3GPP TSG SA WG3 Security **S3-030361**

15 – 18 July 2003

San Francisco, USA

Agenda Item: 7.5

Source: Ericsson

Title: Enhanced Security for A/Gb

Document for: Discussion/Decision

1. Scope

Ericsson has the understanding that in order to create secure negotiation for the Gb scenario a secure channel is required in order to alleviate a bidding down attack. Such a secure channel could be achieved through the use of the security mechanism defined for (U)SIM application toolkit. This channel could then in a secure manner send information to the USIM the capability of an SGSN as well as the policy of the home operator by setting a flag of at least two bits. To what granularity this can be done i.e. if it is possible to make it per roaming partner should be studied by T3. Hence Ericsson proposes that T3 studies the feasibility of creating a file in the USIM and the feasibility to set such a flag per roaming partner.

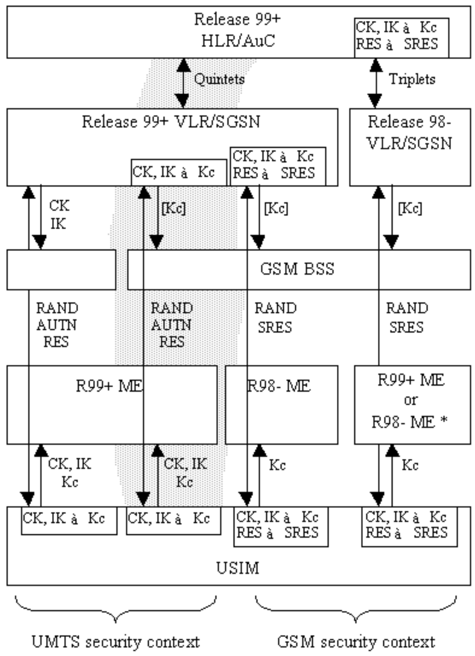
Ericsson also suggests that CN1 studies the feasibility of adding new fields in the communication between the terminal and the SGSN as well as if there are any other impacts in the system that SA3 should be aware of should the by Ericsson proposed scheme be accepted by 3GPP.This paper assuming the working assumptions as agreed at SA3#28 that the increased key length should only be possible with a USIM.

Before 3GPP decides that the approach proposed by Ericsson here is acceptable 3GPP has to study the feasibility from a technical perspective as suggested above. However Ericsson would want that also SA1 study the impact from a service requirement point of view and asks SA1 on their views on the proposal.

2. Background

In [S3-030244] Ericsson discussed increasing the key length for protection over the Gb interface as well as some alternatives on how secure negotiation could be achieved for the Gb interface in order to evolve the work based on the WID as agreed per SA3#27 in [S3-030109].

On the key length issue SA3 sent an LS from SA3#28 to CN1 in [S3-030308] on the use of GEA4 code point for the GEA3 with 128 bit key support. It was concluded by CN1 that this is a feasible way forward in their reply LS in [N1-030820]. Ericsson proposed that the increase of key length should be tied to the USIM and certain releases of the network as indicated in the shaded are in the figure below:



Some reasons for this approach are:

1. It is a clear step for the consumer i.e. shifting the card to a 3G card means increased security

2. It will reduce the number of options in the specifications

3. It will have minimal impact on the system and the network nodes

4. There is a general trend that whenever the operator would require higher security a shift from a SIM to USIM is the suitable way forward cf. the discussions on WLAN and EAP SIM vs. EAP AKA

5. For IMS as a Release 5 work item only USIM and ISIM based access is allowed and not SIM

If the key length is increased the security level is definitely higher. However it was also noted in [S3-030244] that the negotiation of algorithms is easy to attack and hence it seems suitable to consider a secure negotiation scheme should GEA4 and 128 bit key support be introduced in the system. Since there is no mandatory requirement in the legacy systems for the use of integrity protection it was proposed in [S3-030244] that by setting a flag in the USIM by an operator indicating whether insecure negotiation is allowed could solve the problem. Whenever the flag is activated the terminal should then either encrypt the RES or use it as an input to a MAC algorithm as well as protecting the resubmission of the by the terminal proposed algorithms.

It is the understanding of Ericsson that these solutions would comply with the per SA3#28 agreed requirements:

- 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.

2.1 Secure Negotiation for Gb

It was highlighted in [S3-030244] that there are different means protocol wise to ensure that negotiating could be secure under the assumption that a flag is set in the USIM.

It is here now assumed that a MAC algorithm is used for securing the negotiation and in particular that the HMAC-SHA1 is used. Mainly because it is a well known scheme that have been used for a long time however as will be discussed later on this does not preclude future mechanisms e.g. based on encryption could be supported. The final protocol needs to allow for future enhancements. The current protocol is a three way handshake protocol as depicted below:

1. The terminal sends an Attach Request

2. The SGNS then sends an Authentication and Ciphering Request
3. The terminal sends then an Authentication and Ciphering Request

In the Attach Request the terminal includes *MS network capability* information element, which includes what algorithm, the terminal supports e.g. GEA1 through GEA4. In order to signal the HMAC-SHA1 identifier to the SGSN new fields are required. These new fields should be generic enough such that it makes it easy for future enhancements in terms of adding new algorithms, which include new MAC algorithms, and ciphering algorithms.

We denote here with M1 the relevant security parts in the MS Network capability:

M1=(GEA1, GEA2, GEA3, GEA4, HMAC-SHA1)

Note that this would require a new field for the indication of HMAC-SHA1. Ericsson assumes that it should be possible to have also in the future the support of other algorithms than HMAC-SHA1 including also potentially encryption algorithms. Hence for these new algorithms and HMAC-SHA1 it is proposed that it should not use the GEA code points. The message M1 is then stored in the terminal.

Upon receiving this Attach Request an SGSN, which is capable of secure negotiation, stores the message M1 whereas it is assumed that a legacy SGSN would not be able to handle HMAC-SHA1 and would therefore not process it. Here we now assume that the SGSN is capable of storing message M1 for future use. Assuming that SGSN chooses GEA4 and HMAC-SHA1 it then signals that back to the terminal in the Authentication and Ciphering Request i.e. M2=(GEA4, HMAC-SHA1) needs to be included in the Authentication and Ciphering Request requiring new fields for supporting the transportation of the HMAC-SHA1 identifier.

Here the terminal could be checking the Authentication and Ciphering Request that it includes the HMAC-SHA1 identifier verify that the SGSN was capable of secure negotiation. However since this is a weak form of verification the SGSN could instead calculate a MAC over e.g. M2 (=MAC-SGSN which is 96 bits) using IK as input and pad this to M2 i.e. the SGSN then signals M2' instead of M2 where M2'=M2||MAC-SGSN. If the flag has been set not to allow insecure negotiation the terminal could drop the communication should the MAC-SGSN be proven wrong by the terminal.

The flag should probably be of at least two-bit length such that one bit is indicating the capability of the SGSN and another bit indicating the policy of the home operator for smooth migration. Some more details on the flag is discussed under Clause 2.2 below.

If the flag in the USIM has been activated and secure negotiation shall be used the terminal shall given the message exchange above make use of HMAC-SHA1, which is truncated to 96 bits. First the terminal will process the Authentication and Key Agreement algorithms for deriving the RES, CK and IK. The terminal shall then send the message M3 in the Authentication and Ciphering Response indicating also that secure negotiation is used and the identity of the use algorithm i.e.:

M3=(Algorithm=HMAC-SHA1, Secure Negotiation=Yes, HMAC-SHA1(IK, RES||M1))

This would create new information elements in the Authentication and Ciphering Response. It seems feasible that the HMAC-SHA1(IK, RES||M1) could be carried in the Authentication parameter Response. However it would be important to know if there are any limitations from a protocol point of view e.g. the length of the parameters. Since now the RES was included in the HMAC-SHA1 calculation the SGSN is able to verify that the terminal was not only capable of secure negotiation but also that the policy of the USIM and the home operator is to use secure negotiation.

Upon receiving this message the SGSN concludes that Secure Negotiation is used and that the algorithm used is HMAC-SHA1 and retrieves the message M1, the XRES (i.e. the expected Response) and IK and then checks that:

HMAC-SHA1(IK, XRES||M1)= HMAC-SHA1(IK, RES||M1)

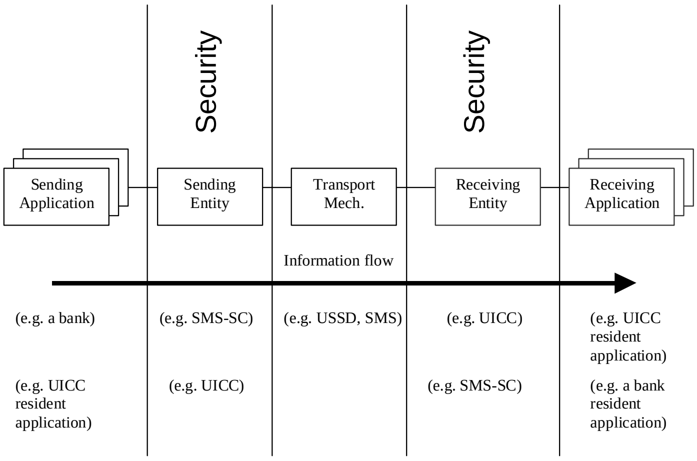
If this is true the user has been authenticated and the SGSN has verified that secure negotiation was possible and that M1 has not been tampered with. If it turns out to be false the SGSN should cancel the continuation of the communication.

In order to progress the work CN1 should study the implications on the Stage 3 specifications and if the approach discussed above is feasible and if there are any protocol restrictions that could affect the work of SA3. Furthermore CN1 should also study if there are any constraints with legacy SGNS should the procedures be implemented in Release 6 specifications.

2.2 Activation of the flag in the USIM

As indicated above the flag should probably be at list two bits. One bit for indicating that the SGSN is capable of secure negotiation and the other bit indicating the policy of the home operator if the terminal should accept insecure negotiation or not. This is probably useful in order to migrate to this function in a smooth way. If the first bit indicates that the SGSN supports secure negotiation the terminal could as described above propose the HMAC-SHA1 however if that is not included in the response from the SGSN for different reasons the terminal could still accept the communication and fallback to the old scheme should the policy say that it is allowed to do so. However when both bits are set then the terminal should not accept falling back to the old scheme. In the discussion that follows the flag is defined as at least two bits. It should also be stressed that the flag is set by the operator and then only read by the terminal telling the terminal the behaviour related to secure negotiation.

The [TS22048] specifies the Stage 1 requirements for the security mechanisms for (U)SIM application toolkit and the system overview is given below:



The secure negotiation mechanism as proposed in this document relies upon that the setting of the flag in the USIM can be done in a secure manner. The message sent by the Sending Application can be protected in several ways e.g. integrity protected, replay protected and confidentiality protected. It should be possible for an operator to activate the flag and if some problems would occur also deactivate the flag. Hence replay protection should be offered as well as integrity protection to the message. Confidentiality protection may also be offered.

The integrity protection could be provided with the means of a Cryptographic Checksum in the Security Header and the replay protection by using a counter in the security header. It is probably useful for the network to get a Secured Response Packet from the USIM such that the Sending Application can verify that the flag has been set or has the value that the operator want it to be.

Considering the potential threats applied between the sending entity and the receiving entity the following recommendations seem suitable:

- Use of CC and Triple DES
- Use of Counter and Replay protection
- Use of Secure Response Packet with the same security level as the received packet
- Optionally use of Ciphering with Triple DES

The control of the security level and the protection of the Packet to the USIM and so forth is under control of the operator and therefore SA3 should not mandate the security level. However the security level offered by secure negotiation relies upon the level of the security for setting the flag hence it could probably be advisable that SA3 adopts an informative annex in relevant specifications with the recommendations whenever the final solution has been adopted.

Since there is currently no file available at the moment for this flag indications there is a need to update [TS 31.102], which is under the responsibility of T3. It should be noted that the UICC may contain more than one USIM on one UICC however it seems feasible to tie this feature on a per UICC basis and hence there might be no need to have this file for all USIMs. This is an issue where SA3 should ask for some views from T3 and what the security implications could be. Furthermore the discussed mechanism could be done with higher granularity such that the flag is set per roaming partner. This would make the required memory space larger but could offer an operator some more flexibility probably at the cost of increased management of the flag. This is also something that T3 should study and advise SA3 the feasibility of such higher granularity of policy and SGSN capability setting.

Note: It is the Ericsson assumption that the setting of the flag is done before the roaming into an SGSN happens in order to avoid failure in service delivery and that it is done at the intervals decided by the Home Operator.

3 Conclusions

Ericsson proposes that liaison statements are sent to CN1 and T3 to study the feasibility from a Protocol point of view as well as USIM point of view based on the principles suggested in this document such that SA3 can further progress the work enhancing the Gb security with 128 bit key as well as introducing a scheme for secure negotiation. The liaison statements to CN1 and T3 should attach this contribution. SA3 is also recommended to send an LS to SA1 such that the service requirements can be considered.

Ericsson proposes that SA3 endorses the principles outlined in this contribution as the working assumption for secure negotiation for the Gb interface.

4. References

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

[S3-030244] Ericsson Enhanced Security for A/Gb, S3#28, 6 – 9 May 2003, Berlin, Germany

[S3-030308] TSG SA3 LS on: GERAN A/Gb mode security enhancements, 3GPP, S3#28, 6 – 9 May 2003, Berlin, Germany

[N1-030820] TSG CN1 LS on: “LS (S3-030308) on increasing the key length for GEA3”, 3GPP, N1#30, San Diego, California, USA, 19 – 23 May 2003