3GPP TSG SA WG3 Security — S3#34 **S3-040596**

July 6 - 9, 2004

Acapulco, Mexico

TSG-SA WG1 #25 **S1-040645**
Montreal, Canada, 28 June - 02 July 2004 **Agenda Item:**

Title:	SA1's answer to LS on VGCS and VBS security
Response to:	LS (S1-040565 = S3-040447) on "Liaison Statement on VGCS and VBS security" from SA WG3
Release:	6
Work Item:	Key Management of group keys for Voice Group Call Services
Source:	**SA1**
To:	SA3
Cc:	ETSI EP RT

Contact Person:
Name: Jörg Swetina (Siemens)
Tel. Number: +43 676 481 24 29
E-mail Address: joerg.Swetina@siemens.com

Attachments: S1-040643, S1-040644: CRs to 42.068 and 42.069 to include requirements on VGCS and VBS security.

1. Overall Description:

SA1 would like to thank SA3 for their LS on VGCS and VBS security.
SA1 understands, that SA3 has already done most of the work to support VGCS and VBS ciphering in Rel-6 and that the remaining open issues mentioned in SA3's LS are not so much addressed to SA1 as to the other recipients of the LS.

However, two CRs to the stage 1 specifications TS 42.068 and TS 42.069 have been agreed in SA1. The wording of these CRs has been aligned as far as possible to the text in F.1.1 of CR S3-040427, which had been attached to SA3's LS.

The CRs to 42.068 and 42.069 are attached for information.

2. Actions:

To SA3 group.

ACTION: SA1 asks SA3 to respond in case of any problems seen with the attached CRs.

3. Date of Next TSG-SA1 Meetings:

SA1#26	11 – 15 October 2004Sophia Antipolis, FR	European friends of 3GPP

TSG-SA WG1 #25 **S1-040643**
Montreal, Canada, 28 June - 02 July 2004 **Agenda Item: 8**

CR-Form-v7

CHANGE REQUEST

•	**42.068**	**CR**	**002**	• **rev**	**-** •	Current version: **5.0.1** •

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	X	Core Network X

Title:	•	Addition of optional over-the-air ciphering for VGCS		
Source:	•	Siemens		
Work item code:	•	SECGKYV	Date: •	28/06/2004
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: •	In LS S1-040565 (S3-040447) SA3 had informed SA1 on their activities concerning VGCS and VBS security. Up to date group call services (VGCS, VCS) did not use over-the-air ciphering - in contrast to what is common practice for "ordinary" telephony services. A work item of SA3 (Key Management of group keys for Voice Group Call Services) has removed this deficiency. TS 42.068 needs to be aligned.
Summary of change: •	To align TS 42.068 to the work done by SA3 a new clause on security requirements is introduced. VGCS shall be able to support over-the-air ciphering
Consequences if not approved: •	Misalignment of stage 1 specification

Clauses affected: •			new clause 5.6		
		Y	**N**		
Other specs affected: •		X		Other core specifications •	43.020
			X	Test specifications	
			X	O&M Specifications	

Other comments: •	The corresponding SA3 work in Rel-6 has already been done.

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked • contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.6 Security requirements

VGCS shall be able to support over-the-air ciphering in order to provide confidentiality protection to group calls.

VGCS ciphering is an operator’s option.

VGCS shall provide means such that only a legitimate service subscriber is able to participate in a ciphered VGCS call when the operator requires confidentiality protection for the group call. To include a subscriber into a ciphered voice group the required group data shall be stored on the USIM. Storing these group data on the USIM may be done e.g. during the USIM personalisation process or via OTA (over-the-air) provisioning.

A pre- Rel-6 VGCS capable mobile shall be able to participate in an un-ciphered group call, if it is part of that group.

TSG-SA WG1 #25 **S1-040644**
Montreal, Canada, 28 June - 02 July 2004 **Agenda Item: 8**

CR-Form-v7

CHANGE REQUEST

• **42.069**	**CR**	**002**	• **rev**	**-**	• Current version:	**5.0.1** •

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 optional over-the-air ciphering for VBS		
Source:	•	Siemens		
Work item code:	•	SECGKYV	Date: •	28/06/2004
Category:	•	**B** 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.	Release: •	Rel-6 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: •	In LS S1-040565 (S3-040447) SA3 had informed SA1 on their activities concerning VGCS and VBS security. Up to date group call services (VGCS, VCS) did not use over-the-air ciphering - in contrast to what is common practice for "ordinary" telephony services. A work item of SA3 (Key Management of group keys for Voice Group Call Services) has removed this deficiency. TS 42.069 needs to be aligned.
Summary of change: •	To align TS 42.069 to the work done by SA3 a new clause on security requirements is introduced. VBS shall be able to support over-the-air ciphering
Consequences if not approved: •	Misalignment of stage 1 specification

Clauses affected: •	new clause 5.6				
	Y	N			
Other specs affected: •	X		Other core specifications	•	43.020
		X	Test specifications		
		X	O&M Specifications		

Other comments: •	The corresponding SA3 work in Rel-6 has already been done.

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked • contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.6 Security requirements

VBS shall be able to support over-the-air ciphering in order to provide confidentiality protection to group calls.

VBS ciphering is an operator’s option.

VBS shall provide means such that only a legitimate service subscriber is able to participate in a ciphered VBS call when the operator requires confidentiality protection for the group call. To include a subscriber into a ciphered voice group the required group data shall be stored on the USIM. Storing these group data on the USIM may be done e.g. during the USIM personalisation process or via OTA (over-the-air) provisioning.

A pre- Rel-6 VBS capable mobile shall be able to participate in an un-ciphered group call, if it is part of that group.