Technical Specification Group Services and System Aspects **TSGS#19(03)0185**

Meeting #19, Birmingham, UK, 17-20 March 2003

Source: **SA WG3**

Title: **1 CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was approved by SA WG3 meeting #27 and is hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030101	33.203	036	1	Rel-5	Malicious UE bypassing the P-CSCF	F	5.4.0	IMS-ASEC	revised by SA

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **036** ⌘ **rev** **1** ⌘ Current version: **5.4.0** ⌘

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

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

Title:	⌘	Malicious UE bypassing the P-CSCF
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	18/03/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one 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 TR 21.900.

Use one 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)*

Reason for change:	⌘	Malicious UE could send SIP messages directly to the S-CSCF and bypass the P-CSCF and I-CSCF.
Summary of change:	⌘	Recommendations added to protect against bypassing P-CSCF. Additionally, if inter-CSCF traffic is not protected by the NDS/IP mechanisms, then physical protection measures or IP traffic filtering should be applied. However, it is highlighted that this is not in the scope of 3GPP specification.
Consequences if not approved:	⌘	Specification would be ambiguous whether this attack scenario applies or not. Without this change the implementation of the specification may result in an insecure system.

Clauses affected:	⌘	Annex X (new)

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

Annex X (informative): Recommendations to protect the IMS from UEs bypassing the P-CSCF

After the UE does a successful SIP REGISTER with the P-CSCF, malicious UE could try to send SIP messages directly to the S-CSCF. This could imply that the UE would be able to bypass the integrity protection provided by IPSec ESP between the UE and the P-CSCF.

NOTE: The TS 24.229 [8] defines a trust domain that consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF, the MGCF, the MRFC and all the AS:s that are not provided by 3rd party service providers. There are nodes in the edge of the trust domain that are allowed to provide with an asserted identity header. The nodes in the trust domain will trust SIP messages with asserted identity headers. The asserted identity information is useful as long as the interfaces in an operator's network can be trusted.

If a UE manages to bypass the P-CSCF it presents at least the following problems:

1) The P-CSCF is not able to generate any charging information.

2) Malicious UE could masquerade as some other user (e.g. it could potentially send INVITE or BYE messages).

The following recommendations for preventing attacks based on such misbehavior are given:

- Access to S-CSCF entities should be restricted to the core network entities that are required for IMS operation, only. It should be ensured that no UE is able to directly send IP packets to IMS-entities other than the required ones, ie. assigned P-CSCF, or HTTP servers.
- Impersonation of IMS core network entities at IP level (IP spoofing), especially impersonation of P-CSCFs by UEs should be prevented.
- It is desirable to have a general protection mechanism against UEs spoofing (source) IP addresses in any access network providing access to IMS services.

If neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.