**3GPP SA3LI#88-e-a S3i230072**

**eMeeting; January 23-27, 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.127** | **CR** | **197** | **rev** | **1** | **Current version:** | **17.7.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Corrections to the RCS clause – diagrams and further clarity on the descriptions | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3-LI (Nokia, Nokia Shanghai Bell, OTD, AT&T) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI17 | | | | |  | ***Date:*** | | | 2023-01-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | ***F*** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 can be 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:*** | | The architecture diagram for RCS shows the triggered and non-triggered POIs as one box in the HTTP Content Server. This way of showing can be interpreted to infer that POIs used for RCS have two X1 interfaces (one LI\_X1 and one LI\_T2/T3) which violates to the ETSI 103 221-1 rules. Either the triggered and non-triggered POIs have to be shown separately or two separate diagrams have to be used to illustrate the two cases. Since having a triggered and non-triggered POI in the HTTP Content Server can happen for the same warrant depending on the scenario, the former approach is considered in this CR. Also, the recent discussions need some changes to the stage 2 descriptions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The labelling of the box is changed from "Content HTTP Server" to "HTTP Content Server/File Transfer Localisation Function". Two separate boxes are added to separate of the triggered and non-triggered POIs. Additional changes to reflect the recent discussion results. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The diagram can be read as conflicting with the ETSI 103 221-1 rules of only one ADMF can make changes to an NE over X1. The stage 2 details are not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.13.2.1, 7.13.4.1, 7.13.2.2.2, 7.13.4.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | S3i230017 | | | | | | | | |

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

#### 7.13.2.1 Overview

The capabilities defined in this clause and the following subclauses apply to the LI for RCS. The LI architecture and functionality for RCS builds on the LI capabilities defined for IMS (see clause 7.4). When LI for RCS is required, the LI functions in IMS are provisioned as described in clause 7.4.

The network functions involved in providing the interception of RCS events are determined based on the deployment option, the network configuration, LI service scope and the RCS communication type. In general, the LI functions involved in the interception of RCS events are located either in the IMS core or in RCS specific network functions.

Additional topology options for RCS are described in clause 7.13.2.2.

The present document refers to any server that provides support, services or functions for RCS as an RCS Server. In general, RCS Servers are IMS Application Servers. The HTTP Content Server supports file upload, URI generation, and file download to allow for the transfer of files over RCS.

The following sub-clauses contain general stage 2 details for LI for RCS.

The RCS Servers shall have LI capabilities to generate xIRI records and xCC when RCS events related to the target UE are handled. The HTTP Content Server shall have LI capabilities to generate xIRI records and xCC when the target UE uploads or downloads a file and when any user downloads a file previously uploaded by a target. If an IRI-TF or CC-TF is required, the relevant RCS Server shall have the CC-TF. The figure 7.13.2-1 gives a reference point representation of the LI architecture for RCS interception.



Figure 7.13.2-1: LI architecture for RCS services

The LICF present in the ADMF receives the warrant from an LEA, derives the intercept information from the warrant and provides it to the LIPF.

The LIPF present in the ADMF provisions the IRI-POI present in each RCS Server, the IRI-TF in the relevant RCS Servers, the MDF2 and the MDF3 over the LI\_X1 interfaces.

If the authentication method used to authenticate at the HTTP Content Server uses a permanent identifier, the LIPF present in the ADMF also provisions the IRI-POI in the HTTP Content Server.

To enable the interception of the target's message contents (e.g. when the warrant requires the interception of communication contents), the CC-POI in each RCS Server and the CC-TF present in the relevant RCS Servers are also provisioned with the intercept data.

If the authentication method used to authenticate at the HTTP Content Server uses a permanent identifier and the interception of the target's communication contents is required, the LIPF present in the ADMF also provisions the CC-POI in the HTTP Content Server.

NOTE 1: The IRI-POI, CC-POI, IRI-TF and CC-TF represented in figure 7.13.2-1 are logical functions and require correlation information be shared between them; they may be handled by the same process within the NF.

NOTE 2: The details on which RCS Servers require IRI-POIs, CC-POIs, and IRI-TFs or CC-TFs is dependent on implementation.

NOTE 3: The IRI-POI, CC-POI represented in figure 7.13.2-1 with LI\_T2, LI\_T3, and LI\_X1 (Management) interfaces are the triggered POIs and are logically separate from the non-triggered IRI-POI, CC-POI represented in figure 7.13.2-1 with LI\_X1 interface.

NOTE 4: The use of File Transfer Localisation Function (figure 7.13.2-1) is a deployment option for the CSP. See clause 7.13.2.2.2 for the details when File Transfer Localisation Function is deployed.

The IRI-POI present in the relevant RCS Server detects RCS registration and deregistration; session establishment, modification, and deletion; and message related events, generates and delivers the related xIRI to the MDF2 over LI\_X2. The MDF2 delivers the IRI messages to the LEMF over LI\_HI2.

When the IRI-TF present in the RCS Server detects a URI for file transfer, the IRI-TF present in the RCS Server sends a trigger to the IRI-POI in the HTTP Content Server over the LI\_T2 interface.

The IRI-POI present in the HTTP Content Server detects file uploads, downloads, or retrieval (i.e. by File Transfer Localisation Function, see clause 7.13.2.2.2), generates and delivers the related xIRI to the MDF2 over LI\_X2. The MDF2 delivers the IRI messages to the LEMF over LI\_HI2.

When interception of communication contents is required, the CC-POI present in the relevant RCS Server generates the xCC from RCS messages and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI\_HI3.

When interception of communication contents is required, the CC-TF present in the RCS Servers sends a trigger to the CC-POI present in the HTTP Content Server over the LI\_T3 interface.

The trigger sent from the IRI-TF to the IRI-POI or the CC-TF to the CC-POI includes the following information:

- File detection rules.

- Target identity.

- Correlation information.

- MDF3 address.

The CC-POI present in the HTTP Content Server generates the xCC from the uploaded file and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI\_HI3.

#### 7.13.4.1 General RCS IRI events

As described in clause 7.13.2, the term RCS Server in the present document refers to any server performing support, services or functions for RCS. In most deployments there will be more than one RCS Server, and the events listed below shall be intercepted in the server responsible for performing the functions described by the event.

The IRI-POI present in the RCS Servers shall generate xIRI when it detects the following specific events or information:

- Registration.

- Deregistration.

- Capability discovery.

- RCS message.

- RCS message report.

- Session establishment.

- Session modification.

- Session release.

- Group chat establishment.

- Group chat modification.

- Group chat release.

- Start of interception with already registered UE.

- Start of interception with already established session.

- Unsuccessful procedure.

The IRI-POI present in the HTTP Content Server shall generate xIRI when it detects the following specific events or information:

- File upload.

- File download.

- Unsuccessful procedure.

NOTE 1: In the following paragraphs, when the requirement applies to both target UE and target non-local ID, the term "target" is used.

The registration xIRI is generated when the IRI-POI present in an RCS Server detects that a target UE has been registered for RCS services.

The deregistration xIRI is generated when the IRI-POI present in an RCS Server detects that a target UE has been deregistered from RCS services.

The capability discovery xIRI is generated when the IRI-POI present in the RCS Server detects that a target UE has updated the target UE’s RCS capabilities. This xIRI is also generated when a target UE gets information about the capabilities and state of another RCS user.

The RCS message xIRI is generated when the IRI-POI present in an RCS Server detects that a target sends or receives an RCS message.

The RCS message report xIRI is generated when the IRI-POI present in an RCS Server detects that a target sends or receives a response to an RCS message.

The session establishment xIRI is generated when the IRI-POI present in an RCS Server detects that an RCS session has been created for a target.

The session modification xIRI is generated when the IRI-POI present in an RCS Server detects that an RCS session has been modified for a target.

The session release xIRI is generated when the IRI-POI present in an RCS Server detects that an RCS session has been released for a target.

The group chat establishment xIRI is generated when the IRI-POI present in an RCS Server detects that the target has joined an RCS group chat session.

The group chat modification xIRI is generated when the IRI-POI present in an RCS Server detects that a group chat session the target is participating in is modified.

The group chat release xIRI is generated when the IRI-POI present in an RCS Server detects that the target leaves a group chat session.

The start of interception with already registered UE xIRI is generated when the IRI-POI present in an RCS Server detects that interception is activated on the target UE that is already registered for RCS services.

The start of interception with an established RCS session xIRI is generated when the IRI-POI present in an RCS Server detects that interception is activated on a target UE that has an already established RCS session. When a target UE has multiple RCS sessions, this xIRI shall be sent for each RCS session with a different value of correlation information.

When additional warrants are activated on a target UE, MDF2 shall be able to generate and deliver the start of interception with already registered UE and start of interception with already established RCS session related IRI messages to the LEMF associated with the warrants without receiving the corresponding xIRI.

The file upload xIRI shall be generated when the IRI-POI in the HTTP Content Server detects that a target UE has uploaded a file or when any UE has uploaded a file destined for the target non-local ID.

The file download xIRI shall be generated when the IRI-POI in the HTTP Content Server detects that a target has downloaded a file or when any UE has downloaded a file previously uploaded by a target UE.

The unsuccessful procedure xIRI is generated when the IRI-POI present in an RCS Server or HTTP Content Server detects that a target UE initiated communication procedure (e.g. session establishment, RCS Message) is rejected or not accepted by the RCS Server before the proper NF handling the procedure itself is involved. The unsuccessful procedure xIRI is also generated when the IRI-POI present in the RCS Server or HTTP Content Server detects that any request from the target UE is not accepted by the RCS Server or HTTP Content Server.

##### 7.13.2.2.2 Implementations that have a File Transfer Localisation Function

As described in GSMA RCC.07, clause 4.1.15.3 [35], the terminating CSP may utilize a File Transfer Localisation Function which retrieves objects from the originating HTTP Content Server and makes the same available to the terminating user.

If the CSP implements a File Transfer Localisation Function, in addition to the architecture information in clause 7.13.2.1, the following requirements apply.

The LI architectue for the File Transfer Localisation Function is depicted in figure 7.13.2-1.

When the IRI-TF present in the RCS Server detects a URI for an incoming file transfer, the IRI-TF present in the RCS Server sends a trigger to the IRI-POI in the File Transfer Localisation Function over the LI\_T2 interface. When interception of communication contents is required, the CC-TF present in the RCS Servers sends a trigger to the CC-POI present in the File Transfer Localisation Function over the LI\_T3 interface. The trigger sent from the TF to the POI includes the following information:

- File detection rules.

- Target identity.

- Correlation information.

- MDF2 (for xIRI) or MDF3 (for xCC) address.

If the authentication method used to authenticate at the File Transfer Localisation Function uses a permanent identifier (see clause 7.13.3), the LIPF present in the ADMF also provisions the IRI-POI in the File Transfer Localisation Function.

In both cases, the IRI-POI present in the File Transfer Localisation Function detects file retrieval (i.e. from the HTTP Content Server) or downloads, generates and delivers the related xIRI to the MDF2 over LI\_X2. The MDF2 delivers the IRI messages to the LEMF over LI\_HI2.

If the authentication method used to authenticate at the File Transfer Localisation Function uses a permanent identifier and the interception of the target's communication contents is required, the LIPF present in the ADMF also provisions the CC-POI in the Localisation Function.

If the interception of communications content is required, the CC-POI present in the File Transfer Localisation Function generates the xCC from the retrieved file and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI\_HI3.

#### 7.13.4.3 RCS events for topologies utilising a Localisation Function

The events specified in clause 7.13.4.1 apply with the following changes:

In addition to the IRI-POI present in the HTTP Content Server (as described in clause 7.13.4.1), the IRI-POI present in the Localisation Function shall generate xIRI when it detects the following specific events or information:

- File transfer.

- File download.

-- Unsuccessful procedure.

The file download xIRI shall be generated when the IRI-POI in the Localisation Function detects that a target UE has downloaded a file or when any UE has downloaded a file previously sent from target non-local ID.

The file transfer xIRI shall be generated when the IRI-POI in the File Transfer Localisation Function detects that File Transfer Localisation Function retireves a file destined to the target UE from the HTTP Content Server. The file transfer xIRI shall also be generated when the IRI-POI in the File Transfer Localisation Function detects that File Transfer Localisation Function retrieves a file from the HTTP Content Server when the file was sent from a target non-local ID.

The unsuccessful procedure xIRI is generated when thi IRI-POI present in the File Transfer Localisation Function detects that any request from the target UE is not accepted by the File Transfer Localisation Function.

### \*\* End of all Changes \*\*