Technical Specification Group Services and System Aspects **TSGS#20(03)0226**

Meeting #20, Hämeenlinna, Finland, 09-12 June 2003

Source: **SA WG3**

Title: **1 CR to 35.206: Addition of missing line to Rijndael S-box listing (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was approved by SA WG3 meeting #28 and is hereby presented to TSG SA#20 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030226	35.206	001	-	Rel-5	Addition of missing line to Rijndael S-box listing	F	5.0.0	SEC1-CSALG01, SEC1-PSALG01	S3-030274

3GPP TSG-SA WG3 #28
Berlin, Germany, 6-9 May 2003

Tdoc ⌘S3-030274

CR-Form-v7

CHANGE REQUEST

⌘	**35.206**	**CR**	**CR001**	⌘**rev**	**-**	⌘	Current version:	**5.0.0** ⌘

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:	⌘	Addition of missing line to Rijndael S-box listing		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC-CSALG01, SEC1-PSALG01	***Date:*** ⌘	06/05/2003
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:	⌘	A line is missing from the S-box listing in the Rijndael block cipher specification. Rijndael is the example kernel function for MILENAGE.
Summary of change:	⌘	Addition of missing line to Rijndael S-box listing.
Consequences if not approved:	⌘	Although the full definitive specification of Rijndael is already referenced by 35.206, it is desirable to correct the Rijndael specification in 35.206 to avoid confusion among implementors.

Clauses affected:	⌘	A2.9				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

***** FIRST CHANGE *****

A2.9 The Rijndael S-box

```
Sbox[256] = {
 99,124,119,123,242,107,111,197, 48,  1,103, 43,254,215,171,118,
202,130,201,125,250, 89, 71,240,173,212,162,175,156,164,114,192,
183,253,147, 38, 54, 63,247,204, 52,165,229,241,113,216, 49, 21,
  4,199, 35,195, 24,150,  5,154,  7, 18,128,226,235, 39,178,117,
  9,131, 44, 26, 27,110, 90,160, 82, 59,214,179, 41,227, 47,132,
 83,209,  0,237, 32,252,177, 91,106,203,190, 57, 74, 76, 88,207,
208,239,170,251, 67, 77, 51,133, 69,249,  2,127, 80, 60,159,168,
 81,163, 64,143,146,157, 56,245,188,182,218, 33, 16,255,243,210,
 205, 12, 19,236, 95,151, 68, 23,196,167,126, 61,100, 93, 25,115,
 96,129, 79,220, 34, 42,144,136, 70,238,184, 20,222, 94, 11,219,
224, 50, 58, 10, 73,  6, 36, 92,194,211,172, 98,145,149,228,121,
231,200, 55,109,141,213, 78,169,108, 86,244,234,101,122,174,  8,
186,120, 37, 46, 28,166,180,198,232,221,116, 31, 75,189,139,138,
112, 62,181,102, 72,  3,246, 14, 97, 53, 87,185,134,193, 29,158,
225,248,152, 17,105,217,142,148,155, 30,135,233,206, 85, 40,223,
140,161,137, 13,191,230, 66,104, 65,153, 45, 15,176, 84,187, 22};
```

***** END OF CHANGES *****