**3GPP TSG-SA3 Meeting #119 S3-244956r1**

**Orlando, USA 11 – 15 November 2024**

**Source: Qualcomm Incorporated**

**Title: Further additions to the enhancement of IOPs in solution #3**

**Document for: Approval**

**Agenda Item: 5.7**

1 Decision/action requested

***This contribution proposes a sequence number handling profile for the IOPS enhancement to address the remaining ENs.***

2 References

[1] S3-243827 draft TR 33.700-29

3 Rationale

This contribution proposes a profile for the sequence number handling profile similar to those in Annex C of TS 33.102 [2]. The provides the missing detail on the impact of key lifetime limitation and the overall enhancement and hence resolve the Editor’s notes in the text.

4 Detailed proposal

It is proposed to approve the below for inclusion in [1].

**\*\*\*\* START OF CHANGES \*\*\*\***

6.3 Solution #3: IOPS based solution for UE to satellite security

6.3.1 Introduction

This solution addresses key issues #1 and #2.

It applies to an architecture when a complete network is deployed in the satellite or set of interlinked satellites.

6.3.2 Solution details

6.3.2.1 IOPS based solution

This solution applies to the case that the whole network, i.e. serving and home network, is hosted in the satellite or set of satellites. For EPS this includes deploying an HSS in the (set of) satellite(s). In this case all the security procedures that are used between the UE and satellite(s) are the same one as used between the UE and network in regular 3GPP access.

Such a type of solution requires the pre-configuration of credentials that are used to authenticate with the UE in the satellite. In order to enable different keys to be configured in different satellites for the same UE, it is proposed to use a solution like the one described in Annex F.4 of TS 33.401 [3].

NOTE: As all the parameters used in Annex F.4 of TS 33.401 [3] relate to the authentication between the UE and network and are in effect under an operator’s control, solution similar to one described could be used.

The solution described in Annex F.4 of TS 33.401 [3] uses bits of the AMF field in the AUTN parameter and also possibly the IND part of the sequence number SQN, as described in Annex C.1 of TS 33.102 [7] to calculate a root key for the authentication between the UE and particular (set of) satellite(s). This means that a different key can be used between the UE and each different (set of) satellite(s). This is achieved using existing information and hence requires no update to the signalling that is used between UE and regular networks.

The solution supports roaming by having the relevant key for the UE provisioned into the satellite PMLN’s HSS (which does not have to be the UE’s HPLMN). Provisioning such a key enables the UE to access the PLMN supported by the satellite.

With this solution, there is only a need to re-establish the security when the UE moves away from the set of interlinked satellites and the overall processing in the HSS in authenticating a UE is the same regardless of the location of the HSS. The authentication latency is small and the reliability is high with the HSS in the satellite(s) as it is always possible to authenticate the UE in a single uninterrupted operation.

6.3.2.2 Enhancement to IOPS solution

##### 6.3.2.2.1 Enhancement description

One part of the IOPS solution that is not discussed in the above clause is the way a new key can be calculated for a particular value of the AMF field in the AUTN parameter by using a value m for each value of the AMF field. An example of the use of value m is described in Annex F.4.2 of TS 33.401 [3]. The effect of that Annex is to base the key derivation on the m value in addition to the n value and hence old keys are in effect deprecated.

The following describes a method that could be used to automatically update the value of m. This is done by including m in the SQN number that is sent to the USIM, e.g.

SQN = (20 bit) m value () | (28 bit) SEQ value

The least significant bits of m would need to be sent in the clear, i.e. not encrypted by AK, so that the USIM can get estimate the value of m. Alternatively if all UEs have the same m value, the whole of m can be sent in the clear. In this example the HSS in the satellite would only be able to generate at most 8228) AVs because change of m value requires a new key to generate AV. This illustrates how this can be used to limit the effect of a compromise of onboard HSS in the satellite and of course different lengths of m can be chosen in practise if a much smaller number of AVs from a particular key is desired. The USIM would store the largest m value used for successful authentication for a particular n value and not accept any AVs with an m value that is less than the stored m value. When the HPLMN provide a new key to the satellite, the HPLMN also provides the value of m to use with that key. This enables the satellite to create the SQN for the AV embedding the value of m to be used by the USIM to ensure that the HSS in the satellite and USIM use the same value of m when creating or processing the AV respectively. The top bits of SQN could alternatively carry some bits of n if a larger value of n that can be supported by the AMF bits is required. Such bits of n would need to be sent in the clear hence it is recommended to use the same n for all UEs connecting to the (set of) satellite(s) to avoid tracking of UEs.

The result of this auto-updating of the m values is that an old key gets deprecated after the successful reception of an AV with a larger m value in the SQN. So for example if a HSS in a satellite always is given a fixed value of n for a particular UE, then once an AV has been processed by the USIM with a particular value of m, then all smaller values of m will not result in a successful processing of the AV by the USIM. This deprecation happens in-band during AV processing rather than by out-of-band methods as currently expected in Annex F.4.2 of TS 33.401 [3]. This is a similar security property to that of AVs generated in a HPLMN HSS in regular deployments. Supporting this enhancement does not prevent the n and m values being updated as described in Annex F of TS 33.401 [3].

##### 6.3.2.2.2 Example sequence number management profile

This clause provides an example sequence number management profile similar to the ones given in Annex C.3 of TS 33.102 [7]. As the actual profile to use is determined by the operator, an example profile belongs in an informative part of a specification. This profile is for sequence numbers which are not time-based.

For this profile it is proposed the m has length 20 bits and SEQ has length 28 bits. Such a choice allows there to be 220 different keys for a particular n value and each key can generate up 228 AVs. It is assumed that all users on a particular (set of) satellite(s) use the same n and m values which prevent a UE being traced based on those values.

NOTE 1: Similar to as noted in clause F.4.1 of TS 33.401 [3], if the AMF bits are not enough to handle the number of the desired different (sets of) satellite(s), then it is possible to use some of the that are proposed to carry m to carry some bits of n. This can be done without changing the rest of the analysis of this solution.

**Generation of sequence numbers:**

The HSS in the satellite shall maintain a counter for each user, SEQHE, related to the current value of n and m for each user. To generate a fresh sequence number, SEQHE is incremented by 1, and the new counter value is used to generate the next authentication vector. SEQHE is set to 0 when either n and/or m are changed for a particular user.

**Verification of sequence numbers in the USIM:**

**Protection against wrap around**: Choose Δ = 214.
Choosing Δ = 214 means that an attack to force the counter in the USIM to wrap around would require at least 228/Δ = 214 > 16,000 successful authentications (cf. note 6 of C.2.3 in TS 33.102 [7]). Note 7 of Annex C.2.3 of TS 33.102 [7] does not apply.

**Age limit for sequence numbers:**There is no clock here. So, the “age” limit would be interpreted as the maximum allowed difference between SQNMS (see section 6.3 of TS 33.102 [7]) and the sequence number received. The use of such a limit is optional. The choice of a value for the parameter L affects only the USIM. It has no impact on the choice of other parameters and it is entirely up to the operator’s security policy. Therefore, no particular value is suggested here.

**User anonymity:** the value of SEQ may allow to trace the user over longer periods. The SEQ part of the SQN can be concealed by an anonymity key as specified in section 6.3 of TS 33.102 [7].

NOTE 2: This can be done be simply selecting 28 bits of the regular 48 bit AK.

6.3.3 Evaluation

The solutions described in clauses 6.3.2.1 and 6.3.2.2 are applicable to the case that the full core network is on board the satellite.

The solutions rely on IOPS solution described in TS 33.401 [3] and does not require further changes to the LTE security procedure other than the IOPS related ones.

It is left out of scope of the solution how the HSSs on the satellites are provisioned with the keys etc.

The enhancement described in clause 6.3.2.2, enables the automatic deprecation of the key(s) deployed in the HSS(s) deployed in satellites, relies on deployment of USIM supporting IOPS with the enhancement described in TS 33.401 [3]. The HSSs in satellite will also need to support generation of AVs that is compatible with such USIMs. This involves a slightly modified handling of the SQN numbers used in AVs compared to regular 3GPP accesses and calculation of keys compared to the existing IOPS solution. The enhancement of the IOPS solution given in clause 6.3.2.2 deprecates the keys in HSS in a similar manner that old AVs are deprecated in regular LTE.

**\*\*\*\* END OF CHANGES \*\*\*\***