Source:	**TSG CN WG 1**
Title:	**CR to Rel-5 on Work Item IMS-CCR towards 24.008**
Agenda item:	**9.14**
Document for:	**APPROVAL**

Introduction:

This document contains **1** CR on **Rel-5 to** Work Item **" IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #15 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
24.008	557	2	Rel-5	Upgrading TFT for supporting IMS services	B	5.2.0	5.3.0	N1-020442

CR-Form-v5

CHANGE REQUEST

| ⌘ | **24.008** CR **557** | ⌘ rev | **2** | ⌘ Current version: | **5.2.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘   (U)SIM ☐   ME/UE **X**   Radio Access Network ☐   Core Network **X**

Title:	⌘	Upgrading TFT for supporting IMS services
Source:	⌘	Motorola
Work item code:	⌘	IMS-CCR ***Date:*** ⌘ 2002-01-31

Category:	⌘	**B**	***Release:*** ⌘ Rel-5

Use <u>one</u> of the following categories:
  F *(correction)*
  A *(corresponds to a correction 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 <u>TR 21.900</u>.

Use <u>one</u> of the following releases:
  2   *(GSM Phase 2)*
  R96   *(Release 1996)*
  R97   *(Release 1997)*
  R98   *(Release 1998)*
  R99   *(Release 1999)*
  REL-4   *(Release 4)*
  REL-5   *(Release 5)*

Reason for change:	⌘	GPRS Session Management needs to provide support for the QoS Resources Authorization and Policy, as specified in 3GPP TS 23.207.
Summary of change:	⌘	The Traffic Flow Template IE is enhanced and it is also used to carry the Binding Information from the MS to the GGSN.
Consequences if not approved:	⌘	TS 24.008 will not provide enough stage-3 support for IMS.

Clauses affected:	⌘	9.5.10, 10.5.6.12

Other specs affected:	⌘	☐ Other core specifications ⌘	
		☐ Test specifications	
		☐ O&M Specifications	

Other comments:	⌘	With the proposed CR the TFT IE can contain (i) no list, (ii) only the "packet filters list", (iii) only the "parameters list", and (iv) both lists.

In case (i), the "Number of packet filter" is 0, the "TFT operation code" is 2 ("Delete existing TFT"), and E-bit is 0.

In case (ii), the "Number of packet filter" is x (x=1-8), the "TFT operation code" is either 1,3,4, or 5 and E-bit is 0.

Note that the encoding in the above cases (i), (ii) is exactly the same with the encoding specified before this CR.

In case (iii), the "Number of packet filters" is 0, the "TFT operation code" is "No TFT operation" and E-bit is 1. Since "No TFT operation" is reserved in pre-R5, a legacy receiver will treat this TFT IE as not present (this is a syntactically incorrect optional IE; see 24.008 section 8.7.1). However, an R5+ receiver will identify that |

there's only a "parameters list" and will decode this list.

In case (iv), the "Number of packet filters" is x (x=1-8), the "TFT operation code" is either 1,3,4, or 5 and E-bit is 1. A legacy receiver will read x packet filters from the "packet filters list" and will perform the operation indicated by the "TFT operation code". It will ignore the "parameters list", which follows right after the x packet filters. However, an R5+ receiver will identify (from the E bit) that there's a "parameters list" and will decode this list.

As explained above, the "No TFT operation" code is included when the TFT IE includes ONLY the "parameters list" (case (iii)). However, the E-bit is set to 1 in cases (iii) and (iv).

Case (iii) is needed when we have to modify a PDP context and send ONLY the Binding Information (i.e. we don't need to include any packet filters). However, case (iv) is needed when we have to activate a secondary PDP context and include both a packet filter list and the Binding Information.

<div style="text-align:center">

FIRST MODIFICATION

</div>

9.5.10   Modify PDP context request (MS to network direction)

This message is sent by the MS to the network to request modification of an active PDP context. See table 9.5.10/3GPP TS 24.008.

   Message type: MODIFY PDP CONTEXT REQUEST (MS TO NETWORK DIRECTION)

   Significance: global

   Direction: MS to network

Table 9.5.10/3GPP TS 24.008: modify PDP context request (MS to network direction) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Modify PDP context request message identity	Message type 10.4	M	V	1
32	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	O	TV	2
30	Requested new QoS	Quality of service 10.5.6.5	O	TLV	14
31	New TFT	Traffic Flow Template 10.5.6.12	O	TLV	3-257

9.5.10.1   Requested LLC SAPI

This IE may be included in the message to request a new LLC SAPI if a new QoS is requested.

9.5.10.2   Requested new QoS

This IE may be included in the message to request a modification of the QoS.

9.5.10.3   New TFT

This IE may be included in the message to request a new TFT or modification of an existing TFT or transfer extra parameters to the network (e.g. the Authorization Token; see 3GPP TS 24.229).

<div style="text-align:center">

NEXT MODIFICATION

</div>

10.5.6.12   Traffic Flow Template

The purpose of the *traffic flow template* information element is to specify the TFT parameters and operations for a PDP context. In addition, this information element may be used to transfer extra parameters to the network (e.g. the Authorization Token; see 3GPP TS 24.229).

The *traffic flow template* is a type 4 information element with a minimum length of 3 octets. The maximum length for the IE is 257 octets.

   NOTE: The IE length restriction is due to the maximum length that can be encoded in a single length octet.

NOTE: A maximum size IPv4 packet filter can be 32 bytes. Therefore, 7 maximum size IPv4 type packet filters, plus the last packet filter which can contain max 30 octets can fit into one TFT, i.e. if needed not all packet filter components can be defined into one message. A maximum size Ipv6 packet filter can be 60 bytes. Therefore, only 4 maximum size IPv6 packet filters can fit into one TFT. However, using "Add packet filters to existing TFT", it's possible to create a TFT including 8 maximum size Ipv4 or IPv6 filters.

The *traffic flow template* information element is coded as shown in Figure 10.5.144/3GPP TS 24.008 and Table 10.5.162/3GPP TS 24.008.
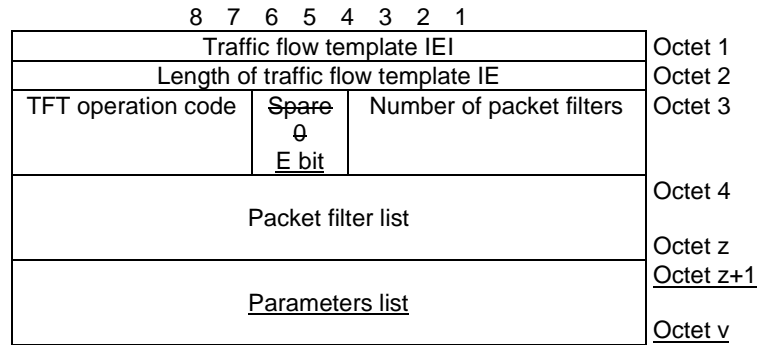
8 7 6 5 4 3 2 1	
Traffic flow template IEI	Octet 1
Length of traffic flow template IE	Octet 2
TFT operation code | ~~Spare 0~~ E bit | Number of packet filters	Octet 3
Packet filter list	Octet 4 ... Octet z
Parameters list	Octet z+1 ... Octet v

Figure 10.5.144/3GPP TS 24.008: *Traffic flow template* information element

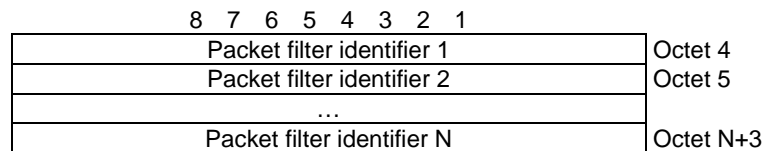| 8 7 6 5 4 3 2 1	
Packet filter identifier 1	Octet 4
Packet filter identifier 2	Octet 5
…	
Packet filter identifier N	Octet N+3

Figure 10.5.144a/3GPP TS 24.008: *Packet filter list* when the TFT operation is "delete packet filters from existing TFT" (z=N+3)

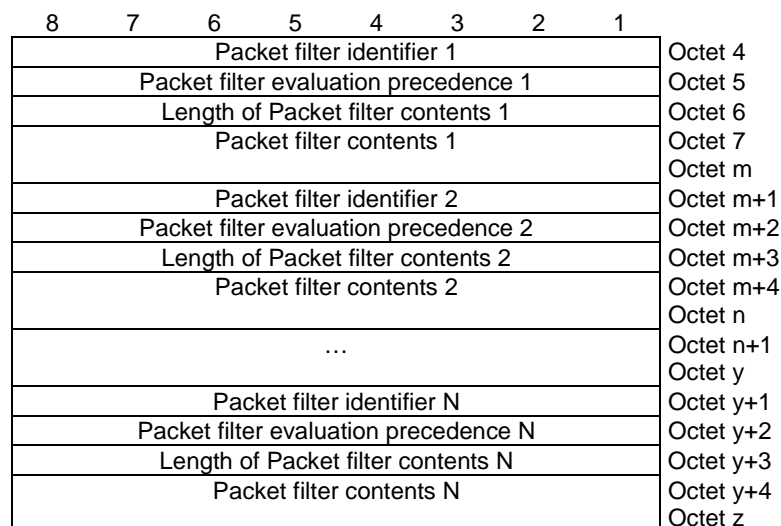| 8 7 6 5 4 3 2 1	
Packet filter identifier 1	Octet 4
Packet filter evaluation precedence 1	Octet 5
Length of Packet filter contents 1	Octet 6
Packet filter contents 1	Octet 7 Octet m
Packet filter identifier 2	Octet m+1
Packet filter evaluation precedence 2	Octet m+2
Length of Packet filter contents 2	Octet m+3
Packet filter contents 2	Octet m+4 Octet n
…	Octet n+1 Octet y
Packet filter identifier N	Octet y+1
Packet filter evaluation precedence N	Octet y+2
Length of Packet filter contents N	Octet y+3
Packet filter contents N	Octet y+4 Octet z

Figure 10.5.144b/3GPP TS 24.008: *Packet filter list* when the TFT operation is "create new TFT", or "add packet filters to existing TFT" or "replace packet filters in existing TFT"

8	7	6	5	4	3	2	1	
Parameter identifier 1								Octet z+1
Length of Parameter contents 1								Octet z+2
Parameter contents 1								Octet z+3
								Octet k
Parameter identifier 2								Octet k+1
Length of Parameter contents 2								Octet k+2
Parameter contents 2								Octet k+3
								Octet p
…								Octet p+1
								Octet q
Parameter identifier N								Octet q+1
Length of Parameter contents N								Octet q+2
Parameter contents N								Octet q+3
								Octet v

Figure 10.5.144c/3GPP TS 24.008: *Parameters list*

Table 10.5.162/3GPP TS 24.008: *Traffic flow template* information element

Table 10.5.162/3GPP TS 24.008: *Traffic flow template* information element

TFT operation code (octet 3)
Bits
8 7 6

0 0 0 Spare
0 0 1 Create new TFT

0 1 0 Delete existing TFT
0 1 1 Add packet filters to existing TFT

1 0 0 Replace packet filters in existing TFT

1 0 1 Delete packet filters from existing TFT
1 1 0 ReservedNo TFT operation

1 1 1 Reserved

E bit (bit 5 of octet 3)

The *E bit* indicates if a *parameters list* is included in the TFT IE and it is encoded as follows:
0   *parameters list* is not included
1   *parameters list* is included

Number of packet filters (octet 3)

The *number of packet filters* contains the binary coding for the number of packet filters in the *packet filter list*. The *number of packet filters* field is encoded in bits 4 through 1 of octet 3 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing TFT" operation and for the "no TFT operation", the *number of packet filters* shall be coded as 0. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 8.

Packet filter list (octets 4 to z)

The *packet filter list* contains a variable number of packet filters. For the "delete existing TFT" operation, the *packet filter list* shall be empty.

For the "delete packet filters from existing TFT" operation, the *packet filter list* shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the *number of packet filters* field in octet 3.

For the "create new TFT", "add packet filters to existing TFT" and "replace packet filters in existing TFT" operations, the *packet filter list* shall contain a variable number of packet filters. This number shall be derived from the coding of the *number of packet filters* field in octet 3.

Each packet filter is of variable length and consists of

- a packet filter identifier (1 octet);
- a packet filter evaluation precedence (1 octet);
- the length of the packet filter contents (1 octet); and
- the packet filter contents itself (v octets).

The *packet filter identifier* field is used to identify each packet filter in a TFT. Since the maximum number of packet filters in a TFT is 8, only the least significant 3 bits are used. Bits 8 through 4 are spare bits.

The *packet filter evaluation precedence* field is used to specify the precedence for the packet filter among all packet filters in all TFTs associated with this PDP address. Higher the value of the *packet filter evaluation precedence* field, lower the precedence of that packet filter is. The first bit in transmission order is the most significant bit.

The *length of the packet filter contents* field contains the binary coded

Table 10.5.162/3GPP TS 24.008 (continued): *Traffic flow template* information element

The *packet filter contents* field is of variable size and contains a variable number (at least one) of *packet filter components*. Each *packet filter component* shall be encoded as a sequence of a one octet *packet filter component type identifier* and a fixed length *packet filter component value* field. The *packet filter component type identifier* shall be transmitted first.

In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 source address type" and "IPv6 source address type" packet filter components, only one shall be present in one packet filter. Among the "single destination port type" and "destination port range type" packet filter components, only one shall be present in one packet filter. Among the "single source port type" and "source port range type" packet filter components, only one shall be present in one packet filter.

Packet filter component type identifier

Bits

8 7 6 5 4 3 2 1
0 0 0 1 0 0 0 0   IPv4 source address type
0 0 1 0 0 0 0 0   IPv6 source address type
0 0 1 1 0 0 0 0   Protocol identifier/Next header type
0 1 0 0 0 0 0 0   Single destination port type
0 1 0 0 0 0 0 1   Destination port range type
0 1 0 1 0 0 0 0   Single source port type
0 1 0 1 0 0 0 1   Source port range type
0 1 1 0 0 0 0 0   Security parameter index type
0 1 1 1 0 0 0 0   Type of service/Traffic class type
1 0 0 0 0 0 0 0   Flow label type

All other values are reserved.

For "IPv4 source address type", the *packet filter component value* field shall be encoded as a sequence of a four octet *IPv4 address* field and a four octet *IPv4 address mask* field. The *IPv4 address* field shall be transmitted first.

For "IPv6 source address type", the *packet filter component value* field shall be encoded as a sequence of a sixteen octet *IPv6 address* field and a sixteen octet *IPv6 address mask* field. The *IPv6 address* field shall be transmitted first.

For "Protocol identifier/Next header type", the *packet filter component value* field shall be encoded as one octet which specifies the IPv4 protocol identifier or IPv6 next header.

For "Single destination port type" and "Single source port type", the *packet filter component value* field shall be encoded as two octet which specifies a port number.

For "Destination port range type" and "Source port range type", the *packet filter component value* field shall be encoded as a sequence of a two octet *port range low limit* field and a two octet *port range high limit* field. The *port range low limit* field shall be transmitted first.

For "Security parameter index", the *packet filter component value* field shall be encoded as four octet which specifies the IPSec security parameter index.

For "Type of service/Traffic class type", the *packet filter component value* field shall be encoded as a sequence of a one octet *Type-of-Service/Traffic Class* field and a one octet *Type-of-Service/Traffic Class mask* field. The *Type-of-Service/Traffic Class* field shall be transmitted first.

For "Flow label type", the *packet filter component value* field shall be encoded as three octet which specifies the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.