pySim - Bug #3552

IMSIs shorter than 15 are not encoded properly

09/13/2018 12:53 PM - ben.foxmoore

Status:	Resolved	**Start date:**	09/13/2018
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	100%
Category:			
Target version:			
Spec Reference:	TS 31.102		

Description

When programming a (sysmoUSIM-SJS1) SIM with an IMSI shorter than 15, the encoded format isn't correct.

This is demonstrated in two ways:
1) pySim-read.py fails to read the IMSI back (private details removed):

```
[ben@thoth pysim]$ ./pySim-prog.py -p 0 -t sysmoUSIM-SJS1 -a $adm -n $name -x 1 -y 1 -i 0010123456
7 -s $iccid -o $opc -k $ki
Insert card now (or CTRL-C to cancel)
Generated card parameters :
 > Name    : $name
 > SMSP    : ---
 > ICCID   : $iccid
 > MCC/MNC : 1/1
 > IMSI    : 00101234567
 > Ki      : $ki
 > OPC     : $opc
 > ACC     : None

Programming ...
Done !

[ben@thoth pysim]$ ./pySim-read.py -p 0
Reading ...
ICCID: $iccid
Traceback (most recent call last):
  File "./pySim-read.py", line 100, in <module>
    print("IMSI: %s" % (dec_imsi(res),))
  File "/home/ben/pysim/pySim/utils.py", line 65, in dec_imsi
    oe = (int(swapped[0])>>3) & 1    # Odd (1) / Even (0)
ValueError: invalid literal for int() with base 10: 'f'
```

2) Our Essential PH-1s running Android 7.1.1 don't detect the SIM programmed this way.

I believe the issue occurs because of a misunderstanding of the TS 31.102 spec regarding IMSI encoding.

The two relevant parts are:

```
the length indicator refers to the number of significant bytes, not including this length byte, re
quired for the IMSI
```

and

```
if a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.
```

The current code base left pads with F, which I think should be right padded instead.

It also encodes the length as half the number of digits in the IMSI (rounded up). This isn't correct for even length IMSIs.
With even length IMSIs, the odd/even parity bit bumps the last digit into an extra byte, which should be counted as well.

I have attached a patch which fixes both of these issues, and also fixes decoding IMSIs with this encoding.

Using this patch, I have tested shorter IMSIs (both even and odd length) on the Essential phone mentioned above, as well as an iPhone 6.
In both cases, the S1 InitialUEMessage now contains the correct IMSI.

History

#1 - 09/13/2018 02:05 PM - laforge

- Assignee set to dexter

#2 - 09/24/2018 01:55 PM - dexter

- Status changed from New to In Progress

- % Done changed from 0 to 100

Hello Ben.

Thanks for posting your fix. I have tested it locally. Pysim has indeed problems with short IMSIs. After applying your patch short IMSIs seem to work fine. I also see the correct IMSI on my blackberry and in sysmo-usim-tool.

See also: https://gerrit.osmocom.org/#/c/pysim/+/11073 utils: fix encoding/decoding of IMSI value

best regards,
Philipp

#3 - 09/24/2018 04:07 PM - ben.foxmoore

Hi Philipp,

That's great news. Also nice to have confirmation that the issue was really there, and wasn't just something we were doing wrong!

Ben

#4 - 09/26/2018 08:37 AM - dexter

Hello Ben,

In order to have the git history correct, can you pass me an email-address that I can set as GIT_AUTHOR_EMAIL for your commit.

best regards,
Philipp

#5 - 09/26/2018 12:53 PM - ben.foxmoore

Hi Philipp,

You can use ben.foxmoore@accelleran.com as my email. My full name is "Ben Fox-Moore".

Thanks,
Ben

#6 - 09/26/2018 04:16 PM - dexter

Hello Ben,

thanks. I have now updated the patch in gerrit.

best regards,
Philipp

#7 - 10/01/2018 07:14 AM - dexter

- Status changed from In Progress to Resolved

Files

0001-Fix-IMSIs-which-are-shorter-than-15-characters.patch	2.72 KB	09/13/2018	ben.foxmoore