3GPP TSG SA WG3 Security **S3-030244**

6 – 9 May 2003

Berlin, Germany

Agenda Item: TBD

Source: Ericsson

Title: Enhanced Security for A/Gb

Document for: Discussion/Decision

1. Scope

This contribution discusses different ways to enhance the security for GERAN. At SA3#27 a priority list was presented in [S3-030113] on which this contribution is based upon. The main focus in this contribution is on GPRS and the discussion on increasing the key length from 64 bit such that a 128 bit key could be supported. It is proposed that as a working assumption:

1. 128 bit key should be possible and coupled to the USIM to reduce the number of options
2. Secure negotiation can be introduced by repeating and protecting the proposed algorithms from the terminal

The proposed solutions consider legacy SGSNs and terminals. Since there will be impact on Stage 3 specifications and potentially the USIM the appropriate 3GPP TSGs should be given actions to study the implications and provide SA3 with feedback.

2. Potential solutions

SA3 has agreed on a WID, cf. [S3-030109], for enhancing the security for the A and Gb interfaces. In GERAN there have also been new work items defined that aim to introduce four different bearer types over the PS-domain: conversational, streaming, interactive and background. This paper then starts from this and discusses potential security enhancements in the PS-domain considering the activities in GERAN. It should be noted that for this discussion the A interface has not been covered in this document although there might be factors pushing for an increase of the level of the security for the circuit switched services.

2.1 Increase the security over the Gb i/f

As discussed in earlier papers in SA3 like [S3-030161] on allowing SIM-based access to IMS the security level with a SIM card is lower than USIM. It therefore seems that it should be suitable to assume that whenever the security level over Gb should increase the logical step is to tie this with a change from a SIM to a USIM. This should also be understandable for the consumers since a shift of cards to a 3G card is a convincing argument that security will be increased. Technically it would also be a simpler way forward considering already the number of different options defined in [33.102]. Furthermore to increase the key length from 64 bits to 128 bits for all different options as defined in [33.102] would have an impact on the communication between HLR and SGSN as well as in the terminal and so forth i.e. it seems unnecessary to introduce too many options and increased complexity. If we instead restrict the work on assuming that an increase in security level is tied to the USIM and a Release 99+ SGSN and HLR/AuC a Quintet will be transported to the SGSN, cf. Figure 2 below, the complexity and the number of options is significantly reduced. The SGSN would for this case have key material available that have enough entropy for providing 128 bits effective key length for encryption.

Since enhancing the security for Gb is a Release 6 work item it would mean that the ME could accept CK, IK and Kc from the USIM. The actual key to use should probably be the CK.

The GEA3 algorithm has been designed such that it can support up to 128-bit key however this characteristic is not signalled between the UE and the SGSN in the current specifications. The Technical specification [55.216] specifies the

length of a key as KLEN, which can be 64-128 bits long. The length of the key can be signalled in MS Network Capability (a new field/new algorithm identifier e.g. GEA4 is required), cf. [24.008]. Also the SGSN needs to send the info back i.e. what algorithm and potentially what key length it has chosen in the Authentication and Ciphering Request i.e. a new field is required.

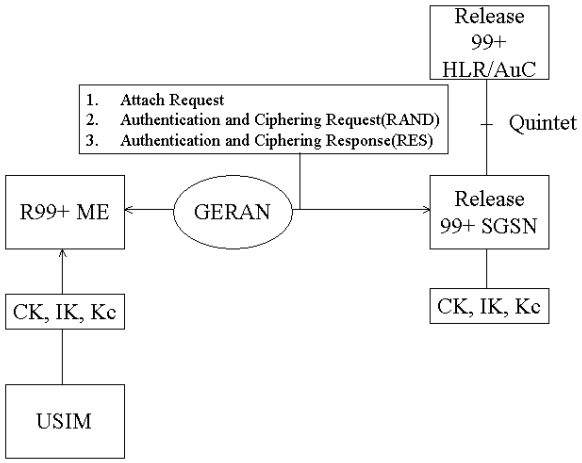

Figure 1 An overview of the signalling between the MS and the SGSN

In the figure below the different options when a USIM is inserted are given:

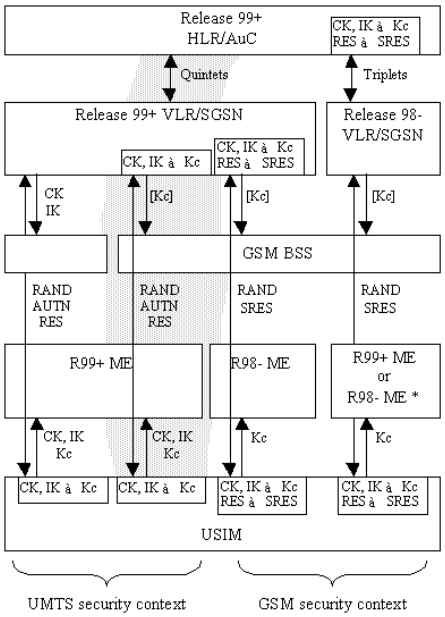

Figure 2 The different options as defined in [33.102]. Note the case when a Quintet is delivered to a Release 99+ SGSN for GSM BSS access and the ME is AKA capable.

2.2 Secure negotiation

One weakness in the existing BSS is that it is easy for a man-in-the-middle to change a proposed algorithm from the UE and hence achieve with a bidding down attack. In the specifications available today the signalling between the negotiation of algorithms between the terminal and the SGSN is done in the following way, cf. also Figure 1 above:

1. The terminal sends an Attach Request towards the SGSN which includes which algorithms the terminal supports
2. Upon receiving this message the SGSN will choose an algorithm and send a challenge towards the terminal in the Authentication and Ciphering Request

Upon receiving the message in 2 the terminal calculates a response and sends it towards the SGSN and the SGSN will check that the response is a valid one

When all these messages have been successfully processed signalling messages (SM and MM) as well as the user plane can now be encrypted with the chosen algorithm.

There are different alternatives at hand to protect the negotiation of algorithms. However apart from security issues that need to be resolved there are also issues around backward compatibility that needs to be looked at. It is assumed that the most suitable way forward is to keep the signalling flow as depicted in the figure above intact rather than introducing new messages due to the legacy reasons.

Apart from legacy requirements it seems suitable to assume that it shall be possible for the SGSN to verify if secure negotiation was used or not. From the UE perspective it could be possible to mandate that the UE e.g. at a stipulated cut off date uses secure negotiation. Another way of accomplishing this is to set a flag in the USIM controlled by the Home Operator stating whether insecure negotiation is allowed or not.

On the solutions side one alternative could be to encrypt message three including the RES and the proposed algorithms utilising a cipher. A suitable MAC of appropriate length to protect the negotiation phase could also be a feasible way forward. These two alternatives are discussed below with the following requirements and assumptions:

i. The signalling flow shall be kept intact i.e. it shall be a three-way handshake

ii. The SGSN should be able to verify that secure negotiation was possible to use

iii. The Home operator can control the use of insecure negotiation by the means of a flag in the USIM

iv. It should work for legacy UEs and SGSNs

Use of a MAC

If a MAC is used the UE and the SGSN should also negotiate the MAC algorithms i.e. in the Attach Request the UE not only indicates the encryption algorithm it supports but also the integrity algorithms. In order to make this work new fields are required. In message three the algorithms proposed by the UE should be repeated but now protected with a MAC. Upon reception of this message the SGSN should check the authenticity of the message and only accept it if the check is successful otherwise the message should be discarded. Since legacy terminals cannot support this feature the SGSN has to accept that message 3 may be unprotected sometimes. In order to facilitate some home control it should be possible for the operator to set a flag in the USIM such that terminal can decide whether insecure negotiation is acceptable or not.

Potential MAC algorithms could be AES in CBC MAC as defined in ISO9797, HMAC SHA1 and Kasumi MAC. Iti left for further study what algorithms that could be used. Hence in message 3 the algorithms proposed by the terminal in message 1 as well as a MAC of e.g. 96-128 bit calculated over appropriate parts of this message. The appropriate key to use for the MAC could be the IK of 128 bits.

A potential way of using a MAC could be as described below.

Let us assume that the terminal supports secure negotiation and the following algorithms:

A. GEA1

B. GEA2

C. GEA3 with 64 bit key

D. GEA3 with 128 bit key

However, a straight-forward protocol will not solve the bidding down issues as seen in the following example. The terminal sends the following algorithms in the first message (were we assume an attacker acts as a man-in-the-middle):

1. Attach Request(***A,B, C,D***, AES MAC, HMAC SHA1) (i.e. Message M= ***A, B, C, D***, AES MAC, HMAC SHA1)
2. The attacker removes algorithm B, C, D, AES MAC and HMAC SHA1 algorithm identifiers from M such that SGSN will receive M'=*A*
3. SGSN then upon receiving this message M' chooses algorithm ***A*** and sends it towards the terminal along with the challenge. Here the SGSN cannot know if the terminal supports secure negotiation or not.
4. The attacker adds a MAC algorithm identifier, e.g. AES MAC, to the message sent by the SGSN. This attack cannot be detected by the terminal
5. The terminal calculates the response RES and the keys IK and CK based on the challenge and chooses algorithm ***A*** as encryption algorithm. The terminal also calculates a MAC using IK and AES MAC protecting the necessary parts i.e. the repeated algorithms
6. The attacker can now remove the MAC tag and all the repeated algorithms towards the SGSN who will not detect the attack.
7. Upon receiving this message the SGSN will just check the RES and assume that algorithm ***A*** has been chosen

This scheme should be modified if the protocol should give secure negotiation between the terminal and the SGSN. The example shows that requirement ii. above could not be satisfied since the attacker was able to bid down i.e. the SGSN cannot know what the policy in the UE mandates. One modification to this scheme would be to add a MAC tag in Step 3, which then would be calculated over IK and message M. An attacker could still remove this part but then again the flag in the USIM should indicate if this message without any MAC algorithm indication nor the MAC itself is acceptable or not. The added value by adding the MAC itself would be that the UE would be certain that if the MAC is present that the SGSN did receive the proposed algorithms in M, this alternative is discussed below. From an SGSN and VN point of view it seems more important to secure Step 5 above from the UE towards the SGSN. In the example the SGSN cannot be certain if the UE is capable of secure negotiation or not and should accept that insecure negotiation could take place.

Assuming that the UE is capable of secure negotiation and that the policy of the Home Operator requires that secure negotiation shall be used the UE could in Step 5 respond in the following way:

5'. AES-MAC(IK, RES, M), where M is the message from step 1, which is sent towards the SGSN. Note: if RES||AES-MAC(IK,M) or RES||AES-MAC(IK,RES,M) is sent the attack described above is feasible

6'. The attacker cannot tamper with this message since a failure in the SGSN would occur

7'. The SGSN upon receiving the message then calculates AES-MAC(IK, XRES, M) and compares this value with what it received from the UE and if it is correct the UE has been authenticated and it can be concluded that also message M was correct. The SGSN can now be certain that the UE was capable of secure negotiation as in Requirement iii.

As already discussed in the work on IMS and the development of RFC3310 3GPP do not have any need to use RES as a password to a conversion function as MD5 or similar. Hence one could argue that this scheme is changing the AKA protocol and it is not clear if 3GPP could accept this for GERAN access or not since AKA is secure as such by sending the RES in clear. The length of the MAC should be at least as long as RES, at least 32 bits but it seems reasonable to assume that in a practical situation it should be at least 96 bits as required for e.g. HMAC-SHA1.

MAC Alternative

There are also other alternative implementations, for instance:

1. Attach Request(***A,B, C,D***, AES MAC, HMAC SHA1) (i.e. Message M= ***A,B, C,D***, AES MAC, HMAC SHA1)
2. SGSN receives message M' (which should be equal to M). If a MAC algorithm identifier was present, it selects e.g. AES_MAC, and responds by: ***A***, RAND, AES_MAC, AES_MAC(IK, ***A***, RAND, AES_MAC, M').
3. UE receives a message from the SGSN. If the message does not indicate a selected MAC, the UE should abort since it is probably under attack. This could be controlled by the operator using a flag in the USIM allowing

for a period that legacy SGSNs do not support secure negotiation. Otherwise, the UE derives RES and IK from RAND. It then verifies the MAC tag using the selected algorithm and the message M it sent in Step 1. If the MAC is not valid, the UE should abort since it is again an indication of attack; either due to the fact that the SGSN received a faked M' in step 1, or, that the response in step 2 was faked. Otherwise, the UE responds by AES_MAC(IK, RES).

4. The SGSN verifies the received message. Note: the scheme above is secure since the SGSN would detect the attack here. This scheme has the advantage that the UE can detect the attack earlier.

This last protocol requires more computation, but has a slight advantage in that a bidding-down attack towards the first message is detected by the UE already in step 3. It also requires some extra overhead (perhaps not significant) since a MAC value has to be added from the SGSN.

Use of a Cipher

By using a block cipher instead of a MAC algorithm the UE would include those instead of the MAC algorithms as discussed above i.e. assuming that the terminal supports AES the terminal could protect message 3 in Figure 1 by encrypting the repeated algorithms as well as the RES.

The terminal sends the following algorithms in the first message:

1. Attach Request(***A,B, C,D***, AES)
2. The SGSN upon receiving this messages picks algorithm ***D*** and AES and sends this back towards the terminal along with the challenge
3. The terminal calculates the RES as well as IK and CK and encrypts the repeated algorithms e.g. utilising IK i.e. Encrypt-with-AES-and-key-IK(RES, ***A,B, C,D***, AES) and adds a flag that the message has been encrypted
4. The SGSN then decrypts the message and checks the RES as well as that the repeated algorithms are the same as in the first message and if this is OK the session will continue otherwise it shall be terminated

It should be possible to add a flag in the USIM such that when the terminal gets the RAND i.e. the challenge without any indication that secure negotiation is used can terminate the session based on the home operator policy, hence forcing a terminal to use secure negotiation. Over the time it is feasible to require that SGSNs support secure negotiation of algorithms. The attack as discussed above would not work. The attacker can no longer tamper with the message since the RES as well as the set of algorithms are encrypted. Hence if the message has been tampered with a failure in the SGSN would occur.

It should be noted that the UE shall signal the cipher IV which will create a need for sending additional bits. Also it is important to consider attacks against the cipher but the AKA protocol would be untouched since the SGSN should check the RES.

3 Conclusions

It should be possible to increase the key length to support any range from 64 bits to 128 bits long keys. The easiest way forward is to assume that only the use of USIMs can be granted the increased security level over BSS accesses including the use of a Release 99+ version of the HLR/AuC, the SGSN and the ME, cf. the shaded area in Figure 2. It is assumed that the terminal could indicate in a new field that it supports a key length of e.g. 128 bits or that a new algorithm GEA4 is defined. The key could be the CK derived from the AKA procedures.

By mandating that a terminal that supports enhanced security for Gb to protect message 3 with a cipher e.g. AES an increased security for agreeing on the strongest algorithm in common is facilitated. A flag should be added in the USIM indicating if the terminal should accept that the SGSN is using insecure negotiation should be included.

Considering that all schemes for secure negotiation discussed in this paper should increase the security level Ericsson gives some slight preference for the ciphering alternative, as it would not change the AKA protocol. However the final decision should be based on the preference from SA3 considering feedback from other 3GPP groups.

Ericsson proposes that the principles discussed in this document are agreed as working assumption for increasing the security for Gb. Ericsson also recommends that the relevant 3GPP groups are informed about the different alternatives and be given an action to give feedback on protocol impacts.

4. References

[S3-030109] TSG SA3 WID: GERAN A/Gb mode security enhancements3GPP, S3#27, 25 - 28 February, Sophia Antipolis, France.

[S3-030113] Vodafone GERAN A/Gb mode security enhancements, 3GPP, S3#27, 25 - 28 February, Sophia Antipolis, France.

[S3-030161] TSG SA3 LS on: “Requirement to allow IMS access by means of SIM”, 3GPP, S3#27, 25 - 28 February, Sophia Antipolis, France.

[33.102] 3GPP TS 33.102, Technical Specification Group Services and System Aspects; Security; Security architecture (Release 5), version 5.1.0.

[55.216] 3GPP TS 55.316 Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS Document 1: A5/3 and GEA3 Specifications (Release 6) version 6.1.0

[24.008] 3GPP TS 24.008 Technical Specification Group Core Network Mobile radio interface Layer 3 specification Core network protocols; Stage 3 (Release 5)