3GPP TSG-SA WG3 Meeting #36
Shenzhen, China, 23 – 26 November 2004

Tdoc ⌘S3-041092

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.222** **CR** **007** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Adding Support for AES in the TLS Profile
Source:	⌘	SA WG3
Work item code:	⌘	GBA-SSC
Date:	⌘	22/11/2004
Category:	⌘	**C**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Currently, only "TLS_RSA_ WITH_3DES_EDE_CBC_SHA" shall be supported both in the UE and the NAF. It is considered general security practice to support several algorithms for confidentiality and integrity protection
Summary of change:	⌘	Adding support for the "TLS_RSA_WITH_AES_128_CBC_SHA" cipher suite.
Consequences if not approved:	⌘	The general security practice of supporting several algorithms is not implemented in TS 33.222

Clauses affected:	⌘	5.3.1

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

Other comments:	⌘	

***** Begin of Change *****

5.3.1 TLS profile

The UE and the NAF shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [14] or higher. Earlier versions are not allowed.

NOTE: The management of Root Certificates is out of scope of this Technical Specification.

5.3.1.1 Protection mechanisms

The UE shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] are optional for implementation for the UE.

The NAF shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA ~~and~~, the CipherSuite TLS_RSA_WITH_RC4_128_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA.. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] are optional for implementation for the NAF.

~~Editor's Note: It is FFS if this specification should mandate any of the AES cipher suites as specified in RFC 3268 [7].~~

Cipher Suites with NULL encryption may be used. The UE shall always include at least one cipher suite that supports encryption during the handshake phase.

Cipher Suites with NULL integrity protection (or HASH) are not allowed.

Editor's Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [8] shall be implemented in this TS.

***** End of Change *****