3GPP TSG-SA WG3 Meeting #23
Victoria, BC, Canada, 14-17 May 2002

Tdoc S3-020233

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **0xx** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Incoming unprotected SIP messages at the UE
Source:	⌘	Ericsson
Work item code:	⌘	IMS
Date:	⌘	2002-05-07
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)

Reason for change:	⌘	A list has been defined in TS33.203 to prevent the P-CSCF to handle any incoming SIP messages on the unprotected port of the P-CSCF. A similar list defined for the UE would improve the protection in the UE against attackers.
Summary of change:	⌘	Added a list of SIP messages, which the UE is allowed to handle if received at the unprotected port during an ongoing Register procedure.
Consequences if not approved:	⌘	Any proxy could send in any SIP message on the unprotected port of the UE and the SIP layer would accept and handle this message.

Clauses affected:	⌘	D.1
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request

Annex D (informative): Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This section is based on section 7 and provides additional specification for the support of IPsec ESP.

D.1 Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are

- ESP transform identifier
- Authentication (integrity) algorithm
- SPI

Further parameters:

- Life type: the life type is always seconds
- SA duration: the SA duration has a fixed length of 2^{32}-1.
- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.
2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.
3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.
4. The UE may send only the following messages to the fixed port for unprotected messages:
   - initial REGISTER message;
   - REGISTER message with network authentication failure indication;
   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.
5. The P-CSCF may only send the following messages to the unprotected port of the UE:
   - Authentication Challenge message;

- 4xx Unacceptable Proposal;

- 4xx Auth Failure;

The SIP layer in the UE is only allowed to handle this list of unprotected SIP messages, if the UE has an ongoing Register procedure and no valid SA. All other incoming SIP messages on the unprotected port shall be discarded by the SIP application in the UE.

[Editors'note:It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.