3GPP TSG-SA3#34
6 - 9 July 2004
Acapulco, Mexico

Tdoc ⌘ S3-040628

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ 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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Additional requirements for Communication over local interface via a Bluetooth link
Source:	⌘	Toshiba, BT and supporting Companies
Work item code:	⌘	(U)SIM Reuse
Date:	⌘	28/05/2004
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:	⌘	Purposes some additional requirements that are necessary for communication over local wireless interface like Bluetooth
Summary of change:	⌘	Insertion of some additional requirements that are deemed necessary for secure communication over Bluetooth.
Consequences if not approved:	⌘	New feature could not be supported. And the specification will be incomplete that may result in inappropriate Bluetooth configurations in the WLAN-UE functional split case. This may result in a compromise of WLAN interworking security

Clauses affected:	⌘	2, 4.1.4, 4.2.4.1, 4.2.4.3, 6.1.1, 6.1.5, C3.1 and Annex A4

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

Other comments: ⌘

***** Start of change *****

1. The full 16 octet PIN shall be used for pairing and initialisation key establishment
2. The initialisation key establishment PIN shall be unique to each device.
3. Out of band secure distribution methods shall be used for the initialisation key establishment PIN
4. Combination keys shall be used for link key generation.
5. The connection shall be terminated and restarted at least once a day to force the use of a new random number in the Bluetooth ciphering process to prevent key stream repeats
6. Users shall be informed in the set up instructions about vulnerabilities that are inherent with Bluetooth devices in discoverable mode.
7. The use of a Separate Bluetooth interface/software stack for the local link that cannot be placed in discoverable mode by the user once the pairing process is complete may be considered for high security applications.
8. Only Bluetooth Version 1.2 shall be used which provides protection against interference from the WLAN interface in the same band shall be used
9. Deliberate denial of service attacks on the Bluetooth shall be minimised by reserving at least 20 channels for local link communication.

***** End of change *****