Interception Internal Interface 2

LI\_X2\_LA Lawful Interception Internal Interface 2 Location Acquisition

LI\_X3 Lawful Interception Internal Interface 3

LI\_X3A Lawful Interception Internal Interface 3 Aggregator

LI\_XEM1 Lawful Interception Internal Interface Event Management Interface 1

LI\_XER Lawful Interception Internal Interface Event Record

LI\_XLA Lawful Interception Internal Interface Location Acquisition

LI\_XQR Lawful Interception Internal Interface Query Response

LMF Location Management Function

LMISF LI Mirror IMS State Function

LMISF-CC LMISF for the handling of CC

LMISF-IRI LMISF for the handling of IRI

LTF Location Triggering Function

MA Multi-Access

MANO Management and Orchestration

MDF Mediation and Delivery Function

MDF2 Mediation and Delivery Function 2

MDF3 Mediation and Delivery Function 3

MRFP Multimedia Resource Function Processor

MSRP Message Session Relay Protocol

N3A Non-3GPP Access

N3IWF Non 3GPP Inter Working Function

N9HR N9 Home Routed

NAS Non-Access Stratum

NCGI NR Cell Global Identity

NEF Network Exposure Function

NFV Network Function Virtualisation

NFVI Network Function Virtualisation Infrastructure

NFVO Network Function Virtualisation Orchestrator

NIDD Non-IP Data Delivery

NPLI Network Provided Location Information

NR New Radio

NRF Network Repository Function

NSSF Network Slice Selection Function

NWDAF Network Data Analytics Function

OSS Operations Support System

PAG POI Aggregator

PCF Policy Control Function

P-CSCF Proxy - Call Session Control Function

PEI Permanent Equipment Identifier

PGW PDN Gateway

PGW-C PDN Gateway Control Plane

PGW-U PDN Gateway User Plane

POI Point Of Interception

PLMN Public Land Mobile Network

PTC Push to Talk over Cellular

RCD Rich Call Data

RCS Rich Communication Suite

S8HR S8 Home Routed

SCEF Service Capability Exposure Function

SCS Service Capability Server

SGW Serving Gateway

SGW-C Serving Gateway Control Plane

SGW-U Serving Gateway User Plane

SHAKEN Signature-based Handling of Asserted information using toKENs

SIRF System Information Retrieval Function

S-CSCF Serving - Call Session Control Function

SIP Session Initiation Protocol

SMF Session Management Function

SMSF SMS-Function

STF Security Terminating Function

STIR Secure Telephony Identity Revisited

SUCI Subscriber Concealed Identifier

SUPI Subscriber Permanent Identifier

TAI Tracking Area Identity

TF Triggering Function

TLS Transport Layer Security

TNGF Trusted Non-3GPP Gateway Function

TrGW Transit Gateway

TWIF Trusted WLAN Interworking Function

UDM Unified Data Management

UDR Unified Data Repository

UDSF Unstructured Data Storage Function

UPF User Plane Function

VNF Virtual Network Function

VNFC Virtual Network Function Component

WAF WebRTC Authorisation FunctionW-AFG Wireline Access Gateway Function

WIC WebRTC IMS Client

WWSF WebRTC Web Server Function

xCC LI\_X3 Content of Communication

xIRI LI\_X2 Intercept Related Information

**\*\*\* End of First Change \*\*\***

**\*\*\* Start of Second Change \*\*\***

## 7.X LI at eP-CSCF for WebRTC access to the IMS

### 7.X.1 Background

Web Real-Time Communication (WebRTC) adds real-time communication to the browser with a focus on peer-to-peer communication. It enables multimedia interaction capabilities in web browsers on any platform without installing a specific plug-in or using a third-party application. WebRTC leaves the signalling plan to service developers, who are free to implement any call control protocol, e.g., SIP over secure WebSocket, XMPP (Extensible Messaging and Presence Protocol) over WebSocket, etc. The only requirement is that the session negotiation data be represented by the SDP (Session Description Protocol). WebRTC clients may have access to IMS through mediation functions for signalling and media. The enhanced P-CSCF (eP-CSCF) is the endpoint for the signalling connection from the WebRTC IMS Client (WIC) and is located in the operator network. The enhanced IMS-AGW (eIMS-AGW) is the endpoint for the media connection from the WIC.

Figure U.1.2-1 of TS 23.228 [13] gives an overview of WebRTC IMS architecture.

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. It provides a web page, which is the user interface (UI) for the user. The WebRTC Authorisation Function (WAF) creates an authentication token for the user and deliver it to the WWSF. The WAF is used in the case of IMS registration scenario using Web Authentication and is not used in the case of IMS registration scenario using IMS Authentication.

NOTE: The LI aspects when the WWSF is provided by third party, is not addressed in the present document.

### 7.X.2 Architecture

The WWSF and eP-CSCF shall provide the IRI-POI function. Figure 7.X.2 gives a reference point representation of the LI architecture with WWSF and eP-CSCF as CP NFs providing the IRI-POI function for WebRTC access to the IMS. This LI architecture is valid in non-roaming situations.



Figure 7.X.2-1 LI architecture for WebRTC access to the IMS

The eP-CSCF shall adhere to all LI requirements pertaining to the P-CSCF in addition to the LI requirements pertaining to the support of WebRTC access to IMS.

The IMS-AGW of the IMS LI architecture detects the media to be intercepted and generates the associated xCC.

### 7.X.3 Target identities

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the WWSF:

- IMPU.

- IMPI.

- NAI (i.e., Web Identity).

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the eP-CSCF:

- IMPU.

- IMPI.

### 7.X.4 IRI events

The IRI-POI in the WWSF shall generate the following xIRIs.

- WIC authorization.

- Start of interception with already authorized WIC.

The IRI-POI in the eP-CSCF shall generate the following xIRI:

- Encapsulated signalling message.

The WIC authorization xIRI is generated when the IRI-POI present in the WWSF detects that the WIC uses a Web identity in the form of an NAI to authenticate with the WWSF and obtains an authorization token.

The start of interception with already authorized WIC xIRI is generated when the IRI-POI present in the WWSF detects that interception is activated on the target WIC that has already been authenticated using its Web identity.

The encapsulated signalling message xIRI is generated when the IRI-POI present in the eP-CSCF detects that a signalling message (e.g., SIP over WebSocket, XMPP over WebSocket, etc) is received from, or sent to, a target WIC.

**\*\*\* End of Second Change \*\*\***

**\*\*\* End of Last Change \*\*\***