3GPP TSG SA WG3 Security#30 **S3-030585**
6 – 10 October, 2003
Povoa de Varzim, Portugal

Source: **Siemens**

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

Document for: **Discussion and decision**

Agenda Item: **7.5**

Abstract

This paper documents the scenarios that have been identified with the absence of the optional service 27 and or 38 on the USIM and the effects on 2G/3G interworking and emergency calls. S3-030402 (SA3#29) and S3-030499 (LS from CN1) have been used as a base.

1 2G/3G interworking and emergency call scenarios

1.1 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-2a First a PS connection is setup via UMTS access, and a PDP context is activated. Thereafter the mobile performs a cell re-selection to GSM. When the mobile tries to perform a routing area update, the request will be **rejected** if GPRS GSM access ciphering is subsequently **activated** by the serving network, because the USIM did not generate the GPRS GSM cipher key. The activated PDP context cannot be used by the mobile, or modified or deleted via DTAP signalling, until the mobile performs another cell re-selection to UMTS. (Note: added from the LS from CN1 to SA3: S3-030499)

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).

1.2 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'.

2 Proposal

From the received LS's to this meeting (S3-030499-CN1) and (S3-030510-T3), neither CN1 nor T3 take the responsibility to incorporate the detailed scenarios within their respective specifications. T3-specification TR 31.900 has been adapted (T3-030694) to mention that there are effects on emergency call set up and handover. The detailed behaviour is missing and it is thought to be out of scope of the T3-specification. This is understandable as the T3 specification is a terminal centric description and the scenarios include core network behaviour.

SA3 should make a decision whether T3-030694 is enough from a 3GPP specification point of view. If SA3 does decide not to document the detailed scenarios within 3GPP then Siemens proposes to forward the scenarios to GSMA SG and ask them to document the scenarios within a public GSMA document.