**3GPP TSG- Meeting #**

**, , -**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *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:***  |  |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *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:*** | There are times encapsulated RCS payloads may need to have unauthorised information removed prior to being included in an IRI record sent over LI\_HI2. In addition, there needs to be a way to signal what information was removed and how it was removed in order for the payload to be correctly decoded and the integrity of the remaining information to be preserved. This CR provides details on information that may need to be removed. |
|  |  |
| ***Summary of change:*** | Details added to the main document for information that may need to be removed from RCS messages.Predefined payload modifications are added to the enumeration in the ASN.1. |
|  |  |
| ***Consequences if not approved:*** | Details for how to remove unauthorised information from RCS will remain undefined. |
|  |  |
| ***Clauses affected:*** | 7.4.1, 7.4.5.3, 7.13.X, M.2.4.4, Attachment TS33128Payloads.asn |
|  |  |
|  | **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 is associated with the following changes in the Forge:Merge request: [!229](https://forge.3gpp.org/rep/sa3/li/-/merge_requests/229) Commit hash: [28521fee1309df29ff6ca292da2bb73cc086915e](https://forge.3gpp.org/rep/sa3/li/-/merge_requests/229/diffs?commit_id=28521fee1309df29ff6ca292da2bb73cc086915e) |
|  |  |
| ***This CR's revision history:*** | S3i230573 |

## \*\*\*\* START OF FIRST CHANGE (MAIN DOCUMENT) \*\*\*\*

### 7.4.1 Introduction

Stage 3 intercept capabilities for SMS at an SMSF are defined in clause 6.2.5. Details on how to remove unauthorised content from SMS messages are defined in clause 7.4.5.2.

Stage 3 for MMS interception follows in clause 7.4.3.

Stage 3 intercept capabilities for RCS are defined in clause 7.13. Details on how to remove unauthorised content from encapsulated RCS messages are defined in clause 7.13.X.

## \*\*\*\* START OF NEXT CHANGE (MAIN DOCUMENT) \*\*\*\*

#### 7.4.5.3 RCS Redaction

When content is not authorised, the unauthorised information shall be redacted from the encapsulated payload reported within an RCS related IRI record prior to its delivery over LI\_HI2.

When location is not authorised the unauthorised information shall be redacted from the encapsulated payload reported within an RCS related IRI record prior to its delivery over LI\_HI2.

See clause 7.13.X for additional details on redacting unauthorised information from RCS records.

## \*\*\*\* START OF NEXT CHANGE (MAIN DOCUMENT) \*\*\*\*

### 7.13.X Redaction of unauthorised information from encapsulated RCS payloads

#### 7.13.X.1 General

RCS consists of multiple layers of protocols, each of which may include information that, depending on the warrant, is not authorized for delivery. If the RCS implementation uses protocols other than SIP and MSRP, the modifications specified below shall be adapted as required to redact the unauthorised information and the modifications made shall be described within the IRI delivered to the LEA using the structure described in Annex M clause 2.2.

All of the requirements for the redaction of unauthorised information from IMS record payloads (see clause 7.12.9) shall also apply to encapsulated RCS payloads.

#### 7.13.X.2 Redaction of location information

##### 7.13.X.2.1 General

Depending on the RCS event being reported and the implementation, location information may be present in the headers of one or more protocol layers, the body of one or more protocol layers, or both.

In all cases, if content is authorised, location information present in the content portion of a user generated payload shall not be redacted.

When location is not authorised, all location information shall be redacted from the encapsulated RCS payload prior to its delivery over LI\_HI2. As such, when location is not authorised, the MDF2 and, optionally, the IRI-POIs in the RCS Server, the supporting IMS elements, and any RCS file transfer elements shall be provisioned with the payload modifications detailed in the subclauses below.

Additionally, if the location present in the RCS payload is the location of the non-target party, and this information is not authorised, the location shall be redacted.

If an implementation has location information in other portions of the payload, when the location is included the appropriate modifications shall be made to the encapsulated payload in addition to those specified below prior to the delivery of the message over LI\_HI2.

##### 7.13.X.2.2 Redaction of location information from presence information

If the geopriv element of presence information is considered to be location, the Content-Type of any body part at any layer of the RCS message is "application/pidf+xml", and if the presence information contains a geopriv element, the character data of each element within each location-info element shall be overwritten with the zero character such that the length of the element does not change.

##### 7.13.X.2.3 Redaction of location information from CPIM messages

In some cases, the information that would normally be present in the P-Access-Network-Info or Cellular-Network-Info headers of a SIP message is sent as implementation specific headers within the CPIM headers. In this case, these headers shall be redacted as described in clause 7.12.9.2 when the delivery of P-Access-Network-Info or Cellular-Network-Info is not authorised.

#### 7.13.X.3 Redaction of communications content

##### 7.13.X.3.1 General

In some cases portions of an encapsulated RCS payload may contain communications content. Unless otherwise specified, all communications content shall be redacted from the encapsulated payload prior to its delivery over LI\_HI2. As such, the MDF2 and, optionally, the IRI-POIs in the RCS Server, the supporting IMS elements, and any RCS file transfer elements shall be provisioned with the payload modifications detailed in the subclauses below.

If an implementation has communications content in other portions of the payload, the appropriate modifications shall be made to the encapsulated payload in addition to those specified below prior to the delivery of the message over LI\_HI2.

##### 7.13.X.3.2 Redaction of text content

If the Content-Type of any body part at any layer of the RCS message is "text" or any of the subtypes of "text", the contents of that body part shall be overwritten with the space character in the original encoding such that the length of the body remains unchanged.

##### 7.13.X.3.3 Redaction of content from the Subject header field

If the delivery of the content of the Subject header is unauthorised, each character of the field-value of the Subject header of any body part of any layer of the RCS message shall be replaced with a space.

##### 7.13.X.3.4 Redaction of content from Geolocation PUSH messages

If the delivery of Geolocation PUSH messages is unauthorised, if the Content-Type of any body part at any layer of the RCS message is "application/vnd.gsma.rcs-ft-http+xml":

- the value of the label attribute of the data element of the rcspushlocation element shall be overwritten with the "space" character such that the length of the attribute does not change.

- the value of the id attribute of the data element of the rcspushlocation element shall be overwritten with the "space" character such that the length of the attribute does not change.

- the character data of each element within each location-info element shall be overwritten with the zero character such that the length of the element does not change.

##### 7.13.X.3.5 Redaction of URLs from file transfer messages

If the delivery of the URL of a file being transferred is not authorised, if the Content-Type of any body part at any layer of the RCS message is "application/vnd.gsma.rcs-ft-http+xml":

- the value of any url attribute of the data element of the file-info element shall be overwritten with the "space" character such that the length of the attribute does not change.

## \*\*\*\* START OF NEXT CHANGE (MAIN DOCUMENT) \*\*\*\*

## M.2.2 Predefined modifications

The current document provides details for the following predefined methods for redacting unauthorised information from encapsulated payloads:

- SMS TP-User-Data content redaction as described in clause 7.12.9.3.2.

- IMS location and content information redaction as described in clause 7.12.9.

- RCS location and content information redaction as described in clause 7.13.X.

## \*\*\*\* START OF NEXT CHANGE (MAIN DOCUMENT) \*\*\*\*

### M.2.4.4 Enumeration: PredefinedPayloadModification

The PredefinedPayloadModifiation shall be set to indicate which predefined payload modification profile was used on the reported modified payload.

Table M.2.4.4-1: Enumeration for PredefinedPayloadModification parameter

|  |  |
| --- | --- |
| Enumeration | Description |
| pANILocationRemoval(1) | Shall be selected if location information was redacted from an encapsulated P-Access-Network-Info header using the process described in clause 7.12.9.2.2. |
| cNILocationRemoval(2) | Shall be selected if location information was redacted from an encapsulated Cellular-Network-Info header using the process described in clause 7.12.9.2.3. |
| sIPGeolocationInfoRemoval(3) | Shall be selected if location information was redacted due to the presence of a Geolocation header using the process described in clause 7.12.9.2.4. |
| presenceInformationLocationRemoval(4) | Shall be selected if location information was redacted from the geopriv element of an encapsulated presence information document using the process described in clause 7.12.9.2.5. |
| tS33128SMSTPDURedaction(5) | Shall be selected if content is redacted from an encapsulated SMS TPDU using the process described in clause 7.4.5.2. |
| tS33128TruncatedSMSTPDU(6) | Shall be selected if content is removed from an encapsulated SMS TPDU using the process described in clause 6.2.5.3. |
| iMSTextContentRemoval(7) | Shall be selected if content is redacted from an encapsulated SIP message using the process described in clause 7.12.9.3.3. |
| iMSSubjectContentRemoval(8) | Sall be selected if content is redacted from an encapsulated SIP message using the process described in clause 7.12.9.3.4. |
| rCSPresenceLocationRemoval(9) | Shall be selected if location is redacted from the geopriv element of an encapsulated presence information document using the process described in clause 7.13.X.2.2. |
| rCSCPIMLocationRemoval(10) | Shall be selected if location in the form of a P-Access-Network-Info header is redacted from application specific CPIM headers using the process described in clause 7.13.X.2.3. |
| rCSTextContentRemoval(11) | Shall be selected if text content is removed from the an RCS message. |
| rCSSubjectContentRemoval(12) | Shall be selected if content is removed from the Subject header of a layer of an RCS Message using the process described in clause 7.13.X.3.3. |
| rCSGeolocationPUSHContentRemoval(13) | Shall be selected if content is removed from an RCS Geolocation PUSH message using the process described in clause 7.13.X.3.4. |
| rCSFileTransferURLRedaction(14) | Shall be selected if URL content is redacted from an RCS File Transfer message as described in clause 7.13.X.3.5. |

## \*\*\*\* END OF MAIN DOCUMENT CHANGES \*\*\*\*

## \*\*\*\* START OF FIRST CHANGE (ATTACHMENTS) \*\*\*\*

---a/33128/r18/TS33128Payloads.asn
+++b/33128/r18/TS33128Payloads.asn

@@ -6935,7 +6935,13 @@ PredefinedPayloadModification ::= ENUMERATED

6935 6935 tS33128SMSTPDURedaction(5),

6936 6936 tS33128TruncatedSMSTPDU(6),

6937 6937 iMSTextContentRemoval(7),

6938 - iMSSubjectContentRemoval(8)

 6938 + iMSSubjectContentRemoval(8),

 6939 + rCSPresenceLocationRemoval(9),

 6940 + rCSCPIMLocationRemoval(10),

 6941 + rCSTextContentRemoval(11),

 6942 + rCSSubjectContentRemoval(12),

 6943 + rCSGeolocationPUSHContentRemoval(13),

 6944 + rCSFileURLContentRemoval(14)

6939 6945 }

6940 6946

6941 6947 PayloadModificationDescription ::= SEQUENCE

## \*\*\*\* START OF NEXT CHANGE (ATTACHMENTS) \*\*\*\*

## \*\*\*\* END OF ALL CHANGES \*\*\*\*