3GPP TSG SA WG3 Security — S3#29 **S3-030402**
15 - 18 July 2003
San Francisco, USA

Source: **Siemens**

Title: **Effects of service 27/38 on 2G/3G Interworking and emergency call**

Document for: **Discussion and decision**

Agenda Item: **7.5 and 7.6**

Abstract

This paper discusses the use of service 27 and 38 and the effects on 2G/3G Interworking and emergency calls.

1 Introduction and overview of specifications

TS 31.102 (T3) clause 4.2.8 defines

- Service 27 as 'GSM access' which resembles feature 1 of TS 33.102 (see later paragraph). The USIM only includes the Key Kc in a 3G authentication response if service 27 is available.
- Service 38 is called 'GSM security context'. Feature 2 of TS 33.102 (See later paragraph) requires that both Service 27 and 38 be present on the USIM.

TR 31.900 (T3) clause 5.1 specifies

"To support a 2G/3G dual mode ME in a 2G radio access network, the USIM may provide functions for 2G backward compatibility. Two particular USIM services are defined for such purposes:

1. ***Service n° 27:*** *"GSM Access". This service is essential when a 2G BSS is involved. The USIM additionally generates the 2G ciphering key Kc required by the 2G air interface. From the security point of view, this behaviour can be characterised as "**3G + Kc mode**" (see below). Further, the USIM supports some additional 2G data storage elements that are necessary for 2G radio access.*
2. ***Service n° 38:*** *"GSM Security Context". This service is required when a 2G VLR/SGSN and/or a 2G HLR/AuC is involved. The USIM performs 2G AKA, i.e. it accepts 2G input data and generates 2G output data. From the security point of view, this behaviour can be characterised as "**virtual 2G mode**" (see below).*

   *A 2G VLR/SGSN never goes with a 3G BSS. Hence when a 2G VLR/SGSN is involved, then a 2G BSS is always part of the transmission chain and service n° 27 is additionally required**, i.e. services n° 27 and n° 38 have to be available at the same time.***

If services n° 27 and n° 38 are not supported by the USIM (which the ME can detect from the USIM Service Table during the USIM activation procedure) network access is impossible in a mixed 2G/3G environment, even if a SIM application is available on the UICC. A 3G ME only accesses the USIM application on the UICC.

From the security point of view, the compatibility services are connected to up to three different operation modes (see also Annex B):

- ***Normal 3G mode:*** *The results of the 3G algorithm are sent to the ME without any change. The USIM receives RAND and AUTN and responds with RES, CK and IK. This mode applies if service n° 27 is not available.*

- ***3G + Kc mode:*** *The 2G ciphering key Kc (derived from CK, IK) is additionally included in the response. The USIM receives RAND and AUTN and responds with RES, CK, IK and Kc. This requires conversion function c3 to be supported by the USIM. If service n° 27 is available in the USIM, this mode is always active and the ME picks the relevant values from the USIM response according to the present network situation.*

- ***Virtual 2G mode:*** *The USIM receives a 2G authentication request with RAND and returns a 2G authentication response with SRES (derived from RES) and ciphering key Kc (derived from CK, IK). This requires a particular algorithm execution mode plus conversion functions c2 and c3 to be supported by the USIM. If service n° 38 is available in the USIM, this mode is not always active. The ME may switch the USIM from normal 3G mode or 3G + Kc mode to virtual 2G mode by sending a particular command parameter according to the present network situation.*

The services n° 27 and n° 38 are both optional. Network operators can decide whether to include them into their USIMs and hence to allow network access with lower security level."

Section 6.8.1.5 of TS 33.102 defines optional USIM features to enable backwards compatibility with GSM.

"The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

Feature 1:	*GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;*
Feature 2:	*GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using R99+ ME not capable of UMTS AKA or R98- ME;*
Feature 3:	*SIM-ME interface (GSM 11.11) to operate within R98- ME or R99+ ME not capable of UMTS AKA.*

A CR to TS 33.102 has been submitted to SA3#29 to correct the inaccuracy in clause 6.8.1.5 saying that GSM access can be forbidden by not implementing Service 27. This however does only apply if that service is not implemented in the ME and if ciphering is active in the BSS. TR 31.900 includes the same inaccuracy.

This contribution focuses on the consequences to 2G/3G interworking and emergency calls.

2 2G/3G interworking and emergency call scenarios

2.1 The effects of Service 27

A serving network does currently not know anything about USIM capabilities (i.e. on the lack of, or existence of any service implemented on the USIM). The dual mode mobile will indicate support of GSM and UMTS bands in the classmark irrespective of the presence of 'service 27'. The classmark does only indicate ME capabilities.

Suppose we take a dual mode mobile and insert a USIM within it that has 'service 27' not implemented.

Some of these scenarios also apply for a R99 single mode GSM capable mobile that supports the USIM interface.

Following scenarios may happen:

SCN-1. First a connection is setup via UMTS access, thereafter a handover is started. The handover will **fail** if GSM access ciphering is **activated** by the serving network because the USIM did not generate the key Kc. The network has no indication of the error reason. The network might repetitively try to handover the mobile, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM access) may be able to correlate this to the failed handover after having viewed the 'GSM network ciphering indicator' on his display.

SCN-2. The mobile tries to location update while being under GSM coverage. The connection will be **rejected** if GSM access ciphering is subsequently **activated** by the serving network because the USIM did not generate the key Kc. The network has no indication of the error reason. The network might repetitively try to activate ciphering, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM access) may be able to correlate this to the failed connection after having viewed the 'GSM network ciphering indicator' on his display.

SCN-3. First a connection is setup via UMTS access, thereafter a handover is started. The handover will **succeed** when GSM access ciphering is **NOT activated** by the serving network.

Now let's consider following scenarios for emergency calls:

SCN-4. An emergency call will succeed while being under GSM coverage when the USIM is NOT inserted. (if the serving network allows USIM-less calls).

SCN-5. An emergency call cannot be set up while being under GSM coverage with ciphering enabled when a USIM is inserted while the USIM did not generate the key Kc.

SCN-6. An emergency call can be set up while being under GSM coverage with ciphering disabled when a USIM is inserted.

Also SCN-1 to SCN-3 applies for Emergency calls;

As can be seen from these scenarios the absence of 'service 27' on the USIM which is inserted in a dual mode ME can have some unexpected effects to the call.

The expected behavior from service 27 (i.e. GSM only access) for a user having such a USIM is similar with that of a mobile indicating MS classmark 'UMTS only'. However if the MS classmark is set to "UMTS only" then a dual mode ME with such a USIM inserted could not make an emergency call anymore over GSM (now irrespective of whether ciphering is enabled or not).

It is therefore important to discuss this first from a service point of view with following list of question that need to be answered:

1) Should an ME with a USIM without service 27 be prevented from accessing GSM systems regardless of whether or not GSM ciphering is enabled?
2) Should an ME with a USIM without service 27 be prevented from handing over from UMTS to GSM regardless of whether or not GSM ciphering is enabled?
3) Should an ME with a USIM without service 27 be prevented from making GSM emergency calls?
4) Should an ME with a USIM without service 27 be prevented from handing over emergency calls from UMTS to GSM?

2.2 The effects of service 38

Suppose we take a dual mode mobile and insert a USIM within it, that has 'service 38' not implemented. Some of these scenarios also apply for a R99 single mode GSM capable mobile that supports the USIM interface.

Following scenarios may happen:

SCN-7. First a connection is setup via UMTS access, thereafter a handover is started. The handover may fail if a new 2G authentication is performed within the target serving network. This may be happen during or after handover. The network might repetitively try to authenticate the mobile, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM security context) may be able to correlate this to the failed handover or dropped call after having viewed the 'GSM network ciphering indicator' on his display.

SCN-8. The mobile tries to location update when a pre-R99 MSC/SGSN is involved. The connection will be rejected if 2G authentication is subsequently **activated** by the serving network because the USIM does not support 2G authentication. The network has no indication of the error reason. The network might repetitively try to authenticate the mobile during the location update, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM security context) may be able to correlate this to the failed connection after having viewed the 'GSM network ciphering indicator' on his display.

Now let's consider following scenarios for emergency calls:

SCN-9. An emergency call will succeed while being under GSM coverage when the USIM is NOT inserted. (if the serving network allows USIM-less calls).

SCN-10. An emergency call cannot be set up while being under GSM coverage if pre-R99 MSC/SGSN is involved. The network might repetitively try to authenticate the mobile, which may cause unnecessary signaling load in the network.

Also SCN-7 to SCN-8 apply for Emergency calls;

Similar scenarios can happen if using a GSM capable mobile with a USIM that has 'service 38' not implemented, but only 'service 27'.

Similar questions as with ‘service 27’ can be asked:

5) Should an ME with a USIM without service 38 be prevented from making GSM emergency calls?
6) Should an ME with a USIM without service 38 be prevented from handing over emergency calls from UMTS to GSM?

3 Proposal

Siemens proposes to ask CN1 if TS 24.008 does cover the above described scenarios. The mentioned CR to TS 33.102 should be attached to make them aware that the result of the call or handover might depend on the ciphering status of the GSM access network. This case was not covered in TS 33.102 so far.

As the behaviour in the described scenarios (SCN-x) are a consequence of an operators decision to use USIMs with service 27 NOT-implemented respectively service 38 NOT-implemented, there may be a need to document this behaviour in detail, in order to make operators aware of the consequences.

SA1 or GSMA could be informed about this in order to find a suitable place to document this. The TR 31.900 (T3) may be a suitable place to incorporate these issues.