

## PSEUDO CHANGE REQUEST

⌘ **33.878 Pseudo-CR** **CRNum** ⌘ rev **-** ⌘ Current version: **0.0.3** ⌘

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

**Proposed change affects:**  UICC apps⌘  ME  Radio Access Network  Core Network

<b>Title:</b>	⌘ Clarification of issues raised in LS from SA2 (S3-041036)		
<b>Source:</b>	⌘ Siemens		
<b>Work item code:</b>	⌘ Early IMS	<b>Date:</b>	⌘ 23/11/2004
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		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) Rel-6 (Release 6)

<b>Reason for change:</b>	⌘ 1) The term 'authenticated PDP context' is not defined in other specifications. 2) The interface used between the GGSN and the HSS needs to be clarified. 3) The logging of events in the GGSN is not to be mandated.		
<b>Summary of change:</b>	⌘ 1) The text clarifies that it is the IMSI, not the PDP context, which is authenticated. 2) The text clarifies that the Gi interface is used. 3) The text is changed to say that the logging of events in the GGSN shall be possible.		
<b>Consequences if not approved:</b>	⌘ Unclear text.		

<b>Clauses affected:</b>	⌘ 7.1, 7.2.2										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<b>Other comments:</b>	⌘ -										

\*\*\*\*\* begin change \*\*\*\*\*

## 7.1 Overview

The early IMS security solution works by creating a secure binding in the HSS between the public/private user identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The GGSN, terminating each user's ~~authenticated~~-PDP context and has assurance that the IMSI used with this PDP context is authenticated. The GGSN shall provide the user's IP address / MSISDN pair to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the MSISDN and the IMPI, and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI. The GGSN informs the HSS when the PDP context is deactivated/modified so that the stored IP address can be updated in the HSS. When the S-CSCF receives a SIP registration request or any subsequent requests for a given IMPI, it checks that the IP address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's IMPI in the HSS.

The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent source IP Spoofing. The mechanism also assumes that the P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the UE (the assumption here, as well as for the full security solution, is that no NAT is present between the GGSN and the P-CSCF).

The mechanism prevents an attacker from using his own IP address in the IP header but spoofing someone else's IMS identity or IP address in the SIP header, so that he pays for GPRS level charges, but not for IMS level charges. The mechanism also prevents an attacker spoofing the address in the IP header so that he does not pay for GPRS charges. It therefore counters the threat scenarios given in clause 6 above.

The mechanism assumes that only one contact IP address is associated with one IMPI. Furthermore, the mechanism supports the case that there may be several IMPUs associated with one IMPI, but one IMPU is associated with only one IMPI.

In early IMS the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to an ~~authenticated~~-PDP context (based on an authenticated IMSI). The mechanism here assumes that there is a one-to-one relationship between the IMSI for bearer access and the IMPI for IMS access.

In the following we use the terms P-CSCF and S-CSCF in a general sense to refer to components of an early IMS system. We note however that early IMS solutions may not have the same functionality split between SIP entities as defined in TS 23.228 [3]. Therefore, the requirements imposed on the SIP/IP core are specified in such a way that they are independent of the functionality split between SIP entities as far as possible. While the exact functionality split of the SIP/IP core may be left open, it is important that any changes to the Cx interface towards the HSS and changes to the interface towards the UE are standardised for vendor interoperability reasons.

\*\*\*\*\* end change \*\*\*\*\*

\*\*\*\*\* begin change \*\*\*\*\*

### 7.2.2 Protection against IP address spoofing in GGSN

All GGSNs that offer connection to IMS shall implement measures to prevent source IP address spoofing. Specifically, a UE attached to the GGSN shall not be able to successfully transmit an IP packet with a source IP address that is different to the one assigned by the GGSN during PDP context activation. If IP address spoofing is detected the GGSN shall drop the packet. It shall be possible for the GGSN to ~~and~~ log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

\*\*\*\*\* end change \*\*\*\*\*