# OsmoNITB - Feature #1593

## UMTS AKA support

02/23/2016 03:49 PM - laforge

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 02/23/2016 |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | neels | **% Done:** | 100% |
| **Category:** | | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

Even over a GSM/GPRS RAN, most phone today can perform mutual authentication based on UMTS AKA.

libosmocore also already has the UMTS authentication code in place for years, but OsmoNITB is not using it. HLR changes are associated with it, as we need to store K+OPC+SQN.

**Related issues:**

| | | |
|---|---|---|
| Related to OsmoNITB - Feature #1711: 3G Auth | **Closed** | **05/14/2016** |
| Related to OsmoSGSN - Feature #1956: UMTS AKA support in OsmoSGSN | **Closed** | **02/20/2017** |

### History

**#1 - 04/28/2016 07:12 PM - laforge**

*- Status changed from New to In Progress*

*- Assignee set to laforge*

**#2 - 08/01/2016 12:23 PM - laforge**

*- Related to Feature #1711: 3G Auth added*

**#3 - 08/09/2016 12:16 PM - laforge**

*- Priority changed from Low to High*

**#4 - 11/11/2016 08:38 AM - laforge**

*- Assignee changed from laforge to neels*

**#5 - 02/02/2017 04:07 PM - neels**

First UMTS AKA test suites have been added to osmo-hlr (testing e.g. correct tuples generated for GSM with UMTS AKA with test vectors taken from 3GPP TS 55.205) and on openbsc on the neels/vlr branch (testing pure UMTS AKA over UTRAN). More details: https://osmocom.org/issues/1711#note-12

**#6 - 02/02/2017 04:07 PM - neels**

https://gerrit.osmocom.org/1695

**#7 - 02/09/2017 03:28 AM - neels**

https://gerrit.osmocom.org/#/q/topic:umts_aka

**#8 - 02/20/2017 01:35 PM - neels**

*- Related to Feature #1956: UMTS AKA support in OsmoSGSN added*

**#9 - 02/20/2017 01:37 PM - neels**

*- % Done changed from 0 to 50*

copied from "3G Auth" #1711:

> Verified with real equipment that our GSM-Milenage algorithm (for abbreviated Milenage on pre-R99 networks) works with a sysmoUSIM-SJS1 configured to do Milenage for both 2G and 3G.
>
> One thing though, I expected this to now do full UMTS Auth when using an R99+ MS, and the GSM-Milenage fallback only when the MS is pre-R99. But even though the USIM is in an R99+ MS (Samsung Galaxy S4m), the LU Request still indicates "GSM phase 2" in the classmark and GSM-Milenage is used instead of normal UMTS Milenage.

Unless we find out how to test this on pre-R99, we will only be able to test full UMTS auth when we have the sysmocom/iu branch rebased onto the VLR developments. So far the msc_vlr end-to-end tests suggest that UMTS AKA will work on real equipment with OsmoNITB (branch neels/vlr).

#### #10 - 02/21/2017 12:33 PM - neels

The Quectel EC20 also sends classmark "GSM phase 2" even though it is R99 with a USIM.
Next: try to find out whether some SI we transmit tells the MS to not do R99.

#### #11 - 02/21/2017 12:46 PM - neels

Indeed SI3 contains a Control Channel Description with a previously spare bit set to 1 for R99 or later, which our MSC sends as 0 and thus indicates to the MS that we're not capable of UMTS.
3GPP TS 44.018 9.1.35 'System information type 3' and 10.5.2.11 'Control Channel Description'

#### #12 - 02/21/2017 02:48 PM - neels

We currently send "MSC is pre R99" for MSC in SI3 and "SGSN is R99+" in SI13.

First test with MSCR set to R99 reveals that now the MS (Quectel EC20) indeed sends R99 in classmark1 and happily runs an authentication sync request (Auth Failure with AUTS token), after which our MSC/VLR fails to send another Authentication Request.

After a few attempts, the LU is successful because no sync is requested.
That's because the USIM was also used on another test setup and has a higher key SQN, and the HLR db by coincidence caught up with that SQN after a few LU requests.

So the conclusion is that basic UMTS AKA works, but we still have some bug in the AUTS process.
Debugging it now.

#### #13 - 02/21/2017 03:21 PM - neels

One problem is that we still missed one spot where our gsup.c code expects a 16 byte AUTS, it has to be 14 instead.
https://gerrit.osmocom.org/1860

There's apparently still some other problem, debugging now.

#### #14 - 02/22/2017 02:35 AM - neels

*- % Done changed from 50 to 90*

Found these fixes:
https://gerrit.osmocom.org/1860
https://gerrit.osmocom.org/1870
https://gerrit.osmocom.org/1864

accompanied by tests and others:
https://gerrit.osmocom.org/#/q/topic:auts

With these fixes and the VLR branch, tests with real equipment show successful UMTS AKA including AUTS resync with OsmoNITB on a GSM network with R99 MSC and MS. Excellent!

#### #15 - 03/04/2017 04:19 AM - neels

*- Status changed from In Progress to Resolved*

*- % Done changed from 90 to 100*

The sysmocom/iu branch has been rebased onto the vlr branch and now also features UMTS AKA in the 3G OsmoMSC (= the OsmoNITB without BSC and with a separate HLR).

**#16 - 04/25/2017 01:57 PM - laforge**

*- Status changed from Resolved to Closed*