TSG-SA WG3 (Security) meeting #12
Stockholm, Sweden, 11-14 April 2000

S3-000222

Agenda Item:

Source: Siemens Atea

Title: Initiation of COUNT-I and COUNT-C

Document for: Decision

TS 25.331 currently describes that two "initial HFN values" are transported from the UE to the RNC. TS 33.102 only mentions one "START" value. This contribution addresses the following issues:

- Do we need a START-C and a START-I?
- What length should START have?
- Where is the START value stored at the user side and how is it managed?

Do we need a START-C and a START-I?

No.

START is needed to prevent that a COUNT-C or COUNT-I is re-used with the same CK or IK. Having only one START value, equal to the most significant bits of the maximum of all COUNT-C and all COUNT-I values, rather than having two, saves on signalling, storage and complexity. We suggest that TS 25.331 be amended to reflect this.

What length should START have?

The RRC HFN for integrity is 28 bits long, the RLC HFN for ciphering can be 20 or 25 bits long, the MAC HFN for ciphering RLC TM channels is 25 bits long. Does this require START to be equal to the maximum value? No. START can be smaller and just initialise the MSB of the different HFN; the remaining LSB are then set to zero.

START can however not be too short. Shortening START will lead to faster incrementation and leads to it that COUNT-C or COUNT-I sooner wraps around, or rather reaches its maximum value, or rather reaches its threshold value. However, the range for START is that large, that some shortening need not be a problem.

In RLC TM – assuming for a while COUNT-C is the fastest to increase (which is certain) and of all logical channels RLC TM is the one increasing fastest – HFN is incremented every 0,72 seconds. Then the 20^{th} bit is incremented every 23 seconds whereas the 16^{th} bit is incremented every 6 minutes. Therefore, with 24 bit, 20 bits, 16 bit START values, the initial HFN values increment every 1,5 seconds, 23 seconds, 6 minutes. And if a call is ended, the remaining time in the current interval between successive HFN increments is "lost". Given the fact the total HFN range accommodates for over 24 million seconds or 400 thousand minutes, loosing some seconds or even minutes does not appear to be a problem. Surely, because there is the recommendation/obligation for the serving network to refresh the keys at least every 24 hours, i.e., every 1440 minutes or 86 thousand seconds.

Therefore, we propose a 16 bit START value.

Where is the START value stored at the user side and how is it managed?

We propose the following:

> The UE and the USIM store a START value. When the USIM is removed, the UE deletes its START value. At insertion of a USIM, the USIM sends its START value to the UE, which stores the received START value.
>
> During an ongoing radio connection, the START value in the UE is defined as the 16 MSB of the maximum of the current COUNT-C and COUNT-I values, incremented by 1, i.e.,
>
> $$START = MSB_{16} (MAX \{COUNT\text{-}C, COUNT\text{-}I \mid \text{for all signalling and user data logical channels}\}) + 1$$
>
> In idle mode, the START value in the UE is the last START value reached during the previous radio connection or the START value received at USIM insertion.
>
> At radio connection establishment when in idle mode, the UE sends a message to the USIM to mark the START value stored in the USIM as invalid.

At radio connection establishment the UE sends the START value to the RNC in the *RRC connection setup complete* message.

The UE and the RNC then initialise the 16 most significant bits

- of the RRC HFN for integrity to START; the remaining 12 LSB are initialised to zero;
- of the RLC HFN for ciphering of RLC AM to START; the remaining 4 LSB are initialised to zero;
- of the RLC HFN for ciphering of RLC UM to START; the remaining 9 LSB are initialised to zero;
- of the MAC HFN for ciphering of RLC TM to START; the remaining 9 LSB are initialised to zero.

Upon connection release the UE sends a message to the USIM with the current START value. The USIM updates the START value and marks it as up-to-date.