3GPP TSG SA WG 3 (Security) meeting #11 **S3-000165**
Mainz, 22-24 January, 2000

3GPP TSG SA2 #11 **Tdoc S2-000306**
Puerto Vallarta, Mexico, 24 - 28 January 2000

Draft Liaison Statement

From: **S2**

To: **T3**

Copy: **S3**

Subject: **Response to T3-99-432, "LS on 'Clarification of the information storage in USIM"**

contact: chris.pudney@vf.vodafone.co.uk
tel: +44 1635 67 3397

The short answer is:
"CK next" and "IK next" need to be treated in the same way as the GSM SIM treats the GSM cipher key.

A longer answer is:
Although it may not be obvious from the GSM specifications, the GSM SIM card does not always store the cipher key that is in use on the radio connection.

For example,
if a call is made from a mobile which already has a valid cipher key, the network may start encryption and THEN authenticate the mobile.

This authentication process does not change the cipher key that is in use on the radio interface, however, the authentication process changes the cipher key that is stored on the SIM card. Ie the SIM card will be storing a cipher key that is different to the one in use: in fact it is storing "the next cipher key to be used".

Some relevant sections from GSM 04.08 are attached for your information.

A test in GSM 11.10, which is not attached, can also be used to derive further insight (see section 26.6.8.4).

3.4.7 Ciphering mode setting procedure

In dedicated mode, the ciphering mode setting procedure is used by the network to set the ciphering mode, i.e. whether or not the transmission is ciphered, and if so which algorithm to use. The procedure shall only be used to change from "not ciphered" mode to "ciphered" mode, or vice-versa, or to pass a CIPHERING MODE COMMAND message to the mobile station while remaining in the "not ciphered" mode. The ciphering mode setting procedure is always triggered by the network and it only applies to dedicated resources.
The cipher mode setting procedure shall not be applied in group transmit mode.

3.4.7.1 Ciphering mode setting initiation

The network initiates the ciphering mode setting procedure by sending a CIPHERING MODE COMMAND message to the mobile station on the main signalling link, indicating whether ciphering shall be used or not, and if yes which algorithm to use.
Additionally, the network may, by the use of the cipher response information element, request the mobile station to include its IMEISV in the CIPHERING MODE COMPLETE message.
The new mode is applied for reception on the network side after the message has been sent.

3.4.7.2 Ciphering mode setting completion

Whenever the mobile station receives a valid CIPHERING MODE COMMAND message, it shall, if a SIM is present and considered valid by the ME and the ciphering key sequence number stored on the SIM indicates that a ciphering key is available, load the ciphering key stored on the SIM into the ME. A valid CIPHERING MODE COMMAND message is defined to be one of the following:

- one that indicates "start ciphering" and is received by the mobile station in the "not ciphered" mode;
- one that indicates "no ciphering" and is received by the MS in the "not ciphered" mode; or
- one that indicates "no ciphering" and is received by the mobile station in the "ciphered" mode.

Other CIPHERING MODE COMMAND messages shall be regarded as erroneous, an RR STATUS message with cause "Protocol error unspecified" shall be returned, and no further action taken.
Upon receipt of the CIPHERING MODE COMMAND message indicating ciphering, the mobile station shall start transmission and reception in the indicated mode.
When the appropriate action on the CIPHERING MODE COMMAND has been taken, the mobile station sends back a CIPHERING MODE COMPLETE message. If the "cipher response" field of the cipher response information element in the CIPHERING MODE COMMAND message specified "IMEI must be included" the mobile station shall include its IMEISV in the CIPHERING MODE COMPLETE message.
Upon receipt of the CIPHERING MODE COMPLETE message or any other correct layer 2 frame which was sent in the new mode, the network starts transmission in the new mode.

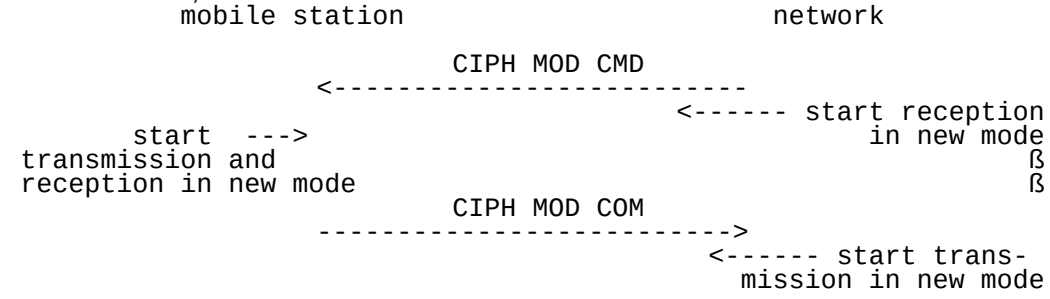

Figure 3.3/GSM 04.08: Ciphering mode setting sequence

4.3.2 Authentication procedure

The purpose of the authentication procedure is twofold:

First to permit the network to check whether the identity provided by the mobile station is acceptable or not (see GSM 03.20);

Second to provide parameters enabling the mobile station to calculate a new ciphering key.

The cases where the authentication procedure should be used are defined in GSM 02.09.
The authentication procedure is always initiated and controlled by the network.

4.3.2.1 Authentication request by the network

The network initiates the authentication procedure by transferring an AUTHENTICATION REQUEST message across the radio interface and starts the timer T3260. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see GSM 03.20). It also contains the ciphering key sequence number allocated to the key which may be computed from the given parameters.

4.3.2.2 Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. It shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network. The new ciphering key calculated from the challenge information shall overwrite the previous one and be stored on the SIM before the AUTHENTICATION RESPONSE message is transmitted. The ciphering key stored in the SIM shall be loaded in to the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in section 3.4.7.2). The ciphering key sequence number shall be stored together with the calculated key.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20).

4.3.2.4 Ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets, i.e. from a challenge parameter RAND both the authentication response SRES and the ciphering key can be computed given the secret key associated to the IMSI.
In order to allow start of ciphering on a RR connection without authentication, the ciphering key sequence numbers are introduced. The sequence number is managed by the network in the way that the AUTHENTICATION REQUEST message contains the sequence number allocated to the key which may be computed from the RAND parameter carried in that message.
The mobile station stores this number with the key, and indicates to the network in the first message (LOCATION UPDATING REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST) which sequence number the stored key has. When the deletion of the sequence number is described this also means that the associated key shall be considered as invalid.
The network may choose to start ciphering with the stored key (under the restrictions given in GSM 02.09) if the stored sequence number and the one given from the mobile station are equal.