**3GPP TSG- Meeting #**

**, , -**

|  |
| --- |
| *CR-Form-v12.3* |
| **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:*** | , Motorola |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | Alignment with SA6 regarding logging, recording, audit and discreet monitoring. |
|  |  |
| ***Summary of change:*** | Replacing of the term “audit” with “replay”, and adding clarification regarding the decryption of user media. |
|  |  |
| ***Consequences if not approved:*** | Terminology mismatch between SA3 and SA6 specifications. |
|  |  |
| ***Clauses affected:*** | 10.1.1, 10.1.2.3, 10.2.1, 10.2.4  |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 1st change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 10 Logging, Recording, Replay and Discreet Monitoring

## 10.1 Logging and replay of service metadata

### 10.1.1 Overview

The MC system generates service metadata. The full range of user events that may be logged by the MC system is out-of-scope of the current specification. This clause defines the security and communications-related data associated to user events that are required to enable the replay of MC user actions within the MC system. Logging of user events is required to support replay service.

To ensure the privacy of MC users’ data, where this information is collected it shall be protected as defined in Clause 10.1.2.4.

### 10.1.2 User events

#### 10.1.2.1 Void

#### 10.1.2.2 Void

#### 10.1.2.3 Security content within user event logs

When a user event occurs in a log, the following security-related information is required:

- IP addresses (source and destination)

- Signalling layer identifiers

- SIP URI (source and destination).

- HTTP target URL

- The initiating user or server

- The receiving user, group, server or [set of multicast users]

- Security parameters (if present in signalling):

- MIKEY message

- Access or Security Token

 - Identifiers for related media bearers (if applicable).

NOTE: These logs are required to support discreet monitoring or replay of user media.

#### 10.1.2.4 Protection of user event logs

User event logs need to be protected as they contain information that impacts the user's privacy. It is up to a user organization how the User event logs shall be encrypted and integrity protected while stored. The user organization is also responsible for granting access to user event logs. This access shall only be granted to authorised users and such access shall be logged.

## 10.2 Replay and Discreet Monitoring of Service Media

### 10.2.1 Overview

Disceet Monitoring is access to service media at a network element within the MC Domain. Where Discreet Monitoring is used to access to user voice communications, it is known as Discreet Listening. Discreet Monitoring includes access to voice, video and data communications. For discreet monitoring the access to media is in real-time. For replay service, the access to media is at some point after the recording.

Discreet Monitoring and Replay services are required functions of a public-safety network. For non-public safety services, these functions shall not be implemented in the network without explicit consent from all users of the MC system.

### 10.2.2 Collection of service media

User media is collected from the media paths within the MC Domain. It is expected that the encrypted media required to be collected (MCPTT, MCData, MCVideo or MC Location) shall be routed from the appropriate MC Service Server to the MC Recording server. In the case of MCData, user media can also be collected in a signalling plane.

Where SDS messages are routed within a signalling path, media will need to be extracted from within MCData signalling paths by the MCData Server. It is expected that the encrypted media routed over the signalling path shall be routed from the MCData Server to the MC Recording server.

The storage solution is out-of-scope of this document.

### 10.2.3 Storing of service media

User Service in the MC System is end-to-end encrypted by default and can be recorded in the MC Recording server.

NOTE a: It’s up to the implementation of the MC Recording server to decrypt and re-encrypt before storing it to mass data storage.

### 10.2.4 Decryption of user media

To decrypt a specific target user's service media for replay or discreet listening at a specific time 'T', the following process should be used for decryption of user media by an authorized decryption entity. The controlling entity shall be either the KMS or a secured logging device.

1. The authorized decryption entity obtains the target user's key material and KMS certificate that was active at time 'T'. The provision of user key material by the KMS grants the authorized decryption entity access to the user’s communication content.

Any request made by an authorized decryption entity shall be controlled and logged (to allow the replay action to be recorded).

NOTE: The release of key material for a user at time 'T' only allows the authorized decryption entity access to content for the defined 'key period' associated to time ‘T’. By limiting the total number of requests (e.g. to 0.1% of users), this limits access to communications. These controls help to ensure that the granted access to user content is time-limited and proportionate.

2. The authorized decryption entity extracts the user events associated with the user at time 'T'.

3. The authorized decryption entity extracts the MIKEY messages from the signalling events and use the targeted user's KMS-supplied key material to decrypt the media encryption keys held within the MIKEY messages.

4. The authorized decryption entity is now able to associate media with user events and use the media encryption keys extracted from MIKEY message to decrypt the media.

5. The decrypted media shall only be shared with an authorized replay user.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 1st change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*