3GPP TSG SA WG3 Security — S3#28 **S3-030227**
6 - 9 May 2003 Berlin, Germany

Source: **Siemens**

Title: **Key length parameter within A5/3 and GEA3 specifications**

Document for: **Discussion and Decision**

Agenda Item: **7.6**

Abstract

This contribution discusses the use of the parameter KLEN within the A5/3&GEA3 specification TS 55.216 .

The conclusion is that the value of the parameter KLEN is currently fixed to 64-bit which value the implementations derive from many other specifications then TS 55.216. Using the same algorithm-id with different key lengths in future may lead to complicated solutions to accommodate that flexibility. It is proposed to write a CR against TS 55.216 in order to avoid confusion for present and future protocol implementations.

1) The use of KLEN according to TS 55.216.

TS 55.216 defines within sections 4.2 the input and output values of use with GEA3 (as example, the same applies to GSM A5/3 sections). Following italic text in an extract of this section.

“The inputs to the algorithm are given in table 7, the output in table 8:

Table 7: GEA3 inputs

Parameter	*Size (bits)*	*Comment*
INPUT	*32*	*Frame dependent input* ***INPUT[0]…INPUT[31]***
DIRECTION	*1*	*Direction of transmission indicator* ***DIRECTION[0]***
K_C	*64–128*	*Cipher key* ***K_C[0]… K_C[KLEN-1]****, where* ***KLEN*** *is in the range 64…128 inclusive (see Notes 1 and 2 below)*
M		*Number of octets of output required, in the range 1 to 65536 inclusive*

Table 8: GEA3 outputs

Parameter	*Size (bits)*	*Comment*
OUTPUT	*8M*	*Keystream octets* ***OUTPUT{0}…OUTPUT{M-1}***

NOTE 1: ***At the time of writing****, the standards specify that* ***K_C*** *is 64 bits long. This specification of the* ***GEA3*** *algorithm allows for possible future enhancements to support longer keys.*

NOTE 2: It must be assumed that ***K_C*** *is unstructured data — it must not be assumed, for instance, that any bits of* ***K_C*** *have predetermined values.”*

2) Cipher key length: fixed or variable ?

The ciphering algorithms for A/Gb mode use a 64-bit key and ciphering algorithm for the Iu-mode use a 128-bit key. The SIM or USIM based-authentication run supplies a ciphering key of a certain length and certain cryptographic strength (which is irrelevant here). The length of the generated key may need to be adapted at UE and network for use according to the effective needed length of the used mode following the some conversion functions and rules specified in TS 33.102 in interworking scenarios. The effective used key length is not signalled between UE and network but is therefore implicit. Currently the needed ciphering key length is fixed 64-bit for Kc (characteristic assigned to A/Gb mode)

As an example according to TS41.061 the GPRS ciphering algorithm requirements are: *italic text*

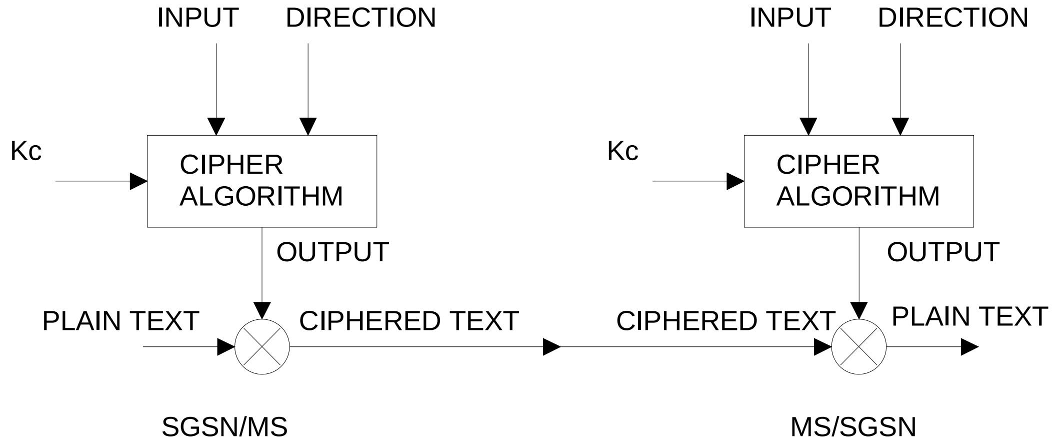

Figure: Basic GPRS ciphering environment

"The parameters of the algorithms are to be as follows:

Kc	*64 bits*
INPUT	*32 bits*
DIRECTION	*1 bit*
OUTPUT	*1600 octets"*

This implies that all Gb-mode algorithms shall apply a 64-bit Kc, *as defined by TS 41.061 GPRS ciphering and TS 44.064 LLC layer*, and this applies to GEA1..GEA3. Using GEA3 with many key-lengths will break that rationale.

Implementations could, based on bad interpretation of specification TS 55.216, supply the GEA3 algo with 128-bits, the leftmost 64-bits being produced by the authentication outcome, the 64 rightmost bits being set to zero. This thinking could be seeded by the note on future longer key lengths, and to be future compliant the error could be made.

Also note that current MAP specifications only allow Kc to be a multiple of 8-bit. Full KLEN flexibility can therefore not be achieved without a major change to the MAP-specifications

If 3GPP wants to apply GEA3 and/or A5/3 with many different key length, than both UE and network need to be signalled and need to agree the length. One endpoint of ciphering supporting all length option need to interwork with endpoints not supporting this. If 3GPP would define a Gb'/A'-mode then again the algorithm key length assignment would be implicit, otherwise the length negotiation may have to be made explicit with additional NAS procedures/parameters between the UE and the network. The easiest way would then be to follow the already established rules to define a new algorithm identifier (A5/4 and GEA4) and derive from this the characteristics of the key length input parameter. Key conversion functions currently base on the mode, changing the key-length rationale will make the handling more complicated or may require extra inter-network signalling.

Therefore Siemens has serious doubts on the future usefulness of the parameter KLEN. Siemens proposes to correct NOTE1 also because it may be interpreted wrong.

3) Conclusion

- The value of the parameter KLEN is currently fixed to 64-bit which value the implementations derive from several specifications. Using the same algorithm-Id with different key lengths in future may lead to problems at that time.
- It is proposed to write a CR against TS 55.216 in order to avoid confusion for present and future protocol implementation. It is proposed that the key length note for GEA3 is substituted by following text: ‘ NOTE 1: ~~At the time of writing, the standards specify that **K_C** is 64 bits long.~~ The~~is~~ specification of the **GEA3** algorithm only allows KLEN to be of value 64~~allows for possible future enhancements to support longer keys~~’. An alternative change , but similar in purpose , is to remove the existence of the KLEN parameter, but this could be regarded as a functional change. Similar text for A5/3 is suggested.
- The current MAP specifications only allow Kc to be a multiple of 8-bit which does not fit the Full KLEN flexibility. A Change Request shall be written to restrict the values of KLEN if the change proposed for NOTE 1 would not be acceptable.