3GPP TSG SA WG3 Security — S3#26 **S3-020687**

19-22 November 2002

Oxford, UK

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.102** **CR** **CRNum** ⌘**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:	⌘	USIM support in GERAN only terminals
Source:	⌘	Lucent Technologies
Work item code:	⌘	Security
Date:	⌘	9/10/2002
Category:	⌘	**B**
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:	⌘	To support Group Release function.
Summary of change:	⌘	Introduces an interface to the f8 function to support group release functionality. Typographical errors in references are also corrected.
Consequences if not approved:	⌘	Group release will be insecure, allowing a denial-of-service attack.

Clauses affected:	⌘	6.7, 6.5.6, 6.6.6.

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

6.5.6 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the integrity protection function f9 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.~~202~~ 204 [14].

6.6.6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.~~202~~ 204 [14].

~~6.7 Void~~6.7 Group Release Authentication Function

In situations when the network loses information about UEs in connected mode, such as after an RNC, MSC or SGSN reset, the RNC(s) should bring all affected UEs down to idle mode, in order to keep the UEs reachable for terminating traffic. The most efficient way is to send a message to all or a group of terminals, forcing them back to idle mode. This function is called Group Release.

To avoid attacks where an adversary sends false Group Release messages, the UEs need to be able to authenticate the message.

The solution is that the RNC generates a secret, random, 128 bit Group Release Key, (GK). GK is common for a group of Ues. The RNC generates a Group Release Indicia (I) by:

$I = f_g(GK, SRNC\ id \| XXX)$,

where $f_g()$ is a one-way function and SRNC id is the 20 bit identifier unique for an RNC and XXX is of 12 bits and is set to 0.~~.~~ The RNC may generate new Group Release Keys periodically, and would then need to calculate and send a new Group Release Indicia to the UEs.

In situations such as those mentioned above, the RNC sends a Group Release message to all affected UEs with GK included, addressed to the group of UEs which share the same GK. (This is the first time that GK leaves the RNC.) Each UE runs $I=f_g(GK,SRNC\ id \| XXX)$, and compares the result to its stored I. If they are equal, the message is considered authenticated and the UE enters idle mode. The UE will delete the stored value I.

Once the GK is sent over the air, the RNC shall generate new Group Release Key, and would then need to calculate and send a new Group Release Indicia to the UEs which had previously been assigned Indica generated by the old Group Key.

The authentication function f_g is derived from the ciphering function f8. The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11]. The following values are used as the input variables for f8:

- GK is used as the CK input (128 bits)
- SRNC_id+XXX is used as the as the COUNT-C input (32 bits)
- BEARER (5 bits) and DIRECTION (1 bit) are set to zero
- LENGTH is set to 128, indicating that the required I is 128 bits in length

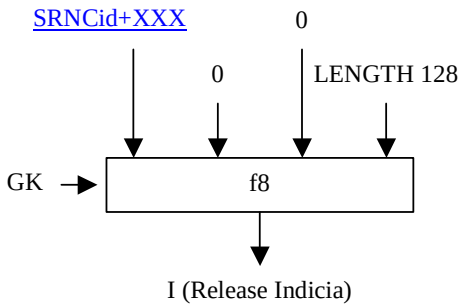

Figure 17: Calculation of Group Release Indicia

The 128-bit output keystream block forms the Group Release Indicia (I). Figure 17 illustrates the use of f8 for this function.