3GPP TSG SA WG3 Security — SA3#35 **S3-040735**

October 5-8, 2004

St Paul's Bay, Malta

Agenda item: 6.9.1 GAA

Title: Safety of key material

Source: Huawei

Document for: Discussion and Decision

1 Introduction

The safety of GBA key material in GAA was discussed in the last meeting, a discussion paper and a pseudo-CR for adding the corresponding text to 33.919 were presented. But it was thought that there was no corresponding text in the GBA TS and it was considered premature to add it at that time

We think the key safety of usage is important for use of GBA. The attached CR to 33.919 introduce the requirement to Application guideline to use GAA. There is another contribution to 33.220 discussing the corresponding solution and proposing to add the solution to 33.220.

3GPP TSG-SA WG3 SECURITY Meeting #35
St Paul's Bay, Malta, 5-8 October 2004

Tdoc ⌘Att1_S3-040735

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.919**	**CR**	**001**	⌘**rev**	**-**	⌘	Current version:	**6.0.0** ⌘

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

St Paul's Bay, Malta

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

Title:	⌘	Key safety with usage		
Source:	⌘	Huawei		
Work item code:	⌘	GAA	***Date:*** ⌘	28/09/2004
Category:	⌘	**F**	***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:	⌘	The key leaking out is potential security threaten during the usage of the service, e.g. leakage of key with not well safed local connections in UE, then a frequent stolen service request may happen within a short time slot. From the whole architecture consideration, GAA and the corresponding Application (NAF) should be able to limit the abnormal using of the shared secret and take action to mitigate it as much as possible.
Summary of change:	⌘	Add a requirement to Application guideline for using shared secret and GBA safely.
Consequences if not approved:	⌘	NAF ignore the abnormal usage of key material ,and potential security threaten of service stolen may happen

Clauses affected:	⌘	7.1			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

7.1 Use of shared secrets and GBA

Some examples of where shared secrets from the innovation of GBA can be used are:

- distribution of symmetric ciphering and integrity keys for securing applications running between the UE and a server in he network. Example protocols that can be used to secure an application and that require a shared secret include HTTP Digest, shared secret TLS and IPsec;
- distribution of passwords and PIN for third party applications;
- for protecting the distribution of certificates between the UE and the certificate authority.

Security of using the shared secrets and GBA:

When the Application use the shared secret generated in GBA, the NAF should be able to limit abnormal using the shared secrets (e.g., encroached a reasonable frequency or times set by the operator)and initiate the bootstrapping renegotiation described in TS 33.220 to get new shared secrets.