

libosmocore - Bug #1968

upon auth resync with osmo_auth_gen_vec_auts(), use MS.SQN + (2 ^ IND)

03/07/2017 01:56 PM - neels

Status: Closed	Start date: 03/07/2017
Priority: Immediate	Due date:
Assignee: neels	% Done: 100%
Category:	
Target version:	
Spec Reference:	
Description USIMs have an IND value denoting the lower number of bits that are "below" the synchronized SQN significance, i.e. we need to flip at least the (IND+1)th bit when doing AUTS resync. For example, receiving an AUTS from a USIM showing MS.SQN = 0, an IND = 5 means that the next auth vector should be produced for MS.SQN = 2^5 = 32. So far we are using MS.SQN + 1, which causes the USIM to ask for resync again and again. Add <i>ind</i> argument to osmo_auth_gen_vec_auts() so that the caller can communicate the USIM's IND setting, and increment SQN by (1 << IND).	
Related issues:	
Related to OsmoHLR - Feature #1969: add IND for proper UMTS auth resync	Closed 03/07/2017
Related to Cellular Network Infrastructure - Support #1965: use sysmoUSIM-SJS...	Closed 03/04/2017

History

#1 - 03/07/2017 01:57 PM - neels

- Status changed from New to In Progress

#2 - 03/07/2017 02:01 PM - neels

- Related to Feature #1969: add IND for proper UMTS auth resync added

#3 - 03/08/2017 10:08 PM - laforge

- Related to Support #1965: use sysmoUSIM-SJS1 with 3G OsmoMSC added

#4 - 03/13/2017 12:11 AM - neels

We need both an *ind* and an *i* argument:

ind defines the amount of bits that are not significant for SEQ and make up SQN.

i defines which IND slot/bucket the current SQN consumer wants SQNs for.

```
|-----SEQ-----|
|-----SQN-----|
|<----->|<-- IND
```

We also need *ind* and *i* in the non-AUTS vector generation code.

Every consumer shall get N vectors as (SEQ + (n << IND) + i),
e.g. for IND 5 bits, the IND value range has 2^5 32 slots,
and a consumer with i 0 gets 32, 64, 96,... where i 1 gets 33, 65, 97...

This is only needed for UMTS auth, but will affect large parts of the public osmo_auth API.
Probably best to add new API to be used for UMTS auth, while the old API remains available.

#5 - 03/20/2017 12:51 PM - neels

- *Status changed from In Progress to Resolved*

- *% Done changed from 0 to 100*

https://gerrit.osmocom.org/#/q/status:merged+project:libosmocore+topic:umts_aka

#6 - 04/25/2017 01:57 PM - laforge

- *Status changed from Resolved to Closed*