Technical Specification Group Services and System Aspects **TSGS#21(03)0483**

Meeting #21, Frankfurt, Germany, 22-25 September 2003

Source: **SA WG3**

Title: **CR to 33.203: Introducing Cipher key Expansion for IMS (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meet	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SAWG3 Doc
SP-21	SP-030483	33.203	042	-	Rel-6	B	Introducing Cipher key Expansion for IMS	5.6.0	6.0.0	S3-030375

3GPP TSG-WG3 Meeting #29
San Francisco, USA, 15th–18th July 2003

Tdoc ⌘S3-030375

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **042** ⌘**rev** ⌘ Current version: **5.6.0** ⌘

*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:	⌘	Introducing Cipher key Expansion for IMS
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	29/06/2003
Category:	⌘	**B**
Release:	⌘	Rel-6

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:	⌘	Currently there is no confidentiality protection for Release 5 IMS between the UE and the P-CSCF. The mechanism in place in Relase 5 is the use of protection as defined in TS33.102 between the UE and the RNC. The aim for the access security was to create a framework that is independent of underlying security. This CR introduces the key expansion function for the encryption key.
Summary of change:	⌘	The change introduces a key expansion function for confidentiality protection
Consequences if not approved:	⌘	There will be no key expansion function in the TS which is required for confidentiality protection

Clauses affected:	⌘	Annex I			
Other specs affected:	⌘	**Y**	**N**		
		X		Other core specifications	⌘ TS24.229, TS24.228
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

Annex I (normative): Key expansion functions for IPsec ESP

Integrity Keys:

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending 32 zero bits to the end of IK_{IM} to create a 160-bit string.

Encryption keys:

Divide CK_{IM} into two blocks of 64 bits each :

$$CK_{IM} = CK_{IM1} \| CK_{IM2}$$

Where CK_IM1 are the 64 most significant bits and CK_IM2 are the 64 least significant bits.

The key for DES-EDE3-CBC is then defined to be

$$CK_{ESP} = CK_{IM1} \| CK_{IM2} \| CK_{IM1},$$

after adjusting parity bits to comply with [20].

[Editors Note: Should AES be implemented in Release 6 time frame the input key to AES shall be CK_{IM}]