3GPP TSG SA WG3 Security — S3#31 **S3-030658**
18 - 21 November 2003
Munich, Germany

SMG10 meeting #4/98 **Tdoc SMG10 98P252**
Issy-les-Moulineaux, 17 to 20 November 1998

ETSI SMG#27 **Tdoc SMG 0531/98**
Praha, 12 to 16 October 1998
Agenda Item: 6.10 and 7.10

Source: **SMG10 (Technical manager for security aspects)**
Date: **October 1998**

ASCI security: After studying of an input document on ASCI security the view was supported that there might be a security risk by the introduction of these services. eMLPP, VGCS and VBS do not represent sources of technical fraud. With careful management, they do not represent a risk to network operators. Their users should be made aware of the small risks of eavesdropping and masquerade. The task of making users aware of the risks, and of implementing good operator control of the services, is the responsibility of operators offering the service. However, SMG10-WPB was concerned that there might be legal liability problems for ETSI because the service is designed to be used in emergency sitiuations and yet is vulnerable to fraud. The chairman will pursue this matter with the chairman of SMG. An LS to be sent to MoU-SG is proposed in Annex A.

Annex A: Proposed LS to MoU-SG on ASCI fraud issues (to SMG#27 for advice)

SMG10 meeting #3/98 **Tdoc SMG10 98P211**
Sophia Antipolis, 28 to 31 July 1998

From: SMG10
To: MoU-SG

Liaison statement to MoU -SG on ASCI –fraud issues

SMG10 has reviewed the enclosed document on ASCI and draws attention to the security issues.

SMG10 believes that MoU-SG should issue guidance to Operators on this topic.

Enclosed Tdoc SMG10 98P181 for information to help draw up the guidance.

Attachment to Tdoc SMG10 98P211: Annex A

SMG10 #3/98 **Tdoc SMG10 98P181**
Sophia Antipolis, 28-31 July, 1998 **Source : Vodafone**

Fraud Review of Advanced Speech Call Items (ASCI)

Introduction

This document is a fraud review of the ASCI services, enhanced multi-level precedence and pre-emption (eMLPP), voice group call (VGCS) and the voice broadcast services (VBS). It has been written to fulfil an action taken by Vodafone at the SMG10 plenary at Lund, April 1998.

SMG10 looked at the ASCI items at the Torino meeting (October 1997) but due to confusion, the resulting liaison statement was not delivered to SMG and subsequent discussion did not take place.

The ASCI project was developed under the instigation of the *Union Internationale des Chemins de Fer* (UIC), for convenient and quick “PMR-type” communication between railway operatives. However, as it has been standardised, it can be used in any scenario, and will be reviewed with this in mind.

Service Descriptions

Enhanced Multi-Level Precedence and Pre-emption (eMLPP) service

The eMLPP service [GSM 02.67] is an enhancement for GSM networks of the ISDN MLPP service to meet the UIC requirements.

The eMLPP service specifies how to handle precedence levels for subscribers within a PLMN including the possibility of pre-emption of ongoing calls. eMLPP defines set-up classes which specify the set-up time and the pre-emption capability. eMLPP is applicable to tele- and bearer services.

eMLPP service consists of two parts: precedence and pre-emption.

- Precedence involves assigning a priority level to a call in combination with fast call set-up.
- Pre-emption involves the seizing of resources that are in use by a call of a lower precedence by higher-level precedence call. This can also involve the disconnection of an on-going call of lower precedence to accept an incoming call of higher precedence.

eMLPP provides different levels of precedence for call set-up and for call continuity in case of handover. There are at maximum seven priority levels.

Table 1: ASCI – Priority levels

A (highest)	for network internal use
B	for network internal use
0	for subscription
1	for subscription
2	for subscription
3	for subscription
4 (lowest)	for subscription

The two highest levels A and B are reserved for network internal use, e.g. for emergency calls or network related service configurations like voice group call services. They can only be used locally, i.e., within the domain of a MSC. The other five levels (0-4) are offered for subscription and can be applied globally if supported by all related network elements.

Usually, the priority depends on the calling subscriber who can select the priority level at set-up. If the subscriber has no eMLPP subscription (or no MLPP subscription in case of a call from the fixed network) a default priority level is given.

The call set-up time is defined as the time from pressing the send-button to the point at which the called party, or at least one called party in the case of a multi-party call, can receive information. There are three classes of set-up time performances and examples of the call set-up times are:

- class 1 fast set-up 1–2s;
- class 2 normal set-up <5s;
- class 3 slow set-up <10s

The network decides the call set up class to assign to a call when the call setup (with eMLPP indicated) message is received from the MS.

For precedence calls, the network shall have the possibility to pre-empt ongoing calls with lower priority, in ascending order of priority. Pre-emption is possible at call set-up or at handover.

Table 2: ASCI – Example on eMLPP service composition

Priority level	Set-up time	Pre-emption	Examples
A	class 1	yes	VBS/VGCS emergency application
B	class 2	yes	Operators calls
0	class 2	yes	TS 12 Emergency calls
1	class 3	Yes	Premium rate calls
2	class 3	No	Standard rate calls
3	class 3	No	Default for no eMLPP subscription
4	class 3	No	Low tariff calls

Security Options

There is the option for the network to postpone or not perform authentication at call set up (and ciphering) for a call with a high priority requiring a class 1 set-up. This applies to both MO and MT calls. The network can announce that such calls are possible (i.e. that an eMLPP MS may send a SETUP message before an AUTH_REQ message) using the BCCH.

Authentication is still performed at location update however, so if fast call set up is to be used, the subscriber must be already registered in the network.

Voice Group Call Service (VGCS, [GSM 02.68])

Definitions (also apply to VBS)

A GSM subscriber who has subscribed to VGCS or VBS is a **service subscriber**.

A group of service subscribers who wish to communicate with each other using VGCS or VBS will be assigned a **group ID** for that group.

The **calling subscriber** may be any service subscriber which has subscribed to the related group ID and is entitled to establish a call/broadcast by the terms of his subscription or any dispatcher who is entitled to be calling subscriber and is registered in the network.

Particular fixed line or mobile users are identified as **dispatchers**.

Destination subscribers are all service subscribers which belong to a group identified by the group ID which have their present location in the service area and pre-registered dispatchers.

Principle: The VGCS [GSM 02.68] allows speech conversation of a predefined group within a predefined area (the Group Call Area). The initiator of a group call may be a service subscriber or a user of a fixed network. The speaker may change during the ongoing call.

Establishment of a voice group call

The group call shall be established in a service area that is comprised of one or a cluster of cells. Service areas shall be predefined at registration. In case of a service subscriber initiating a VGCS, the service area is uniquely identified by **the actual cell in which the service subscriber resides at the moment of VGCS call initialisation** and by the group ID they issue. A dispatcher initiating a VGCS call will be connected to a related predefined service area.

Ongoing call

The service shall permit only one talking service subscriber at any moment; additionally up to five dispatchers can be talking simultaneously at one time. Dispatchers should hear all combinations of voices other than their own. Listening service subscribers shall hear the combination of all voices. The talking service subscriber shall gain some audible indication if any dispatchers are talking simultaneously.

Security Options

As a network option the mobile station of the talking service subscriber can be requested to send its IMSI to the network in order so that the talker's IMSI be stored in the event records.

- ***Authentication of calling subscribers at VGCS invocation is optional.*** *(The omission of authentication applies to call set up only. The subscriber must be perform authentication as normal for location update)*

- ***Authentication of the talking service subscriber is optional.***

- ***Confidentiality on the radio path for the talker is optional.***

Voice Broadcast Service (VBS, [GSM 02.69]

VBS [GSM 02.69] specifies the capability to set-up a point to multi-point connection for the uni-directional distribution of speech. The call is initiated by a subscriber or a fixed destination (dispatcher) into a predefined geographical area (service area) to a predefined group of subscribers located in this area (and additionally up to eight (including the initiator) fixed destinations).

Destination subscribers must be within the service area to initiate or receive the broadcast.

Dispatchers in VBS receive all voice broadcasts to groups of which they are a part. In addition, they can initiate broadcasts to groups of which they are a part.

The broadcast call shall be established in a service area that is comprised of one or a cluster of cells. Service areas shall be predefined at registration.

Establishment of a voice broadcast call

In case of a service subscriber initiating a VBS call, the broadcast area is uniquely identified by the **actual cell in which the service subscriber resides at the moment of VBS call initialisation** and by the called group ID. A dispatcher initiating a VBS call will be connected to a related predefined broadcast area. Since a dispatcher may be registered to more than one broadcast area and group ID an indication of the wanted broadcast area and group ID has to be given in form of a dedicated address called by the dispatcher.

Release of a Broadcast call

Service subscribers who leave the broadcast area during an on going VBS call cease to be destination subscribers. Service subscribers which enter the broadcast area during an on going VBS call shall become destination subscribers within 500ms after reception of the first paging message related to the VBS call.

The calling subscriber shall remain within the broadcast call until he terminates the call, loses contact with the network or leaves the broadcast area.

Optional requirements

- ***Authentication of calling subscribers at VGCS invocation is optional.*** *(The omission of authentication applies to call set up only. The subscriber must be perform authentication as normal for location update)*

- ***Authentication of the destination subscribers is not required.***

- ***Confidentiality on the radio path is optional.***

Fraud Potential

eMLPP

The risks with eMLPP stem from the possibility of non-authentication (“fast call setup”) for high priority calls. There is the possibility of intruders masquerading as other MS.

The fast call setup option (authentication postponed or not performed at all) is only open to eMLPP subscribers, and presumably only those with a high priority. An intruder would therefore require the identity of the MS with such a priority in order to perform the masquerade.

This identity could be obtained through insider fraud, or, if the eMLPP transmits its IMSI to the network or receives a new TMSI from the network, in the clear. to obtain the IMSI by eavesdropping, the intruder, would have to know that the target MS had eMLPP. In such a case, the intruder would have to shadow the target user and hope that the identity could be revealed and scanned. Insider fraud seems more likely.

Authentication can only be omitted at call setup, it is still required for location update and registration. Therefore the intruder can only masquerade a subscriber who is **already registered in the network** and not requiring location update. The presence of the intruder may be revealed when the genuine subscriber attempts to make a call while the intruder already has a call in progress or where both the intruder and genuine subscriber respond to a paging message.

The “fast call setup” option should only be used in emergency situations. There should therefore be the possibility of procedures at the network where all records of calls with fast call setup and checked regularly with the user. Also, the calls would only be to specific destinations, and this could be used for online or offline checking.

Therefore, the monetary gain from being able to masquerade as a MS with high priority seems low, assuming that the use of fast call setup is sparse and carefully monitored. However, there may be a more serious use, that of masquerade as the operative with fast call setup, with intent to mis-inform. This could only be done if the genuine user’s voice was not known to the listeners but is a possibility and a serious consideration, especially where details of emergency situations are being communicated. Users of eMLPP should be aware of the possibility of masquerade.

Unlike VBS and VGCS, non-authentication with eMLPP can occur anywhere, not just within a specified service area.

The risks can be made all but negligible, and fast call setup retained, if instead of not performing authentication, the network merely **postpones** it until after the call is setup.

VBS and VGCS

If the group chooses not to use confidentiality then the group members run the risk of eavesdropping on the air interface. However, as long as the group members are informed of the lack of confidentiality, they can take responsibility for the risk of eavesdropping and it need not be a cause of concern.

The option for the calling subscribers and other participating group members to be un-authenticated is of more concern.

The identities of all members of a group must be registered with the network before operation of the group can begin. There is therefore no possibility of new identities being allowed into a group call or broadcast during a call.

However, there is the possibility of intruders masquerading as members of the group if authentication is not used. This would allow the intruder to set up or receive voice broadcasts and group calls. As for eMLPP, authentication at location update is still performed, so the intruder can only masquerade as subscribers who are already registered in the network. The genuine subscriber may recognise the presence of the intruder by degradation in service, as illustrated for eMLPP.

Group members should be informed that in forming a group where authentication is optional, they run the risk of intruders masquerading as members of the group. However, charging liability questions aside[1], the group members are the only parties affected by the risk and it need not, therefore, be of cause to the network operator who has good procedures in place. It can reasonably be assumed, that for a group call, or group broadcast, there would be at least one listener who would be able to recognise, by voice, if an intruder were masquerading as the caller.

As VGCS and VBS can only be used within defined areas to defined other parties, the motivation for an outsider to attempt to initiate calls seems low. The opportunities for eavesdropping seem more of a lure, but only a collection of fools would use unciphered links for regular communication of sensitive information.

Conclusions

With suitable internal security (for list of subscribers with high priority eMLPP) and procedures (high priority eMLPP given only in exceptional cases, and regular usage checks), a network operator has a minimal risk of fraud. If the network postpones the authentication for fast call set-up, rather than not performing it, there seems to be no risk[2]. The subscriber to eMLPP can be made responsible for any fraud conducted in return for the privilege of fast call set-up. The subscriber should accept the risk of eavesdropping on the unciphered link and the possibility of masquerade with intent to misinform.

VGCS and VBS can only be used within defined areas. The motivation for call originated fraud by an outsider therefore seems low. Again, there is a risk of eavesdropping and masquerade, which subscribers should be aware of and have accepted as a risk.

eMLPP, VGCS and VBS do not represent sources of technical fraud. With careful management, they do not represent a risk to network operators. Their users should be made aware of the small risks of eavesdropping and masquerade.

The task of making users aware of the risks, and of implementing good operator control of the services, is the responsibility of operators offering the service. The sending of a liaison to MoU SG regarding the risks with the ASCI services is therefore recommended.

References

[GSM 02.67]	enhanced Multi-Level Precedence and Pre-emption service, (eMLPP), Stage 1, GSM 02.67 version 5.0.5
[GSM 02.68]	Voice Group Call Service (VGCS), Stage 1, GSM 02.68 version 5.1.3
[GSM 02.69]	Voice Broadcast Service (VBS), Stage 1, GSM 02.69 version 5.1.1

Acknowledgements

This document incorporates descriptions of ASCI written by Volker Kessler (Siemens AG) as part of the ACTS USECA project.

[1] Realistically, in setting up a group where authentication is optional, group members must accept all call charges attributed to the group. The possibility of repudiation must not be given, as there is no way of establishing it.

[2] Apart from that of “denial of service” if an intruder repeatedly sets up calls which are torn down by the network after authentication fails. If this does occur the MSC could withdraw the right for all fast call set up, or, if this is required for other MS, simply cancel the user registration in the VLR. Re-registration would require location update, which would involve authentication.