3GPP TSG SA WG3 Security#30 **S3-030584**
6 – 10 October, 2003
Povoa de Varzim, Portugal

Agenda Item: 7.6

Source: Siemens

Title: Evaluation of secure algorithm negotiation proposals

Document for: Discussion/Decision

1. Introduction

In [S3-030361] Ericsson proposed an approach for secure algorithm negotiation for the Gb-interface. The most critical point within the concept of secure algorithm negotiation is the ability for the terminal to verify that the network could actually execute the new secure algorithms negotiation. [S3-030361] aims to achieve this by using OTA mechanism towards the UICC.

At the same meeting Vodafone [S3-030463] proposed an alternative approach based on RAND modifications, which was not discussed in detail due to the arrival of the document after the submission deadline. The mechanism seemed simpler at first look while no additional algorithms (e.g. HMAC-SHA1) for secure algorithm negotiation need to be introduced within the SGSN & MSC/VLR and the UE.

This document analyses the aforementioned proposals (section 3 and 4). Before the evaluation is started the requirements agreed at previous SA3 meetings are repeated (section 2).

2. Requirements

SA3 did agree at SA3#28 Berlin that a secure algorithm negotiation mechanism shall meet following requirements (See Report S3-030311- *italic text*): "

- *The signalling flow should be kept intact. i.e. it should be a three-way handshake;*
- *Both the SGSN and UE should be able to verify that secure negotiation was possible to use;*
- *The solution should allow the use of legacy UEs and SGSNs."*

SA3 did also take the working assumptions that '*that increased key-length will only be possible with the use of the USIM. The use of SIM for secure negotiation should be subject to future contribution.*'

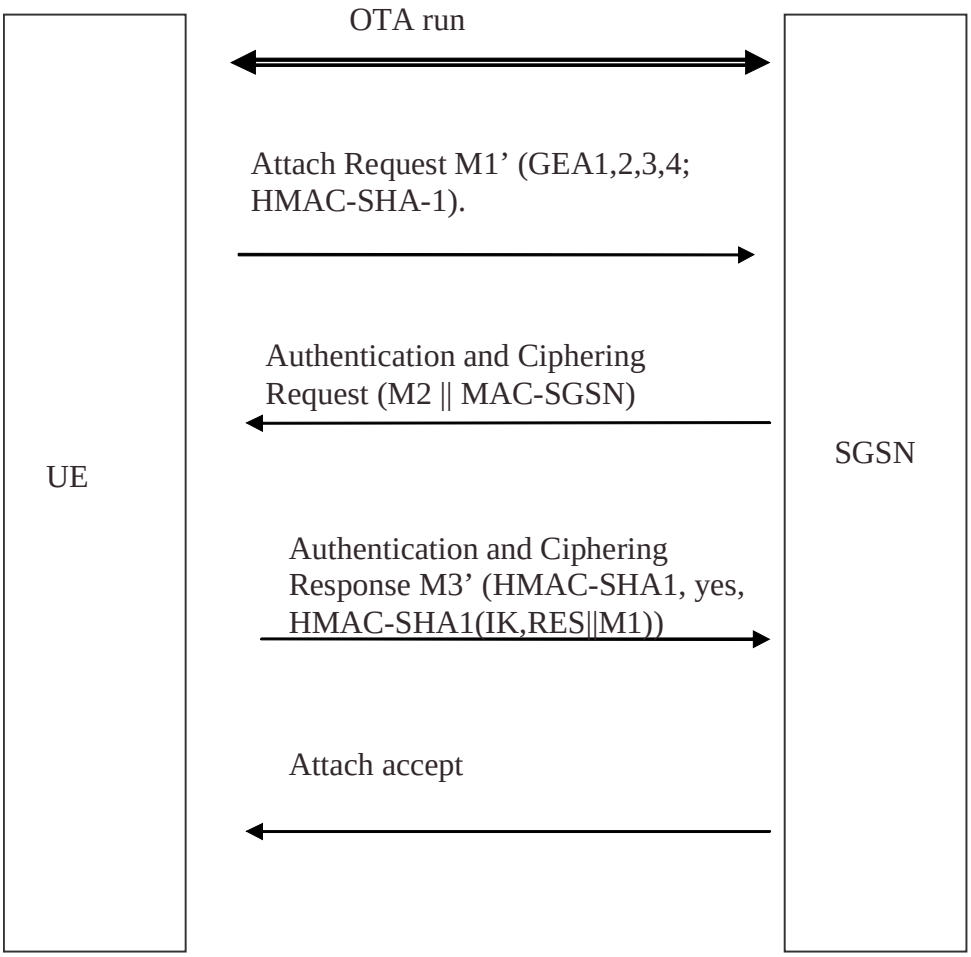
The above means that the GEA4 algorithm shall only be selected by the terminal if UMTS AKA is being executed at the same time. Each Rel5+ terminal shall be able to support UMTS AKA. An explicit requirement for the terminal to verify this then needs to be included in the specifications.

At SA3#29 in San Francisco and at later discussions it became clear that a solution for secure algorithm negotiation is desirable for use with SIMs too, to be able to counteract the man-in-the-middle threat negotiating down the used algorithm to A5/2. Therefore SA3 should add the requirement that a secure algorithm negotiation protocol should apply for both SIM and UICC.

3. Evaluation of Ericsson's secure negotation protocol [S3-030361]

The proposal made by Ericsson at SA3#29 proposes to modify the three way authentication handshake to include secure algorithm negotiation. In addition an OTA run may be needed in advance of the authentication run to securely communicate serving network settings (i.e. the indication of the support of secure algorithm negotiation by the network) to the UE.

The flow according to [S3-030361]:



Whereby M1, M2 and M3 are the messages as known from current specifications (See TS 24.008). The three way handshake is kept but the message content (M1',M2',M3') is changed and additional algorithm support is required at both terminal and SGSN.

Eval-1. The requirements from S3-030311 shall be fulfilled.

The requirement 'should allow the use of legacy UEs and SGSN' can be interpreted in different ways. Anyhow a modification to UE and SGSN are needed to introduce secure negotiation, therefore the requirement should be interpreted more as 'interworking with legacy UEs and SGSN shall be supported'. This translated requirement is fulfilled together with the other two. However the approach is vulnerable to a man in the middle attack (As highlighted by [S3-030463]), where the attacker masquerades as a network that does not support secure algorithm negotiation. The user is not likely to notice if an unexpected visited network identity appears briefly on his screen and it is unlikely that the user is aware of all acceptable VN network identities. The proposed solution is therefore not a secure one unless additional mechanisms are introduced to ensure VN-identity authenticity. This is a big disadvantage of this proposal.

Eval-2. Complexity in case of heterogeneous implemented ciphering settings at different VLR/SGSNs.

It is judged impractical to perform updates towards the UICC for each SGSN/VLR separately. This also will require a large list of identities and settings that need to be managed at the UICC.

Eval-3. Complexity in case of homogeneous implemented ciphering settings in networks.

It is judged that it is not feasible for the home network to inform the USIM via OTA of the visited network's capabilities whenever the mobile roams onto a new visited network (As highlighted by [S3-030463]). The list of identities that need to be managed at the UICC is reduced by taking the homogenous approach. Updating the settings just before the Authentication towards a foreign network should be avoided as it delays call set up.

Eval-4. Impacts imposed by adopting the proposed solution

The impacts are isolated at SGSN and UE's, No changes to the AuC are required.

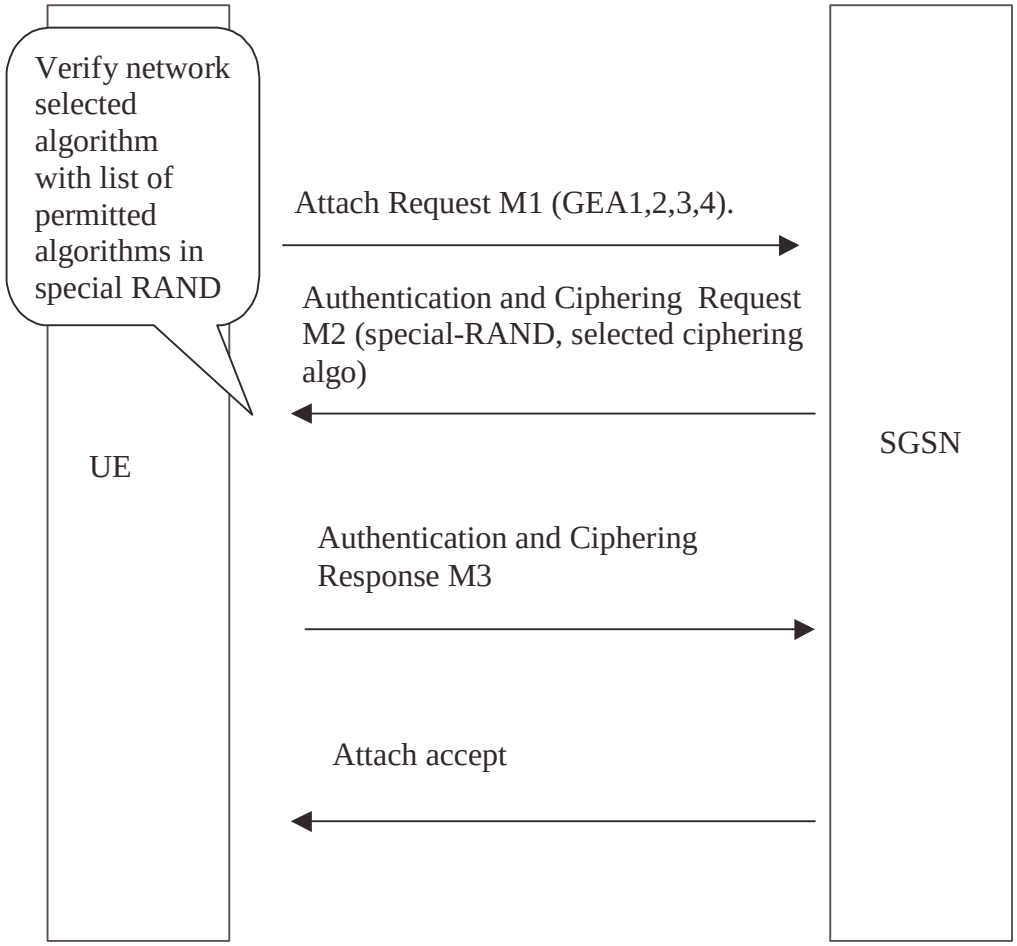
A procedure is needed towards the UICC to check if the VN-identity is within the list of networks that support secure negotiation. As listed in Eval-1, the UE does currently not have an authenticated VN-identity available.

Eval-5. Scope of applicability

An SA3 working assumption was that for use with GEA4 only a USIM shall be supported. However it seems logical to use the secure negotiation method also together with A5/3 and GEA3 to prevent a man-in-the middle downgrading the ciphering algorithm to the weakest one (i.e A5/2). A5/3 and GEA3 both have 64-bit ciphering and using it shall be possible both with a SIM and a USIM. The presented secure negotiation method in this section require new fields on the UICC. But as the SIM specification is frozen from Rel-5 on, it is not possible to introduce new fields on SIM for storing the VN identities that support secure negotiation.

4. Evaluation of special-RAND proposal [S3-030463]

The adoption of the proposal to reserve a certain number of bits in the RAND (called special-RANDs) to transport the network permitted ciphering algorithms to the UE can result in an unmodified three way handshake (i.e. The message M1,M2 and M3 would be kept unchanged). The secure algorithm negotiation would not exist as an explicit procedure but enforcement of secure algorithm negotiation would become part of the UE tasks. If a network supports 'secure algorithm negotiation' it will generate special-RANDs. If the UE supports the special-RANDs then it will be able to recognise the special RAND and extract the permitted network algorithms-list from the special-RAND and compare it with the selected ciphering algorithm from the Authentication and ciphering request message. If the network did not select an algorithm permitted according to the special-RAND then the UE shall answer with a Authentication and Ciphering failure message. It is Siemens understanding that the Special-RAND mechanism shall be transparent for the BSS. The figure illustrates the unmodified flow.



Eval-1. The requirements from S3-030311 shall be fulfilled.

The requirements are fulfilled.

Any attempt of an attacker to change one of the (cleartext) RAND-bits will result in a failed authentication.

A side effect is that keeping a number of bits fixed in the RAND reduces the randomness of the RAND. The effective RAND length in [S3-030463] is reduced from 128-bits to about 80-bits. 2^{80} is still considered as a large enough key-space for the key Kc/CK as a reuse of same RAND will not happen that frequent. *Unnecessary (further) reduction of the RAND randomness should be avoided i.e. the required number of bits for the bit mapping of the capabilities to the RAND shall be minimized!* **It is proposed that SAGE confirms that the reduction to 80-bit randomness does not have any consequences.**

Eval-2. Complexity in case of heterogeneous implemented ciphering settings at different VLR/SGSN.

This situation can only be handled by requiring adaptation to AV-requesting procedures to include the requesting-node identity (or the inclusion of the supported Algo-id of the requesting node). The introduction of these changes into the core network will take a long time to be in place in all networks. Another consequence is that the use of AV-precalculations on the AuC will become inefficient. This will also have an influence on the call setup due to the added authentication delay.

Eval-3. Complexity in case of homogeneous implemented ciphering settings in networks.

To avoid the above disadvantages in Eval-2, the HN operator should actively take care that all the equipment in their networks supports the same algorithms. The AuC will then need to be able to distinguish between request coming from the HN and coming from different VN. This may be done by including a VN-identity within the AV-request (or a list of supported algo-Ids). The AuC will still be able to precalculate AVs in most cases as most users stay in the HN. The AuC could produce special-RAND for users roaming in anothers operator network if that network supports an homogenous implementation of ciphering, and has introduced the VN-identity within the AV-request.

Eval-4. Impacts imposed by adopting the proposed solution.

This impacts the AuC and AV-requesting procedures (affects SGSN/VLR). There are no impacts on the air-interface.

A consequence of producing RANDs per VN-identity or Node-id is that AV cannot be forwarded anymore between the Networks/nodes. The AuC will also need to distinguish between a RAND request for the A and the Gb-mode to be able to set other RAND bits (Key separation).

It is assumed that for Iu-mode access the secure negotiation based on Special-RAND is not needed as the Iu-mode access has a build-in algorithms negotiation protection mechanism. The mechanism for Iu-mode access is secure as long as none of the integrity algorithms can be broken in real time. If the special-RANDs are not to be used for Iu-mode access then the requesting-node shall be able to indicate this to the AuC. Whereas currently an SGSN providing Iu-mode and Gb-mode can use the same AV on both access modes this will not be the case anymore. But using the Special-RAND over Iu-mode access would not harm.

Eval-5. Scope of applicability.

This solution is also usable in case SIMs are used as it does not require an changes to it. The interpretation of the special RAND is to be done by the Rel-6 UE. It also is possible to apply this to A53 and GEA3 Rel-6 terminals, however the effects of this to the GSMA requested introduction date of October 2004 for A53 and GEA3 mobiles shall be clarified.

5. Conclusions

From the two proposals that were available at SA3#29, the special-RAND mechanism is the only mechanism that provides guaranteed secure algorithm negotiation. However it also requires changes to AV-requesting procedures which will affect the core nodes MSC/VLR, HLR/AuC and SGSN. Also the AV-generation function in the HLR/AuC will be affected.

In order to limit the effects on the core nodes, Siemens proposes to agree following working assumption for the further analysis of the Special-RAND mechanism:

- The permitted algorithm settings should be maintained and kept **homogenous** per operators network
    - in order to keep open the possibility for pre-calculation of AV's at the AuC.
    - as the network 'forgets' the RAND after it has been used. [E.g. during Location Update (VLR->VLR) and inter-SGSN routing area update (SGSN->SGSN), only the current ciphering key and CKSN are provided to the new network node. I.e. the new network node does not know what has been indicated as permitted algorithms to the MS.]

Following items need further clarification:

- The use of the special-AV for UMTS network access shall be clarified.
- The relationship of the special-RAND with new A5/3 & GEA3 mobiles need clarification. Manufactures have been requested by GSMA to have products ready by October 2004. The introduction of the Special-RAND feature as part of Rel-6 (which is expected to be stable in March 2003) could jeopardise that date.
- The triggerpoint for (re-)authentication in the network should match the validity criteria of the RAND-information. If that is not possible it could create undesired effects on calls. (See network forgets the RAND).

It is also proposed that SAGE confirms that the reduction to 80-bit randomness does not have any consequences.

It seems also prudent to involve CN1 and CN4 to further analyse this proposal in parallel in order to speed up the specification of a solution.

The proposal from [S3-030361] should not be pursued anymore as it is insecure and provides several operational disadvantages.

6. References

[S3-030361] Ericsson: Enhanced Security for A/Gb, S3#29, 15 – 18 July 2003, San Francisco, USA

[S3-030463] Vodafone: Cipher key separation for A/Gb security enhancements, S3#29, 15 – 18 July 2003, San Francisco, USA