3GPP TSG SA WG3 Security — S3#10 **S3-000074**

19-21 January, 2000

Antwerpen, Belgium

TSG-SA WG3 (Security) meeting #9 ***TSGS-WG3#9(99)549***

Helsinki, 7-9 December, 1999

Proposed CR to 33.102 section 6.4.3 on USIM triggered authentication and key setting during PS connections

(Source: Vodafone)

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time a~~n~~ CS mode RRC connection is ~~released~~ established an operator-controlled THRESHOLD value is transferred from the USIM to the UE. When the connection is released, the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is compared with the THRESHOLD value~~stored in the USIM.~~, it is then stored in the USIM. If the ~~When the next RRC connection is established that value is read from the USIM and incremented by one.~~ hyperframe number exceeds the maximum value denoted by THRESHOLD then the UE shall trigger authentication at the next RRC connection request. When the next RRC connection is established the previously stored HFN value is read from the USIM and incremented by one.

Each time a PS mode RRC connection is established an operator-controlled THRESHOLD value is transferred from the USIM to the UE. The current value of the hyperframe number (the current value of COUNT) of the bearers that are protected in that RRC connection is monitored in the UE. If the hyperframe number counter reaches the maximum value denoted by the THRESHOLD value then the UE shall trigger authentication immediately (i.e. during the connection).

~~The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out.~~USIM triggered authentication shall involve the generation of a new access link key set (a cipher key and an integrity key) and their immediate use through the security mode negotiation procedure that follows authentication.

~~This mechanism will ensure that a cipher/integrity key set cannot be reused more times than the limit set by the operator.~~