3GPP TSG_CN   **Tdoc NP-000266**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source:	**TSG_N WG "1"**
Title:	**Removal of P-TMSi signature from "Service Request"**
Agenda item:	**5.1.2**
Document for:	**Discussion**

<u>**Introduction**</u>:

This document contains **"1"** CRs on **Work Item "GSM-UMTS interworking",** that have been REJECTED by **TSG_N WG "1",** and are forwarded to **TSG_N Plenary** meeting #8 for Discussion.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N1-000644	24.008	CR204		F	R99	3.3.1	3.4.0	Removal of P-TMSI signature in Service Request message

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

24.008	**CR**	**204**		Current Version:	**3.3.1**	

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	**TSG CN #8**	for approval	**X**	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG   *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM ☐   ME **X**   UTRAN / Radio ☐   Core Network **X**
(at least one should be marked with an X)

Source:	Ericsson		**Date:**	2000-05-02

Subject:	Removal of P-TMSI signature in Service Request message

Work item:	GSM-UMTS interworking

Category:	F	Correction	**X**	**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification			Release 99	**X**
					Release 00	

| **Reason for change:** | According to 24.008 version 3.2.1, the MS shall delete the P-TMSI signature after a successful completed Service Request procedure if the P-TMSI signature has been sent in the Service Request message. Whenever the P-TMSI signature is deleted, the network has to allocate a new one. In UMTS the P-TMSI signature should only be used whenever it is useful as integrity protection is introduced.

This CR proposes to remove the P-TMSI signature from the Service Request message.

The removal of the P-TMSI signature from the Service Request message was agreed at the previous S2 #11 meeting in CR no. 123 in Tdoc 354 to TS 23.060 ver. 3.2.1. |
|---|---|

Clauses affected:	4.7.1.3, 4.7.13.2, 9.4.20

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:	CR 123 to TS 23.060 in Tdoc 254, is attached to this zip file.

4.7.1.3   P-TMSI signature

The network may assign a P-TMSI signature to an MS in an attach, routing area update, or P-TMSI reallocation procedure. Only in combination with a valid P-TMSI, this P-TMSI signature is used by the MS for authentication and identification purposes in the subsequent attach , routing area update~~, service request~~ or detach procedure. If the MS has no valid P-TMSI it shall not use the P-TMSI signature in the subsequent attach, routing area update~~, service request~~ or detach procedure. Upon completion completion of the subsequent attach routing area update~~, service request~~ or detach procedure the used P-TMSI signature shall be deleted.

<div align="center">

*** Next Modification ***

</div>

4.7.13   Service Request procedure (UMTS only)

The purpose of this procedure is to transfer the PMM mode from PMM-IDLE to PMM-CONNECTED mode, and/or to assign radio access bearer in case of PDP contexts are activated without radio access bearer assigned. In latter case, the PMM mode may be PMM-IDLE or PMM-CONNECTED mode.This procedure is used for;

-    the initiation of CM layer service (e.g. SM or SMS) procedure from the MS in PMM-IDLE mode.

-    the network to transfer down link signalling,

-    uplink and downlink user packet.

For downlink transfer of signalling or user packet, the trigger is given from the network by the paging request procedure, which is out of scope of this specification.

Service type can take either of the following values, "signalling", "data" or "paging response". Each of the values shall be selected according to the criteria to initiate the Service request procedure.

The criteria to invoke the Service request procedure are when;

a)   the MS has any signalling message, that requires security protection, to be sent to the network in PMM-IDLE mode (i.e., no secure PS signalling connection has been established). In this case, the service type shall be set to "signalling".

b)   the MS, either in PMM-IDLE and PMM-CONNECTED mode, has pending user packet to be sent and no radio access bearer is established for the PDP context. The procedure is initiated by an indication from the lower layers. In this case, the service type shall be set to "data".

c)   the MS receives a paging request for PS domain from the network in PMM-IDLE mode. In this case, the service type shall be set to "paging response".

After completion of a Service request procedure, the pending service is resumed and uses then the connection established by the procedure. If the service type is indicating "data", then the radio access bearers for all the activated PDP contexts are re-established. The selective re-assignment capability is not supported for the simplicity of the function.

4.7.13.1 Service Request procedure initiation

The MS initiates the Service request procedure by sending a SERVICE REQUEST message. The timer T3317 shall be started after the SERVICE REQUEST message has been sent and state GMM-SERVICE-REQUEST-INITIATED is entered. The message SERVICE REQUEST shall contain the P-TMSI and the Service type shall indicate either data, signalling or paging response.

4.7.13.2 GMM common procedure initiation

The network may initiate GMM common procedures, e.g. the GMM identification or the GMM authentication and ciphering procedure, depending on the received information such as GPRS ciphering key sequence number, and P-TMSI and P-TMSI signature.

4.7.13.3 Service request procedure accepted by the network

An indication from the lower layers that the security mode setting procedure is completed, or reception of a SERVICE ACCEPT message, shall be treated as a successful completion of the procedure. The timer T3317 shall be stopped, and the MS enters GMM-REGISTERED state and PMM-CONNECTED mode.

*** Next Modification ***

9.4.20 Service Request (UMTS only)

This message is sent by the MS to transfer to establish logical association between the MS and the network. See table 9.4.20/TS 24.008.

Message type: Service Request

Significance: dual

Direction: MS to network

Table 9.4.20/TS 24.008: Contents of Service Request message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Service Request	Message type 10.4	M	V	1
	Ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	1/2
	Service type	Service type 10.5.5.20	M	V	1/2
	P-TMSI	Mobile station identity 10.5.1.4	M	LV	6
~~19~~	~~P-TMSI signature~~	~~P-TMSI signature 10.5.5.8~~	~~O~~	~~TV~~	~~4~~

~~9.4.20.1 P-TMSI signature~~

~~This IE is included if a valid P-TMSI signature is available.~~

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.060	**CR**	**123**		Current Version:	**3.2.1**	

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	**SA #7**	for approval	**X**	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM [ ]   ME **X**   UTRAN / Radio [ ]   Core Network **X**
(at least one should be marked with an X)

Source:	Ericsson	**Date:**	2000-02-29

Subject:	Removal of P-TMSI Signature in Service Request

Work item:	Release 99

Category: F   Correction   **X**   **Release:**   Phase 2 [ ]
(only one category   A   Corresponds to a correction in an earlier release [ ]   Release 96 [ ]
shall be marked   B   Addition of feature [ ]   Release 97 [ ]
with an X)   C   Functional modification of feature [ ]   Release 98 [ ]
    D   Editorial modification [ ]   Release 99 **X**
    Release 00 [ ]

Reason for change:	Removal of P-TMSI signature from the Service Request procedure.

The general principle is that whenever the P-TMSI signature is sent unciphered, the MS shall delete the P-TMSI signature when it has been sent unciphered . Therefore the P-TMSI signature shall only be included wherever it is useful.

A service request initiated when the MS is in PMM-IDLE state will be sent unciphered. Since the service request procedure can not re-allocate a P-TMSI signature, it will normally trigger a P-TMSI re-allocation procedure. This seems quite unnecessary since the P-TMSI signature is not a very useful concept in UMTS where we have introduced integrity protection.

If the service request includes the P-TMSI signature then at time for the next RA update the MS do not have a P-TMSI signature (e.g. inter-system change). This is a drawback since the P-TMSI signature was introduced in GSM GPRS to make sure that the unciphered RA updates were sent from a valid MS. |

Clauses affected:	6.8.2.3, 6.12

Other specs affected:
Other 3G core specifications	**X**	→ List of CRs:	3G TS 24.008
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:	

help.doc

<---------- double-click here for help and instructions on how to create a CR.

6.8.2.3   P-TMSI Signature

P-TMSI Signature is optionally sent by the SGSN to the MS in Attach Accept and Routeing Area Update Accept messages. If the P-TMSI Signature has been sent by the SGSN to the MS since the current P-TMSI was allocated, then the MS shall include the P-TMSI Signature in the next Routeing Area Update Request, Detach Request, ~~Service Request,~~ and Attach Request for identification checking purposes. If the P-TMSI Signature was sent, then the SGSN shall compare the P-TMSI Signature sent by the MS with the signature stored in the SGSN. If the values do not match, the SGSN should use the security functions to authenticate the MS. If the values match or if the P-TMSI Signature is missing, the SGSN may use the security functions to authenticate the MS. The P-TMSI Signature parameter has only local significance in the SGSN that allocated the signature.

If ciphering is supported by the network, the SGSN shall send the P-TMSI Signature ciphered to the MS. Routeing Area Update Request and Attach Request, into which the MS includes the P-TMSI Signature, are not ciphered.

> *** *Next Modification* ***

6.12   Service Request Procedure for UMTS

The Service Request procedure is used by a 3G-MS in PMM-IDLE state to request the establishment of a secure connection to a 3G-SGSN. The MS in PMM-IDLE state initiates this procedure in order to send uplink signalling messages (e.g., Activate PDP Context Request) or user data. This procedure is also used by an MS in PMM-CONNECTED state to request resource reservation for active PDP contexts.

6.12.1   Service Request Initiated by MS Procedure

The MS in PMM-IDLE state sends the Service Request message to the 3G-SGSN in order to establish the PS signalling connection for the upper layer signalling or for the resource reservation for active PDP contexts. After receiving the Service Request message the 3G-SGSN may perform authentication and it shall perform the security mode procedure. After the establishment of the secure PS signalling connection to a 3G-SGSN the MS may send signalling messages, e.g., Activate PDP Context Request, to the 3G-SGSN, or the 3G-SGSN may start the resource reservation for the active PDP contexts depending on the requested service in the Service Request message. This procedure is also used by an MS in PMM-CONNECTED state to request the resource reservation for the active PDP contexts.
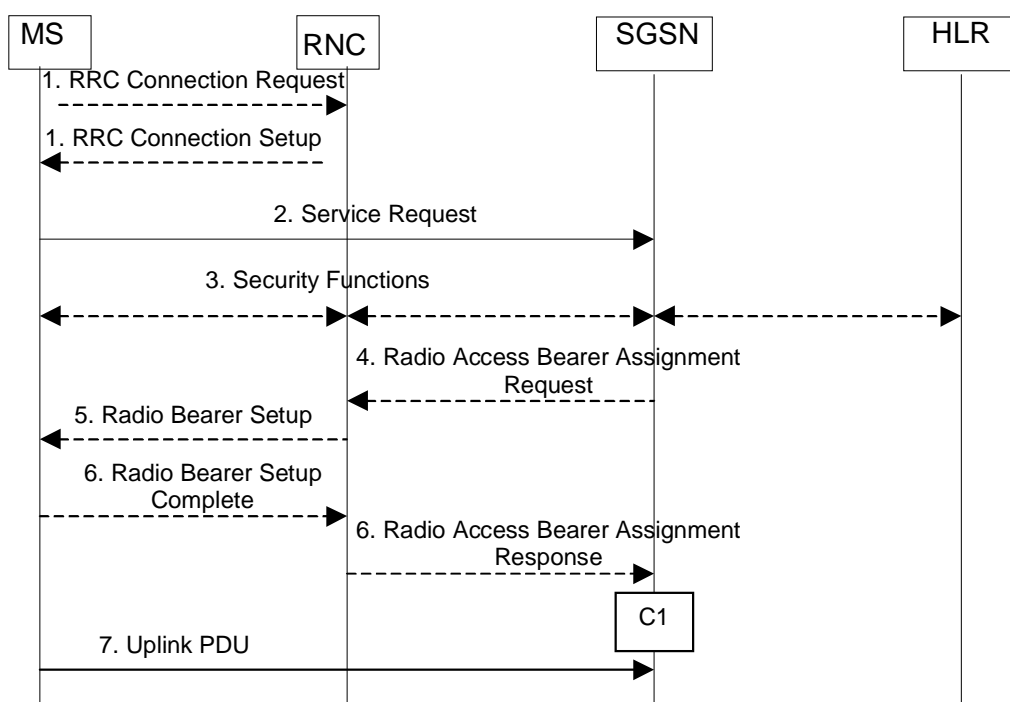

Figure 47: Service Request Initiated by MS Procedure

1) The MS establishes an RRC connection, if none exists for CS traffic.

2) The MS sends a Service Request (P-TMSI, ~~P-TMSI Signature~~, RAI, CKSN, Service Type) message to the SGSN. Service Type specifies the requested service. Service Type shall indicate one of the following: Data or Signalling. At this point, the SGSN may perform the authentication procedure.

   If Service Type indicates Data then a signalling connection is requested established between the MS and the SGSN, and resources for active PDP context(s) are requested allocated, i.e., RAB establishment for the activated PDP context(s).

   If Service Type indicates Signalling then the signalling connection is requested established between the MS and the SGSN for sending upper-layer signalling messages, e.g., Activate PDP Context Request. The resources for active PDP context(s) are not requested allocated.

3) The SGSN shall perform the security functions if the service request was initiated by an MS in PMM-IDLE state.

4) In case Service Type indicates Data, the SGSN sends a Radio Access Bearer Assignment Request (NSAPI(s), TEID(s), QoS Profile(s), SGSN IP Address(es)) message to re-establish radio access bearer for every activated PDP context.

5) The RNC indicates to the MS the new Radio Bearer Identity established and the corresponding NSAPI with the RRC radio bearer set up procedure.

6) SRNC responds with the Radio Access Bearer Assignment Response (NSAPI(s), TEID(s), QoS Profile(s), RNC IP Address(es)) message. The GTP tunnel(s) are established on the Iu interface.

7) The MS sends the uplink packet.

The MS knows that the Service Request message was successfully received in the SGSN when the MS receives the RRC Security Mode Control Command message. It is, however, possible that the security mode procedure is not performed, e.g., if the Service Request message indicating Service Type = Data is sent after an RA update procedure via the same PS signalling connection. For such cases, the Service Accept message may be needed and it should be treated by the MS as a service acceptance indication.

If the service request cannot be accepted, the network returns a Service Reject message to the mobile station.

For an MS with GPRS-CSI defined, CAMEL interaction may be performed, see referenced procedure in 3G TS 23.078:

C1) CAMEL-GPRS-Attach-Request.

6.12.2   Service Request Initiated by Network Procedure

When the 3G-SGSN receives a downlink packet (e.g., Request PDP Context Activation, MT SMS, user data) for an MS in PMM-IDLE state, the 3G-SGSN sends a paging request to UTRAN. The paging request triggers the Service Request procedure in the UMS
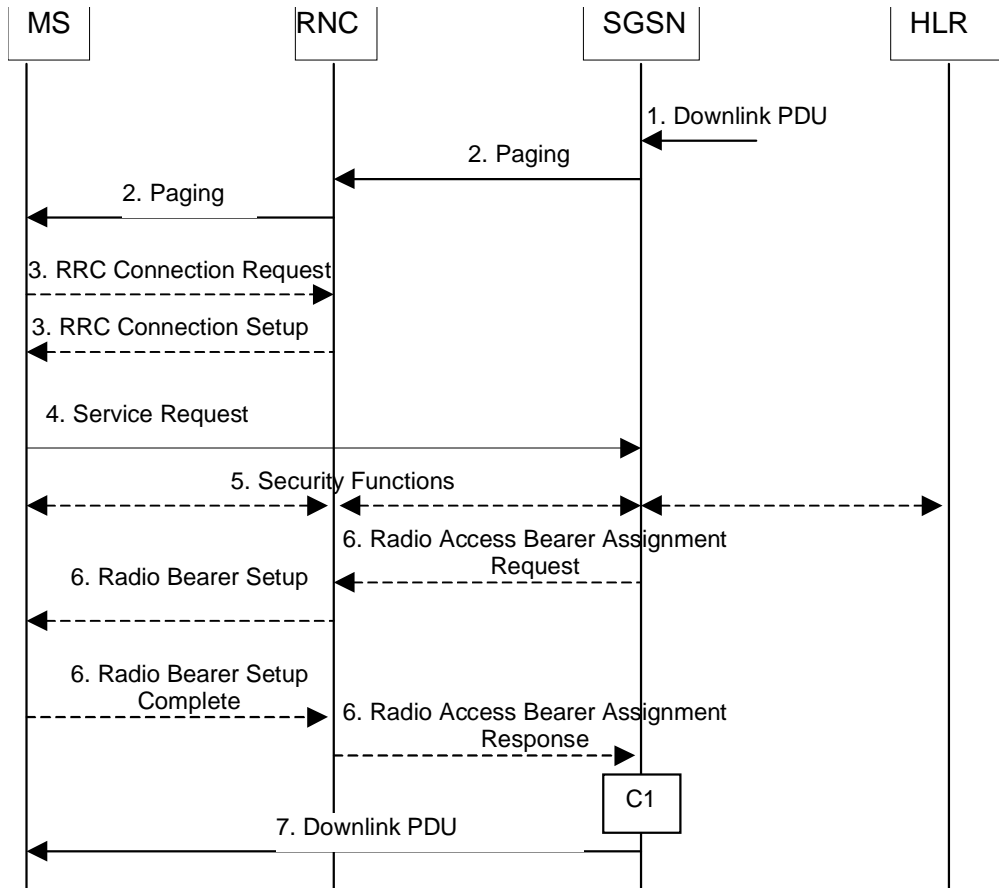
Figure 48: Service Request Initiated by Network Procedure

1) The SGSN receives a downlink PDP PDU for an MS in PMM-IDLE state.

2) The SGSN sends a Paging (IMSI, P-TMSI, RAI, Paging Cause) message to the RNC. The RNC pages the MS by sending a Paging (P-TMSI or IMSI, Paging Cause) message to the MS.

3) The MS establishes an RRC connection if none exists for CS traffic.

4) The MS sends a Service Request (P-TMSI, P-TMSI Signature, RAI, CKSN, Service Type) message to the SGSN. Service Type specifies Paging Response. The Service Request is carried over the radio in an RRC Direct Transfer message and over the Iu interface in the RANAP Initial MS message. At this point, the SGSN may perform the authentication procedure. The SGSN knows whether the downlink packet requires RAB establishment (e.g., downlink PDU) or not (e.g., Request PDP Context Activation or MT SMS).

5) The SGSN shall perform the security mode procedure.

6) If resources for the PDP contexts are re-established, the SGSN sends a Radio Access Bearer Assignment Request (NSAPI(s), TEID(s), QoS Profile(s), SGSN IP Address(es)) message to the RNC. The RNC sends a Radio Access Bearer Setup (RAB Identity, NSAPI) to the MS. The MS responds by returning a Radio Access Bearer Complete message to the RNC. The RNC sends a Radio Access Bearer Assignment Response (NSAPI(s), TEID(s), QoS Profile(s), RNC IP Address(es)) message to the SGSN in order to indicate that GTP tunnels are established on the Iu interface and radio access bearers are established between the RNC and the MS.

7) The SGSN sends the downlink packet.

For an MS with GPRS-CSI defined, CAMEL interaction may be performed, see referenced procedure in 3G TS 23.078:

C1)   CAMEL-GPRS-Attach-Request.