3GPP TSG SA WG3 (Security) meeting #30 **S3-030516**

6-10 October 2003

Povoa de Varzim, Portugal

Source:	**Secretary SA WG3 (M. Pope, MCC)**
Title:	**Documents approved by e-mail after SA Wg3 meeting #29**
Document for:	**Information**
Agenda Item:	**5.1**

The attached documents were subject to e-mail approval after the last SA WG3 meeting and are provided here for information.

S3-030473	Reply to LS N4-030722 (=S3-030337) on adapting Cx interface protocols for security purposes	SA WG3	Approved by e-mail by 28 July 2003
S3-030474	LS on 'Effects of service 27/38 on 2G/3G Interworking and emergency call'	SA WG3 (e-mail)	Approved by e-mail 13 August 2003
S3-030475	Reply to LS on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030476	Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030477	Reply to LS on DoS attacks against the 3GPP WLAN Interworking system	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030478	CR to TS 33.102: IMEISV retrieval before completion of security mode setup procedure	SA WG3 (e-mail)	Approved by e-mail 5 September 2003
S3-030479	CR to 33.102: Mitigation against a man-in-the-middle attack associated with early UE handling	SA WG3 (e-mail)	Approved by e-mail 19 September 2003

3GPP TSG SA WG3 Security — S3#29 **S3-030473**
15 – 18 July 2003
San Francisco, USA

Title:	Reply to LS N4-030722 (=S3-030337) on adapting Cx interface protocols for security purposes
Work Items:	Support for subscriber certificates (SEC-SC), Security issues of Presence Capability (PRESNC), MBMS
Source:	3GPP SA3
To:	3GPP CN4
Cc:	-

Contact Person:
Name: Günther Horn
Tel. Number: +49 89 636 41494
E-mail Address: guenther.horn@siemens.com

Attachments: none

SA3 thanks CN4 for their LS. CN4 had the following actions on SA3:

CN4 asked SA3 to consider

a) the synchronisation problem of authentication vectors described in CN4's LS
b) security requirements of inter domain usage of Cx protocol,

and give guidance to CN4.

SA3 would like to respond to CN4's questions as follows:

a) SA3 is aware of the synchronisation problem of authentication vectors and has agreed to address the problem in the framework of a generic authentication architecture for Release 6. Work will be progressed on this issue at the SA3 ad hoc meeting in September. SA3 will keep CN4 informed of the progress of this work.
b) SA3 does not currently envisage an inter domain usage of the Cx protocol, or Cx-like protocols.

Action on CN4:
none

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Portugal
SA3#31	18 – 21 November 2003	London

3GPP TSG SA WG3 Security — S3#29 **S3-030474**
15 – 18 July 2003
San Francisco, USA

Title: **LS on 'Effects of service 27/38 on 2G/3G Interworking and emergency call'.**
Source: 3GPP SA3
To: 3GPP T3, CN1
Cc: **-**

Contact Person:
Name: Marc Blommaert
Tel. Number: +32 14 25 3411
E-mail Address: Marc.blommaert@siemens.com

Attachments: S3-030402, S3-030465

SA3#29 have approved S3-030465: 'Clarification on the usage of the c3 conversion function'. A part of the clarification now reads: 'An ME with a USIM that does not support GSM cipher key derivation (Feature 1) …. cannot operate in any GSM BSS ***with 64-bit key ciphering enabled***'. The input document S3-030402 to the same meeting detailed many scenarios where the outcome of a call setup or 2G/3G interworking was dependent on the activation of ciphering in the BSS.

SA3 found it useful to document these scenarios and thought that T3 specification TR31.900 would be the adequate place.

Actions:

To T3:
- To check if TR 31.900 is in accordance with the CR approved by S3 (S3-030465) and adapt if not.
- To consider the incorporation of the scenarios from S3-030402 section 2 into TR 31.900.

To CN1:
- To check the scenarios from S3-030402 section 2 on completeness and correctness.
- To check if TS 24.008 is in accordance with the CR approved by S3 (S3-030465) and adapt if not.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

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.

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 5.2.0 ⌘

*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:	⌘	Clarification on the usage of the c3 conversion function
Source:	⌘	Siemens, Nokia, T-Mobile
Work item code:	⌘	Security ***Date:*** ⌘ 08/07/2003
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:

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:	⌘	- The support of the USIM Service n° 27: called "GSM Access" is optional. With this service the USIM generates the 2G ciphering key Kc required by the 2G air interface. The Kc is derived from the CK and IK with the conversion function c3. The c3 algorithm is described in section 6.8.1.2 of TS 33.102. The function c3 may only be performed in the network and the USIM. If an operator decides to issue USIMs without USIM Service n° 27 it is the intention of the operator that *64-bit 2G ciphering* shall not be possible. Thus c3 shall not be performed in the ME if the USIM Service n° 27 is not available. This essential mandatory requirement for the ME is not explicitly stated in TS 33.102. - Erroneous sentence on the lack of c3 function on the USIM, specifying that the ME cannot operate under any BSS. - The last sentence in 6.8.1.5 has been corrected.
Summary of change:	⌘	- It is clarified that the conversion function c3 shall not be performed in the ME. - It is clarified that with the lack of c3 function on the USIM, the ME cannot operate under BSS with *ciphering enabled.* - Split of the last sentence of 6.8.1.5 to correct the logic of the sentence.
Consequences if not approved:	⌘	Risk of erroneous ME implementations which are performing the c3 in the ME, completely bypassing the operator's intentions to forbid 64-bit 2G ciphering.

Clauses affected:	⌘	6.8.1.5			
Other specs affected:	⌘	**Y** / **N**		⌘	TR 31.900
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

***** Begin of Change ****

6.8.1.5 USIM

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.

When the ME provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM shall store CK and IK as current security context data. If the USIM supports access to GSM cipher key derivation (feature 1), the USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the R99+ ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the R99+ ME.

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. The USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then stores the GSM cipher key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the R99+ ME shall be informed. An ME with a~~A~~ USIM that does not support GSM cipher key derivation (Feature 1) shall not perform the GSM cipher key derivation (conversion function c3) in the ME and therefore cannot operate in any GSM BSS with 64-bit key ciphering enabled. An ME with a~~A~~ USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN. ~~-~~A USIM that does not support GSM AKA (Feature 2) cannot work within ~~or in a both~~ a ~~R99+~~ ME that is not capable of UMTS AKA ~~-~~and cannot work within a~~in~~ R98- ME.

**** end of change ****

3GPP TSG SA WG3 Security — S3#29 **S3-030475**
15 - 18 July 2003
San Francisco, USA

Title: **Reply to LS on** the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes

Response to: **S2-032746 (S3-030433)**

Release: **Rel-6**

Source: **SA3**

To: **SA2**

CC: IREG, IREG Packet Group, GSMA WLAN Task Force, GSMA Security Group

Contact Person:

Name: Sébastien Nguyen Ngoc
Tel. Number: +33 145 29 47 31
E-mail Address: sebastien.nguyenngoc@francetelecom.com

Attachments: **None**

Overall Description:

SA3 thanks SA2 for their LS on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes.

SA3 believes that hiding the IP address of the PDG on GRX using NAT or other techniques would not be useful from a security point of view. There are potential threats on the PDG, and those should be addressed so that the PDG is secured against attacks. No issues were raised in SA3 with the suggestion in SA2's liaison that a PDG address on GRX could be made visible and accessible to specific authorised UEs.

However, SA3 does not envision that NAT is a useful mechanism to meet these threats. Furthermore, NAT would add additional complexity to the system and is known to introduce incompatibilities with common tunnelling protocols like IPSec. Therefore SA3 does not recommend the use of NAT on the IP address of the PDG.

Actions:

To SA2:

SA2 is kindly asked to take above conclusion into their architectural discussions.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

3GPP TSG SA WG3 Security — S3#29 **S3-030476**
15 - 18 July 2003
San Francisco, USA

Title: Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking

Work Items: WLAN Interworking

Source: 3GPP SA3
To: 3GPP SA2
Cc:

Contact Person:
Name: Colin Blanchard
Tel. Number: +44 1473 605353
E-mail Address: colin.blanchard@bt.com

Attachments: none

SA3 thanks SA2 for their LS on Address discovery using public DNS for WLAN interworking. SA2 had asked SA3 to answer the following questions

- Is allowing IP address of the WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

- Is allowing IP address of the PDG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

SA3 would like to respond as follows:

It was not clear to SA3 about what is meant by "public DNS" and in fact the following elements need to be considered separately:

1. **DNS Client**: The UE DNS Client's resolver will use a recursive name server for its queries. The Client can get the IP address for the recursive name server via static configuration or DHCP. The DHCP occurs after authentication to the WLAN and could be configured to provide the recursive name servers to use for WLAN/3G interworking. This would require the WLAN operator to configure the DHCP to support this.

2. **Recursive Name Servers:** The Recursive Name Server answers recursive queries from the UE's on the WLAN. It performs the necessary non-recursive queries to other name servers to get the correct Resource Records. The WLAN operator or 3G operator could operate the Recursive Name Servers. These DNS servers could probably be configured to answer queries for host names on the Internet and for

host names on the PLMN. These DNS servers would have to be secured of course. **SA3 have assumed that a "public" Recursive Name Server might be considered one that can resolve names on the Internet (i.e., uses Internet DNS for resolving names) and allows all authenticated WLAN clients to use it. The Recursive Name Server should be configured so that only users on the WLAN can query it (not accessible from the Internet) and should be controlled by the operators according to the roaming agreement.**

3. **Delegated Name Servers**: These DNS servers hold the Resource Records (e.g., A records) for the WAG and/or PDG. **SA3 have assumed that these will be managed and controlled by the operators of the WAG or PDG. SA3 weren't sure whether "public" DNS referred to name servers that are accessible to queries from the Internet or perhaps sit on the Internet DNS tree?** However, it is not clear to SA3 what DNS tree will the WAG & PDG names be placed in, Internet or an alternate. For example, would it use an ICANN-assigned TLD or a special TLD (e.g.,. gprs).

On the specific question asked by SA2 on "Is allowing IP address of the PDG/WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking" SA3 would like to make the following comments:

1. If the Internet DNS is to be used, then the Recursive Name Servers have to have access to the Internet in order to query the root servers and TLD servers. It is not necessary that the Recursive Name Servers be reachable from the Internet other than to receive replies to its queries (e.g., it should not answer queries from the Internet). The Delegated Name Servers need to be reachable from the Recursive Name Servers, but it is not then necessary that they are reachable from the Internet

2. Addresses used in the GRX should not be re-used on the Internet. However, this possibility should be considered. The Delegated Name Servers should be sure to resolve to the correct PDG addresses.

3. If DNS servers are used for determining IP addresses of WAG or PDG for tunnel establishment purposes, SA3 does not see any issues in satisfying the 3GPP security requirements, as the security threats against the DNS servers can be mitigated using existing mechanisms, as is already is the case with many current DNS server deployments. It is also recognized that more can be done to secure the DNS, such as deployment of TSIG and/or relevant aspects of DNSSEC

4. As well as protecting the DNS servers themselves, the communication between the UE and the DNS server has to be secure from modification by an attacker e.g. through the use of 802.11 security on the air interface and network security between the AP and the DNS server.

Finally, it should be noted that as an alternative it might be possible to deliver the IP address of the PDG or WAG to the UE using EAP-AKA authentication instead of using DNS. However, it is recognised that it is far from trivial to pass additional information in EAP and at the moment, SA3 see no way to provide such information in EAP-SIM or EAP-AKA. If EAP-SIM/AKA were extended to carry the Home PDG address, then this would work in any environment in which EAP-SIM or EAP-AKA would work. It should be noted that this will not hide the IP address of the tunnel endpoint, it will only make its discovery inconvenient.

Conclusion

Based on the assumptions and mechanisms described above, SA3 believes the DNS could be used for discovery of either WAG or PDG addresses by the UE.

Action on SA2:

To comment on the assumptions highlighted in bold above

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp
SA3#30	6 – 10 October 2003	Porto
SA3#31	18 – 21 November 2003	London

3GPP TSG SA WG3 Security — S3#29 **S3-030477**
15 - 18 July 2003
San Francisco, USA

Title: **Reply to LS on DoS attacks against the 3GPP WLAN Interworking system**
Response to: **S2-032730 (S3-030428)**
Release: **Rel-6**

Source: **SA3**
To: **SA2**
CC : **-**

Contact Person:
Name: Anand Palanigounder
Tel. Number: +1-972-684-4772
E-mail Address: anand@nortelnetworks.com

Attachments: **None**

Overall Description:

SA3 thanks SA2 for their LS on Denial of Service attacks against the 3GPP WLAN Interworking system. SA3 reviewed the conclusions reached in the attached paper titled "Security analysis for tunnel establishment" (S2-032483) and concluded the following:

SA3 agrees with the conclusion reached in the document except that, in case there is no WAG in the VPLMN or traffic routed through it, PDGW will be the one being affected by the Denial of Service attack.

Two ways of facing the attack have been identified by SA3. Both have similar results, although different architectural implications SA2 can take into consideration:

- Firewall policies in the WAG will protect the attack in the boundaries of the GRX. In this case, suitable WAGs are needed, which are able to absorb the attack. This option has the advantage of stopping the attack in the boundaries of the backbone network, but it requires support in the VPLMN (the WAG). This option applies equally to the tunnel-switching and end-to-end tunneling approaches – in either case measures at the WAG are needed in order to block the DoS attack at the boundary of the GRX network.
- If the HPLMN does not want to rely on the fact that traffic from the WLAN AN to the PDGW is always routed through a WAG, or that the WAG performs some of the needed firewall functionality, then the PDGW may need firewall functionality (either in the same node or outside) to enforce the policies. In the same way, PDGWs which are able to absorb the attack will be required. This option has the advantage of not requiring any support in the VPLMN (for roaming cases). However, the attack has to be detected and absorbed in the PDGW of the HPLMN of the user.

SA3 also would like to point out that IP address spoofing is also possible with both end-to-end tunneling and switched tunneling approaches. In order to mitigate the DoS attacks due to address spoofing, once the attack is identified, cooperation in tracking down and terminating the attacks is needed from the operators involved (e.g., HPLMN, VPLMN, WLAN etc.). SA3 further notes that, once the DoS attack is identified, it may be easier to track down the attacker(s) at the WAG than at the PDGW. However, it is not necessarily any easier to identify such attacks on WAG as opposed to the attacks on the PDGW.

Actions:

To SA2:

SA2 is kindly asked to take above conclusions from SA3 in their architectural discussions.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

3GPP TSG-SA3#29 **Tdoc ⌘S3-030478**

15th – 18th July, 2003 San Francisco, USA

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.102** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.2.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	IMEISV retrieval before completion of security mode setup procedure
Source:	⌘	SA WG3
Work item code:	⌘	LATE_UE
Date:	⌘	27/08/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

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:	⌘	The Serving Network needs to be able to retrieve the IMEISV before ciphering is started to be able to handle faulty ciphering behavior of not fully ciphering tested early UE's. TS 33.102 currently forbid the retrieval of IMEISV before completion of security mode set-up procedure. Such a restriction has not been implemented within Stage-3 specification (i.e. TS 24.008).
Summary of change:	⌘	Remove the restriction to retrieve IMEISV before security mode setup procedure has been completed.
Consequences if not approved:	⌘	The Serving Network will not be able to recognise and handle Early UE with faulty ciphering behavior when ciphering is activated.

Clauses affected:	⌘	6.4.5; 5.1.5

		Y	N		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	

Other comments:	⌘	

***** Start of change *****

5.1.5 Mobile equipment identification

~~In certain cases,~~The SN may request the MS to send it the ~~mobile equipment identity~~ IMEI or IMEISV of the terminal. ~~The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls.~~ The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI or IMEISV may~~is not~~ be unprotected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

***** End of change *****

***** Start of change *****

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI, ~~and~~IMEI or IMEISV), and
- Authentication and key agreement.

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

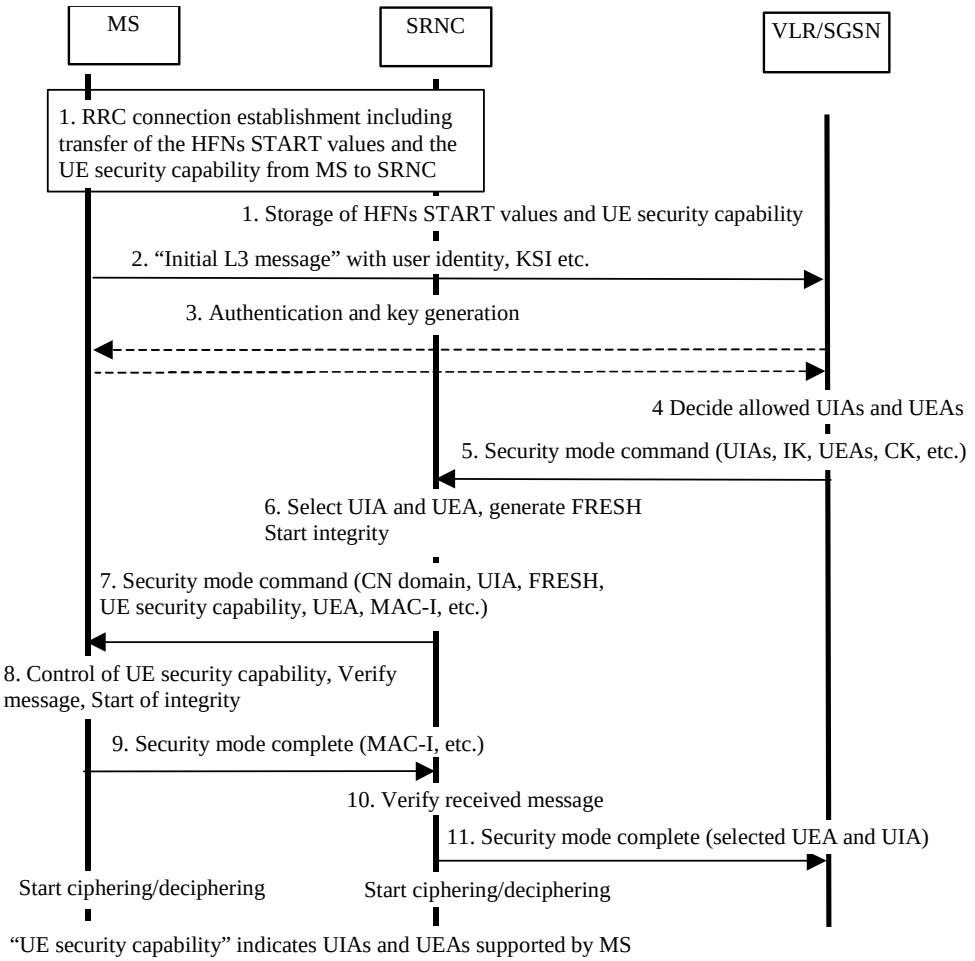

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

***** End of change *****

CR-Form-v7

CHANGE REQUEST

⌘ TS 33.102 CR 182 ⌘rev - ⌘ Current version: 5.2.0 ⌘

*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:	⌘	Mitigation against a man-in-the-middle attack associated with early UE handling
Source:	⌘	SA WG3
Work item code:	⌘	LATE_UE
Date:	⌘	19/09/2003
Category:	⌘	C
Release:	⌘	Rel-5

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:	⌘	If an unprotected IMEISV is used to establish security without ciphering (i.e. with UEA0) for UEs which have faulty UEA1 implementations then a man-in-the-middle attack is possible. A mechanism to mitigate against this attack needs to be specified.
Summary of change:	⌘	Add a mechanism to mitigate against a man-in-the-middle attack associated with early UE handling.
Consequences if not approved:	⌘	A man-in-the-middle attacker would be able to disable ciphering for UEs which are capable of ciphering.

Clauses affected:	⌘	2, 6.4.5			
Other specs affected:	⌘	Y: Other core specifications	⌘	24.008, 25.413	
		N: Test specifications			
		N: O&M Specifications			
Other comments:	⌘				

***** Start of change *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[22] 3GPP TS 23.195 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".

***** End of change *****

***** Start of change *****

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement.

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

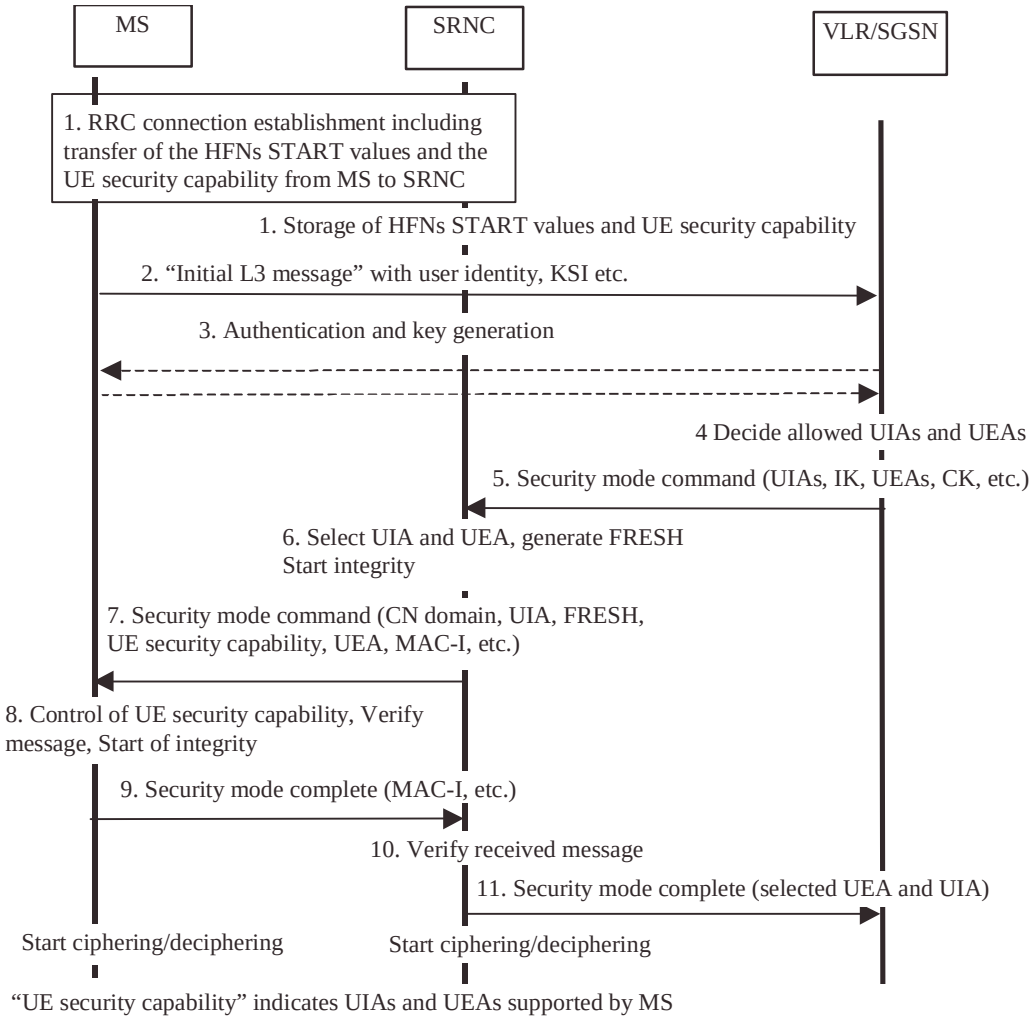

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

Mechanisms are defined to allow networks to overcome early UE implementation faults [22]. A potential early UE implementation fault could be a faulty UEA1 implementation. To allow networks to handle early UEs which have faulty UEA1 implementations, the SGSN/VLR may configure the security mode command based on the UE's IMEISV so that certain UEs which claim to support UEA1 shall have security established without ciphering (i.e. with UEA0), while other UEs which claim to support UEA1 shall have security established with ciphering (i.e. with UEA1). This procedure shall involve the SGSN/VLR retrieving the IMEISV from the UE before the security mode set-up procedure has started.

If the above procedure to handle UEs which have faulty UEA1 implementations is implemented and the security mode set-up procedure results in security being established without ciphering (i.e. with UEA0) then the SGSN/VLR shall request the IMEISV from the UE for a second time immediately after the security mode set-up procedure has been completed. This second IMEISV request is integrity protected. If the IMEISV request is not successful, or if the second IMEISV received is different from the IMEISV received before the security mode set-up procedure was started then the connection shall be released.

***** End of change *****