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

Tdoc S3-020228

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:	⌘	Removal of encryption between UE and P-CSCF as optional feature in Rel-5
Source:	⌘	Ericsson
Work item code:	⌘	IMS-ASEC
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:	⌘	It is understood that confidentiality (encryption) between the UE and the P-CSCF shall not be implemented within Rel-5 (not even optionally).
Summary of change:	⌘	Optional support of confidentiality protection between UE and P-CSCF is removed. Parameters to negotiate encryption mechanisms and algorithms are however kept for consistency with sip-sec-agree draft.
Consequences if not approved:	⌘	No standard encryption mechanisms would be available for used within Rel-5
Clauses affected:	⌘	5.1.3, B.1, D.2.1
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.

5 Security features

5.1.3 Confidentiality protection

~~Confidentiality mechanism need not be required for the first hop between the UE and the P-CSCF~~Confidentiality protection shall not be applied between the UE and the P-CSCF. It is recommended to offer encryption for SIP signalling at link layer i.e. between the UE and the RNC using the existing mechanisms as defined in [1].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

Annex B (informative): Mechanisms 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.]

B.1 [6.2] Confidentiality mechanisms

Confidentialy protection shall not be applied to SIP signalling between the UE and the P-CSCF.~~IPsec ESP may optionally be implemented for providing confidentiality of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. If ESP confidentiality is used, it shall be applied in transport mode between UE and P-CSCF. If ESP confidentiality is provided, it is always provided in addition to ESP integrity protection.~~

~~The SAs that are required for ESP shall be derived from the 128-bit integrity key CK_{IM} generated through IMS AKA, as specified in chapter 6.1.~~

~~If confidentiality is required, for each direction, there is one ESP SA for both confidentiality and integrity that shall be used between the UE and the P-CSCF. The encryption transform is identical for the two SAs in either direction. The encryption key for the SA inbound from the P-CSCF is CK.~~

~~The encryption key for the SA inbound from the P-CSCF is CK_{IM_in}. The encryption key for the SA outbound from the P-CSCF is CK_{IM_out}.~~

~~The encryption keys are derived as $CK_{IM\_in} = h1(CK_{IM})$ and $CK_{IM\_out} = h2(CK_{IM})$ using suitable key derivation functions h1 and h2.~~

~~The encryption key derivation on the user side is done in the ISIM. The encryption key derivation on the network side is done in the P-CSCF.~~

~~The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.~~

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.2 Security mode setup for IPsec ESP

This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.

D.2.1 General procedures specific to the ESP protection mechanism

The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs. The UE and the P-CSCF shall always include "NULL Encryption algorithm" in their respective lists of supported algorithms.

The P-CSCF shall use an unprotected port to be able to receive specific unprotected messages. This unprotected port has to be communicated to the UE, by using the *info* field of message SM6. This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM6. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.

The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.3).