Proactive SIMs

Nov 2021

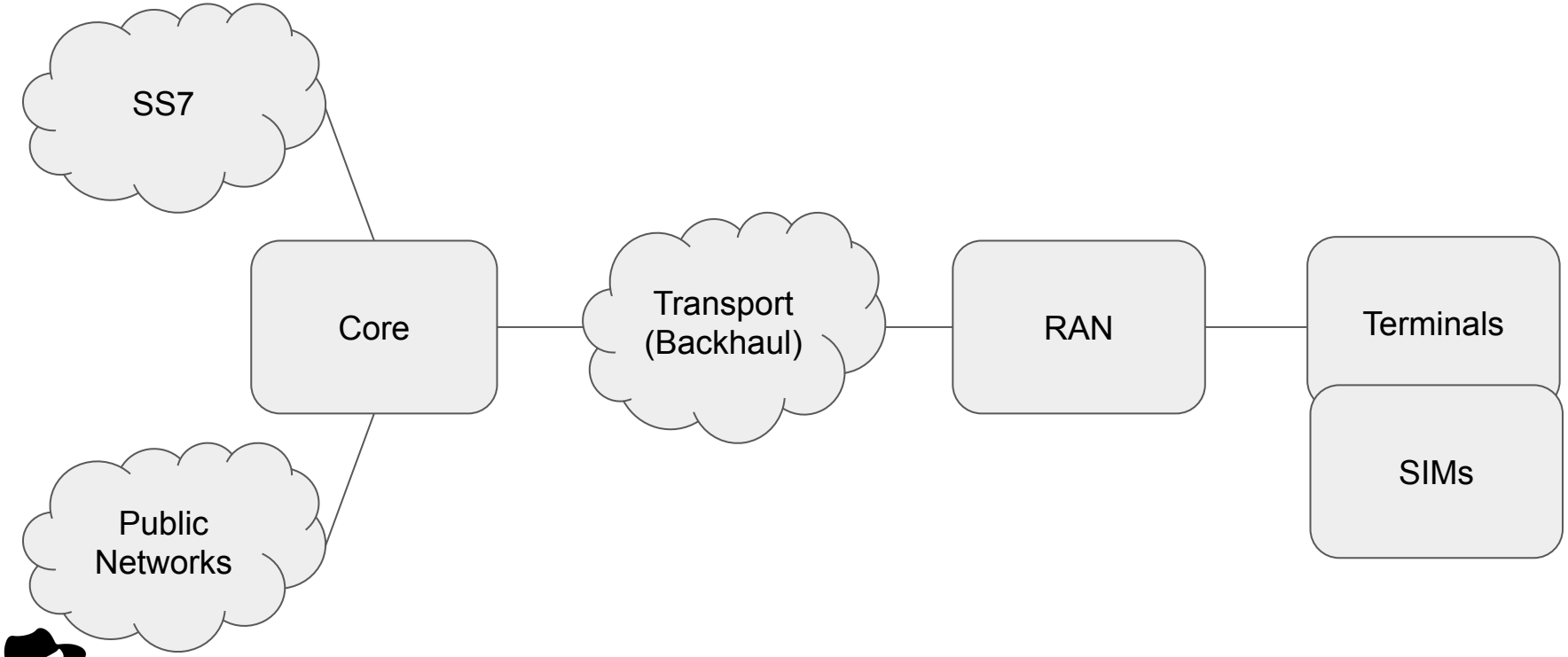
David Allen Burgess
@dburgess00
david.allen.burgess@gmail.com

Telecom is not IT

How I got interested in proactive SIMs.

The SIM

Segments of a mobile network



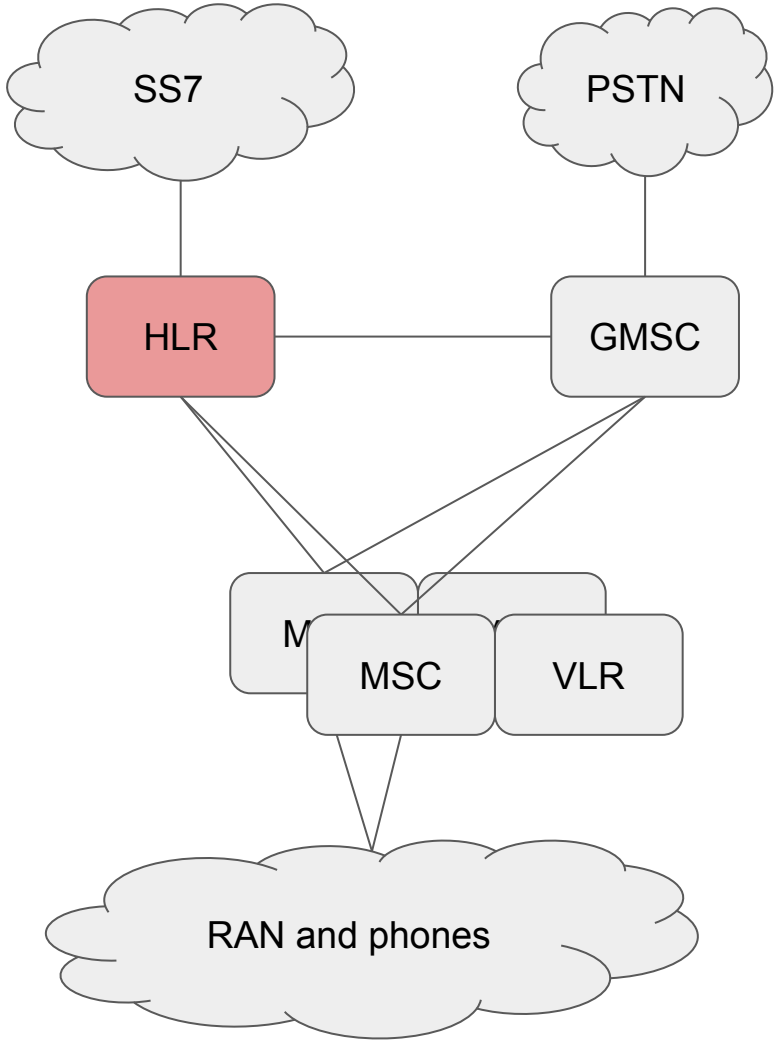
The CS core network

Home Location Register (HLR) - The master subscriber database. Holds all customer and SIM data.

Mobile Switching Center (MSC) - Connects the circuits for telephone calls. Usually one MSC handles 20k - 200k subscribers. Early MSCs were just ISDN switches with some added SW.

Visitor Location Register (VLR) - Handles authentication and mobility management functions. Usually one VLR per MSC.

Gateway Mobile Switching Center (MSC) - A specially designated MSC that connects to other operators or to the PLMN.



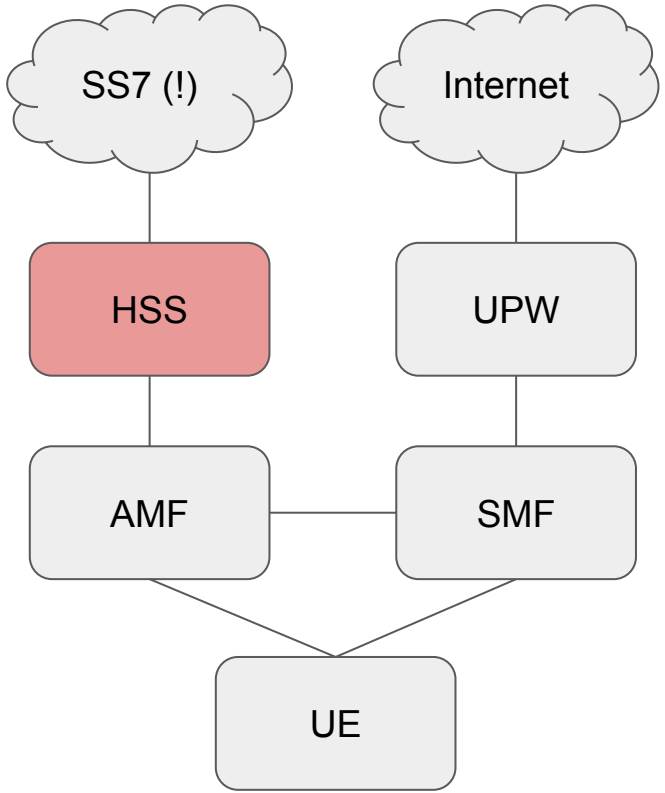
The PS core network (5G)

Home Subscriber Server (HSS) - New name for the old HLR, now with DIAMETER, but SS7 is still commonly used for roaming..

Access and Mobility Management Function (AMF) - Functionally similar to MME.

Session Management Function (SMF) - Functionally similar to SGW.

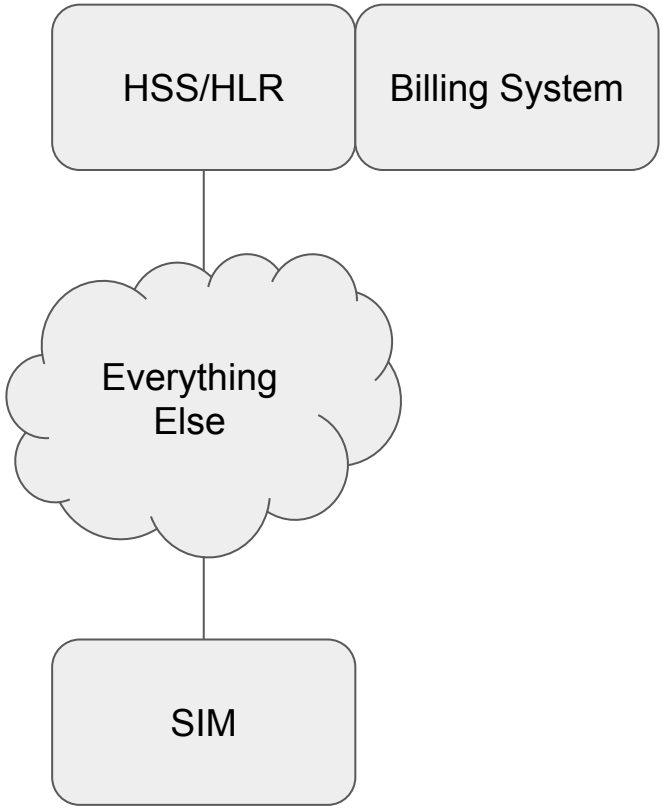
User Plane Function (UPW) - Functionally similar to PGW.



A High-Level View of the Network

Deep in the core is the HSS/HLR, the subscriber database, and home of the secret keys used for security procedures, which are also hidden in the SIM.

At a high level, the mobile device, the RAN, and the core are just a transport between the SIM and the HSS/HLR.



Brief intro to SIMs

Where the SIM sits

Basic SmartCard operation

The SIM Tool Kit (STK)

JavaCards

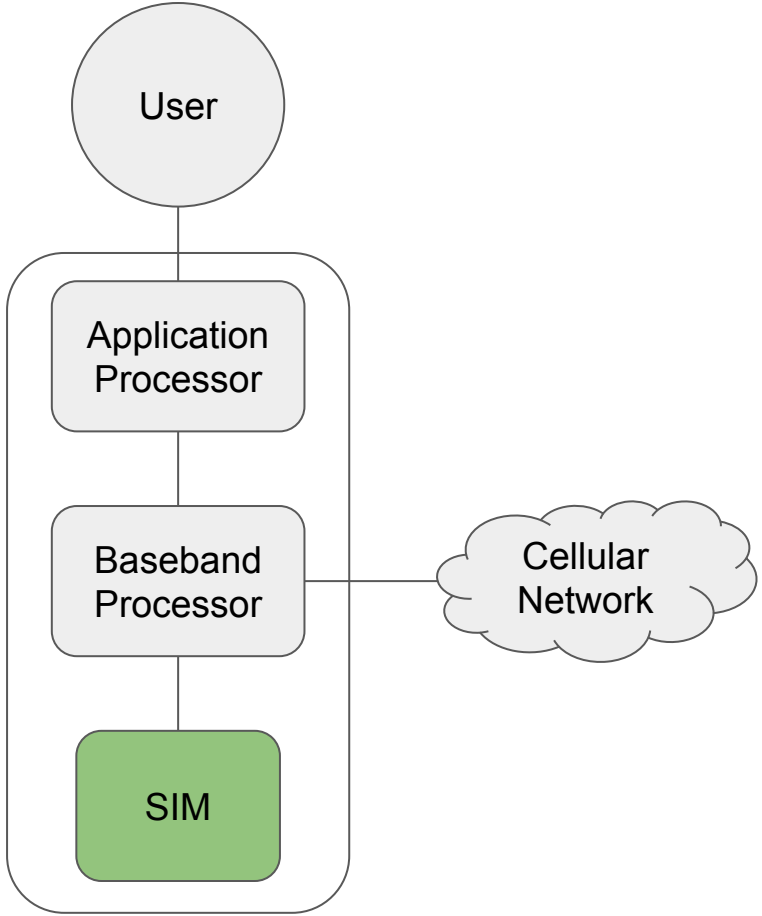
Proactive SIMs

Where the SIM sits

The SIM is a complete computer system, with its own OS and software.

When it is installed, it becomes part of you phone, and can drive operations of the phone without your knowledge.

Note that in this arrangement the application processor has no direct access to communication between the SIM and the baseband processor. From a telecom standpoint, the application processor is a bolt-on accessory.

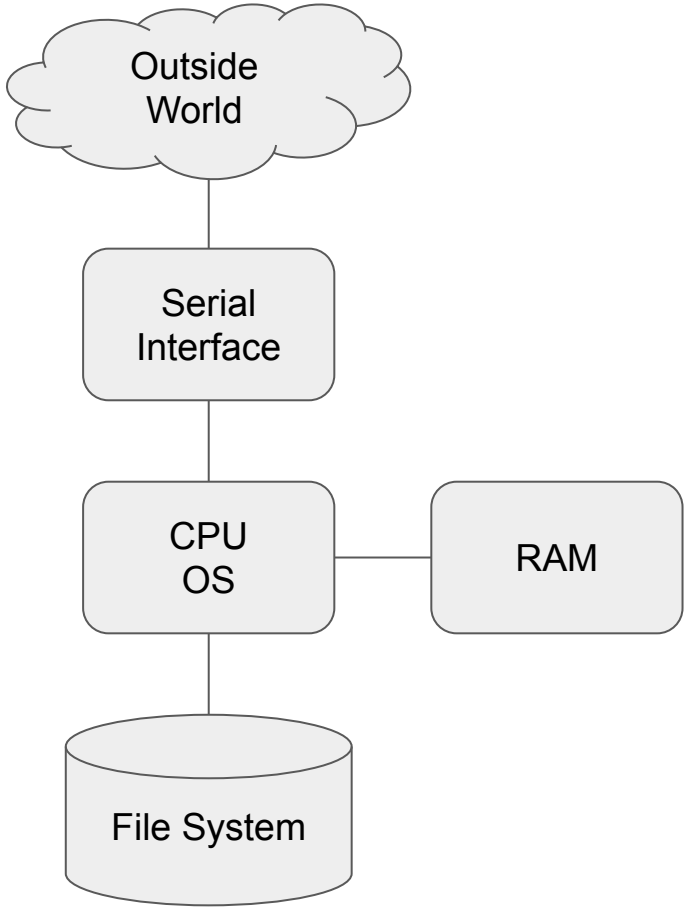


ISO 7816 “smart card”

ISO 7816 defines the smart card, a plastic card with an embedded computer system, containing a microprocessor, RAM, and non-volatile storage. This computer communicates with the outside world through a serial interface. Despite this limited communication channel, it is a full computer, running its own OS.

One of the key features of the basic smart card is that the non-volatile storage is organized into a file system with access controls. For example, some files, once they are written, cannot be read from outside of the card.

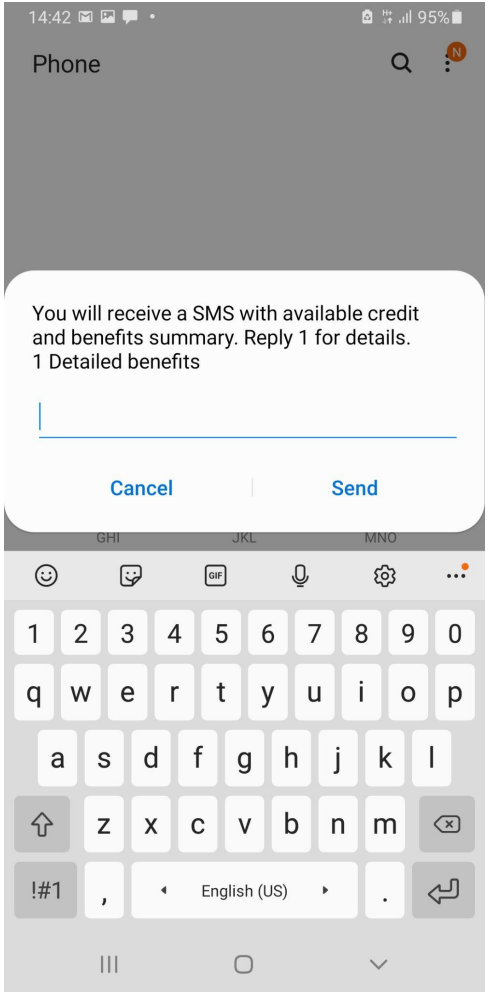
Half of all of the smart cards in the world are SIMs. Most of the SIMs outside of China are made by two companies: Gemalto (Netherlands) and Oberthur (France).



SIM Extensions and the SAT

The SIM Application Toolkit (SAT) is a set of standardized extensions to the Smartcard API that allows the SIM to run complete interactive applications through its host phone, and store and access user-specific records, like contact directories and SMS.

(3GPP 31.111, GSM 11.14)



JavaCards

A JavaCard is an ISO 7816 smart card with a scaled-down Java Virtual Machine (JVM) built into its OS.

The JVM makes it easier to develop SAT-based applications (“applets”). These applets can be loaded and managed remotely via SMS.

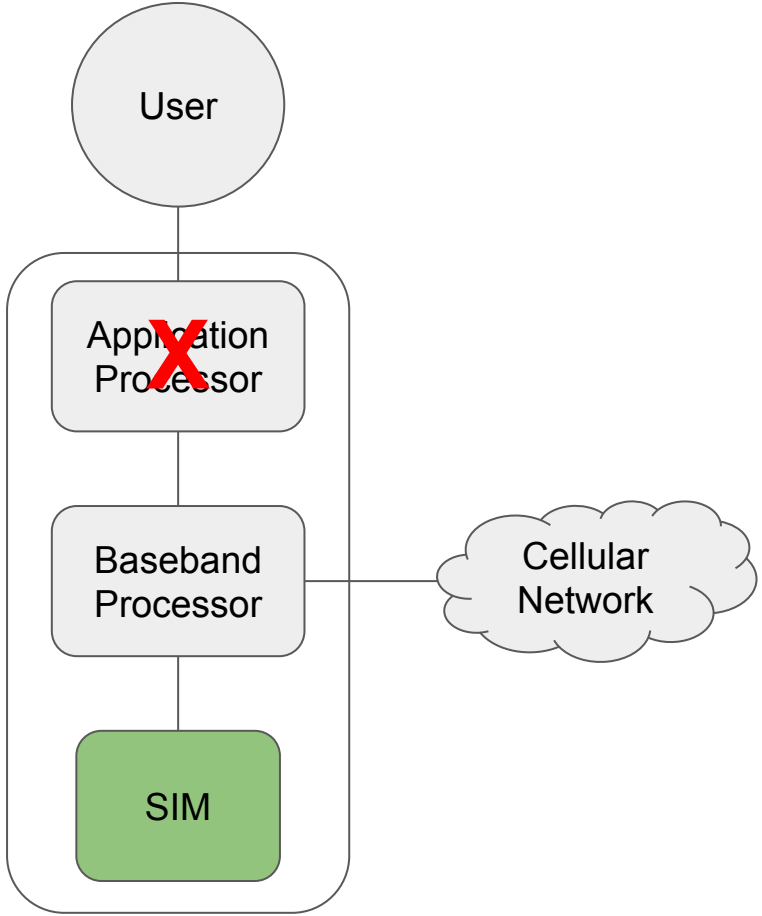
All current SIMs are JavaCards.

How this started

Back in the days of feature phones, there was no application processor, just a keypad and a display.

The SIM was the only general-purpose computing element in the phone.

So operators designed the SIM to control the phone and to host complex applications.

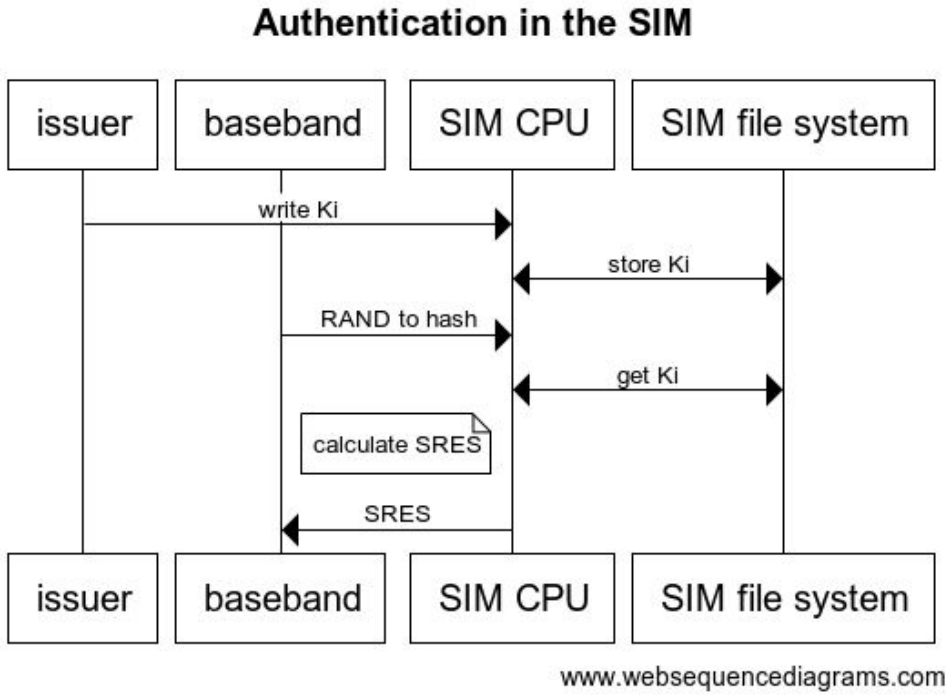


Example of SIM operation

This is the procedure between the phone and SIM when the phone needs to generate an SRES for authentication.

The phone cannot read Ki once it is written. It can only give the SIM CPU a RAND and get back the corresponding SRES.

Any attempt to read the Ki directly will result in a file access failure.

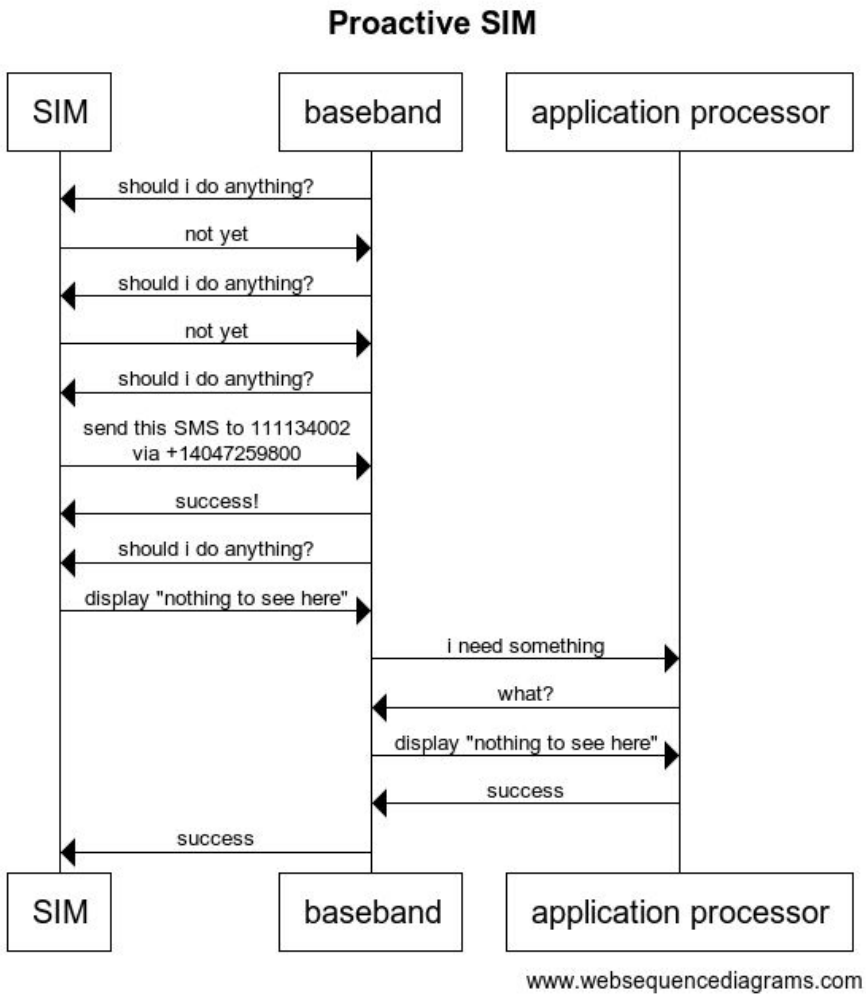


Proactive SIMs

Proactive SIMs can initiate operations for their own reasons, and control the baseband processor and application processor to perform actions, like sending SMS or displaying messages.

To implement this, the baseband polls the SIM every 15-60 seconds asking it if there are any proactive commands.

Nearly all SIMs in the market today are proactive.



What can they do? (GSM 11.14, 3GPP 31.111, Sec 6)

Get event notifications:

- Service changes
- Location updates
- Periodic timers
- On-shot timers
- Call and SMS events
- User active, idle changes

Request information:

- IMEI/SV
- PLMN/LAC/CID
- Timing advance and neighbor measurements
- BCCH neighbor list
- Current time, time zone
- WLAN SSID and status
- Battery level
- GPS location

And remember, the SIM has a real file system and can store this information between uses.

Communicate:

- SMS
- USSD sessions
- TCP data sessions
- UDP datagrams
- Telephone calls, DTMF
- Arbitrary AT commands
- Launch a web browser with a URL

Other than the browser request, this communication bypasses the application processor. Without the the right tools, this activity is totally hidden.

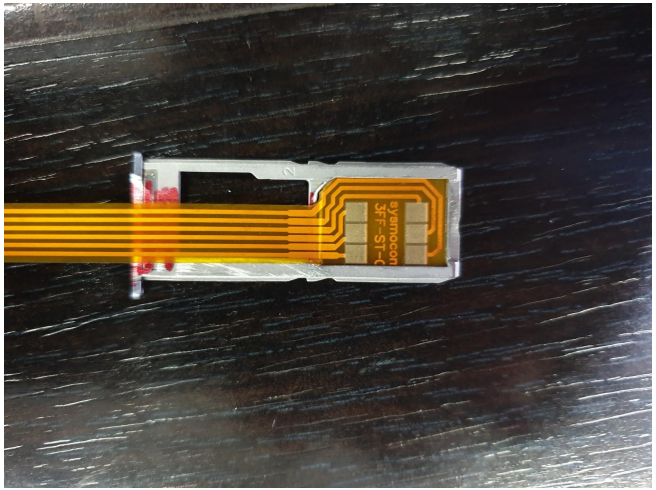
The first case:
What is AT&T doing at 1111340002?

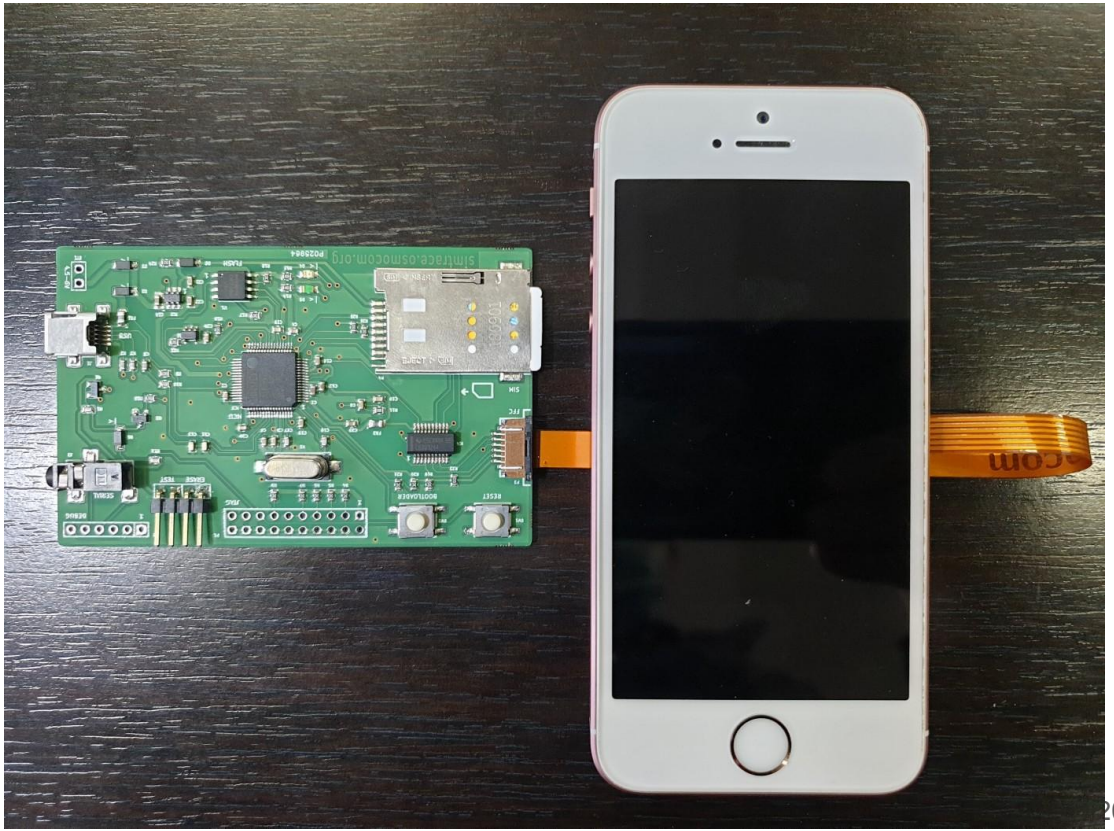
The procedure

Step #1 - Test a SIMS on the bench to form hypotheses

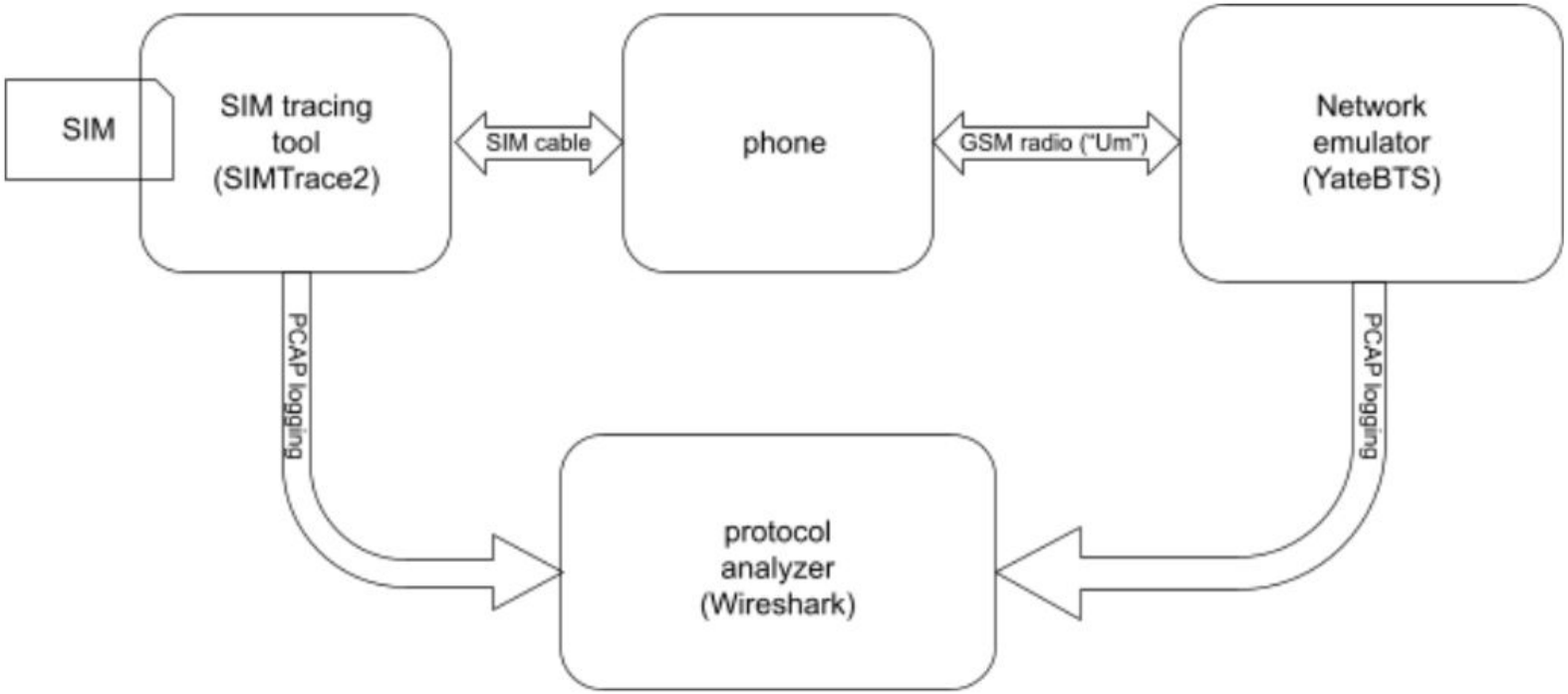
Step #2 - Subpoena to AT&T to verify hypotheses

A Test Bench for Studying Proactive SIMs





A Test Bench for Studying Proactive SIMs



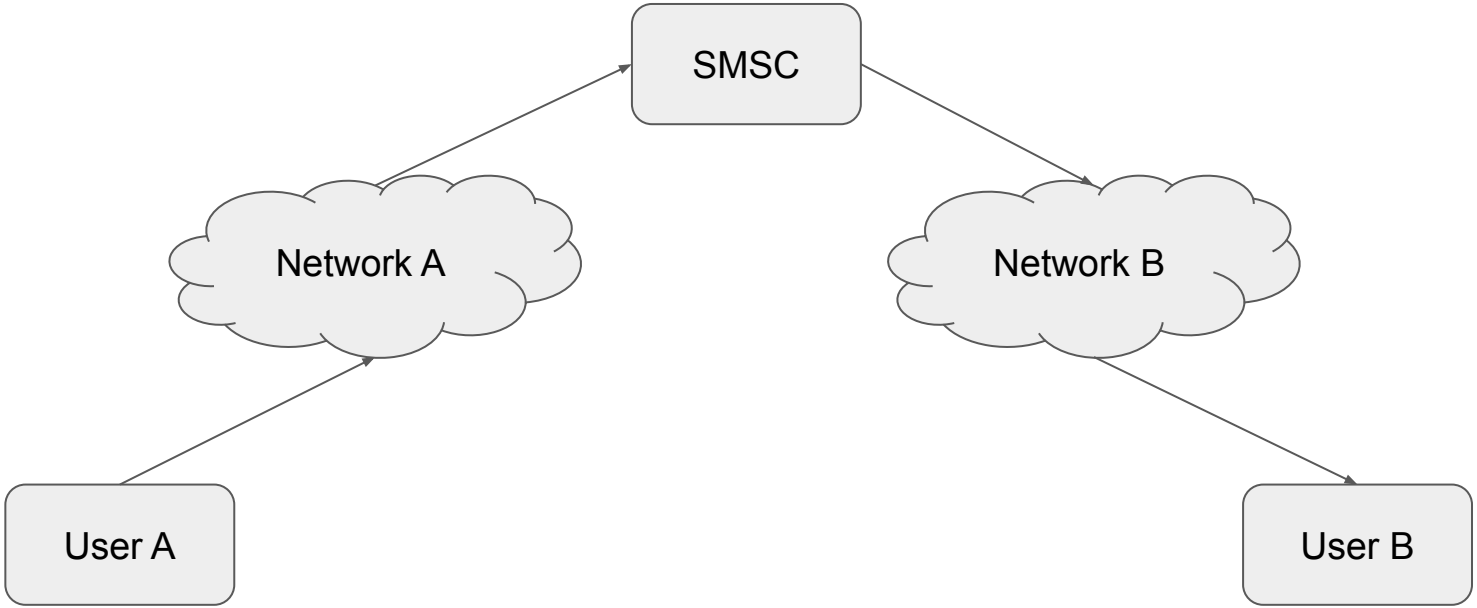
Procedure

1. Configure YaetBTS to mimic AT&T GSM (310-410).
2. Set the SIM in the trace tool.
3. Power up.
4. Watch Wireshark with a filter for GSM SMS.

And …

1. The SIM sets up proactive polling.
2. The SIM repeated requests the IMEISV.
3. The SIM tells the baseband to send SMS.
4. We get the same SMS arriving in YateBTS.

SMS and the CS core network



The AT&T SMS to 1111340002 via +14047259800

- Binary format SMS.
- TLV encoding.
- Encodes IMEISV (current and previous), IMSI, PLMN, LAC, CID, terminal profile.
- Sends this to a special-purpose SMSC inside the AT&T network.
- Triggered by change of IMEISV, either moving to a new phone, or a baseband firmware update.

```
RP-Destination Address - (14047259800)
        Length: 7
        1... .... = Extension: No Extension
        .001 .... = Type of number: International Number (0x1)
        .... 0001 = Numbering plan identification: ISDN/Telephony
Numbering (ITU-T Rec. E.164 / ITU-T Rec. E.163) (0x1)
        Called Party BCD Number: 14047259800
```

```
Reassembled LAPDm (158 bytes):
0000  09 01 9b 00 00 00 07 91 41 40 27 95 08 f0 8f 11   ........A@'.....
0010  00 0a 81 11 11 43 00 20 00 f4 ff 82 ee 01 50 22   .....C. ......P"
0020  09 08 39 01 14 20 95 64 66 89 23 09 ff ff ff ff   ..9.. .df.#.....
0030  ff ff ff ff ff 24 09 33 25 76 03 08 91 23 76 f8   .....$.3%v...#v.
0040  25 20 ff ff ff ff 7f 9f 00 df ff 00 00 1f e2 08   % ..............
0050  11 06 c7 c0 00 00 00 00 40 00 70 02 00 00 00 18   ........@.p.....
0060  61 01 26 10 00 00 00 00 00 00 00 00 00 00 00 00   a.&.............
0070  00 00 00 00 20 0a 98 10 14 40 72 52 49 66 96 98   .... ....@rRIf..
0080  21 07 13 00 14 03 e2 03 e2 27 10 00 00 00 00 00   !........'......
0090  00 00 00 00 00 00 00 00 00 00 00 28 01 00         ...........(..
```

From an IR.21

SCP 1 4047259425 SUN -05:00

SCP 1 4047259431 SUN -05:00

SCP 1 4047259514 SUN -05:00

SCP 1 4047259527 LOGICA -05:00

SCP 1 4047259770 ERICSSON -05:00

SCP 1 4047259800 SUN -05:00

SCP 1 4047259825 ERICSSON -5:00

So now the lawyer sends a subpoena to AT&T demanding documents or witnesses to explain what that SCP at +14047259800 is used for.

AT&T in Deposition

- They avoided the subpoena for a month, but finally produced a witness for deposition.
- Referred to this SMS as a “service change message”.
- Confirmed that the message was triggered by an iOS update that has included a firmware update for the baseband processor.
- Confirmed that the SMS was not related to any particular actions of the user.

Other examples

- T-Mobile USA
  - M2M SMS, ASCII payload
  - unknown purpose
- **Verizon**
  - **TCP/IP sessions**
  - **Port 8334, various IPv4**
- Orange Romania
  - Similar to AT&T

https://telecom-expert.com/proactive-sim-examples/
For links to Pastebins.

Command Type: OPEN CHANNEL (0x40)
Command Qualifier: 0x03
Device identity: 8182
  Source Device ID: SIM / USIM / UICC (0x81)
  Destination Device ID: Terminal (Card Reader) (0x82)
Alpha identifier:
Bearer description: 03
  Bearer Description: default bearer for requested transport layer (0x03)
Buffer size: 058e
  Buffer Size: 1422
Network Access Name: 08767a7761646d696e
  APN: vzwadmin
UICC/terminal interface transport level: 0220fb
  Transport protocol type: TCP, UICC in client mode, remote connection (0x02)
  Transport port: 8443
Other address (data destination address): 213f3706d1
  Coding of Type of address: IPv4 address (0x21)
  IPv4 address: 63.55.6.209

Why should we care?

Why should we care?

1 - Many SIMs have buggy web browser applets.

Why should we care?

1 - Many SIMs have buggy web browser applets.

2 - Governments own telcos.

Why should we care?

1 - Many SIMs have buggy web browser applets.

2 - Governments own telcos.

3 - This activity is totally undocumented otherwise.

An Invitation

david.allen.burgess@gmail.com

Extra slides not included in the final presentation

Segments of a mobile network

Core Network - Where phone calls get connected, where packets get routed to and from the Internet, where SIMs are authenticated, where bills are generated.

Radio Access Network (RAN) - Creates and manages the radio connections between the user terminals and the core.

Transport Network - Connects the RAN to the core. Also called “backhaul”.

User Terminal - Usually, a phone. Also called the Mobile Station (MS) or User Equipment (UE), depending on the generation of technology. The user terminal also contains the SIM, a smartcard that is provided by the operator.

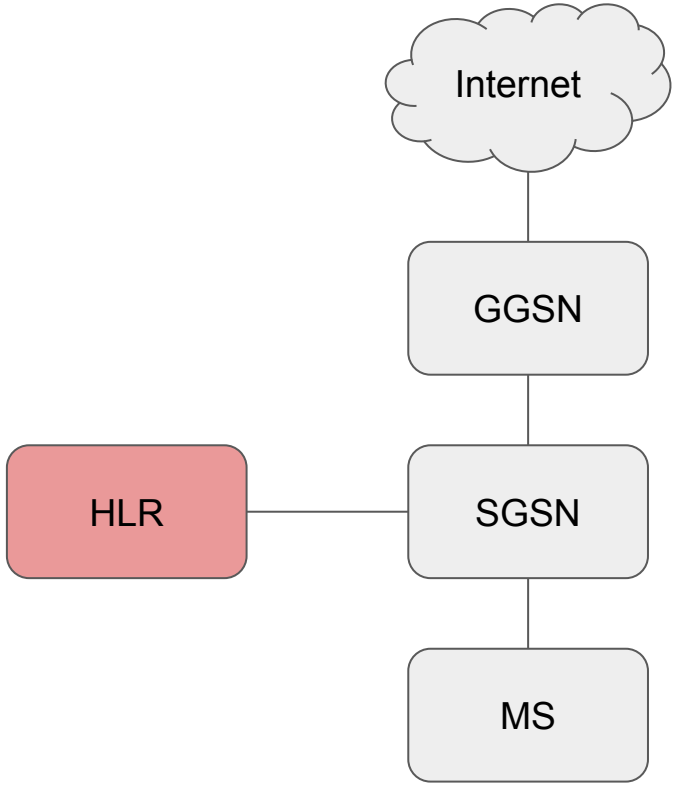
SS7 Network - Connects core networks to each other.

The PS core network (pre-4G: GPRS, UMTS)

Home Location Register (HLR) - The master subscriber database. Holds all customer and SIM data. (Same as for CS.)

Serving GPRS Support Node (SGSN) - Performs mobility management and authentication functions similar to the VLR. Routes IP streams between terminals and GGSNs.

Gateway GPRS Support Node (GGSN) - Connects IP data sessions to the public Internet. Provides a consistent IP address as the phone moves from one cell to another.



The PS core network (4G: SAE, EPC)

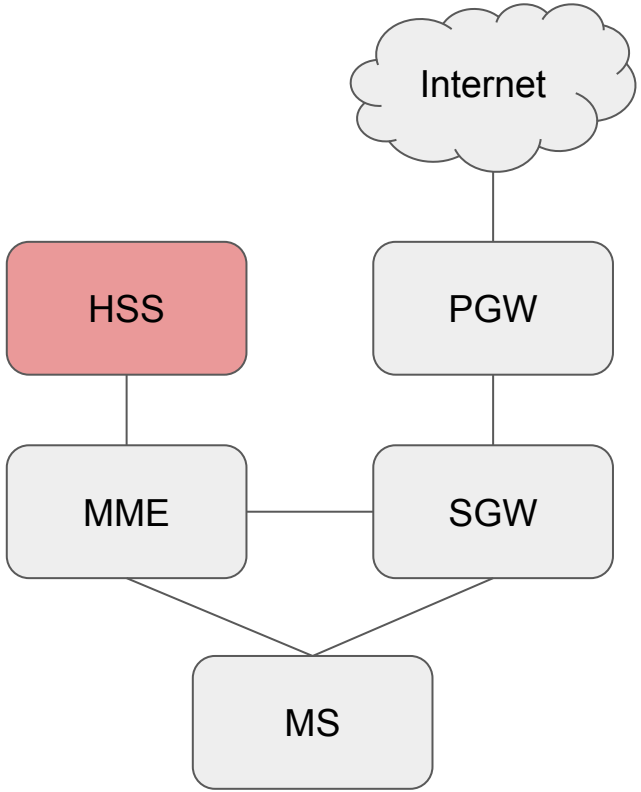
Home Subscriber Server (HSS) - Functionally the same as an HLR, but with different interface protocols.

Mobility Management Entity (MME) - Performs mobility management and authentication functions. Usually clustered, load-balancing.

Serving Gateway (SGW) - Routes IP streams between terminals and PGWs.

(The MME and SGW together fill the role of the SGSN.)

Packet Data Network Gateway (PGW) - Connects IP data sessions to the public Internet. Provides a consistent IP address as the phone moves from one cell to another. Similar to the GGSN.



SMS and the CS core network

But for this webinar, we focus on SMS.

SMS is a store-and-forward service, similar to email.

Unlike many telecom services, it is best-effort only.

Messages to not go directly from user to user, but are delivered to and from a Short Message Service Center (SMSC).

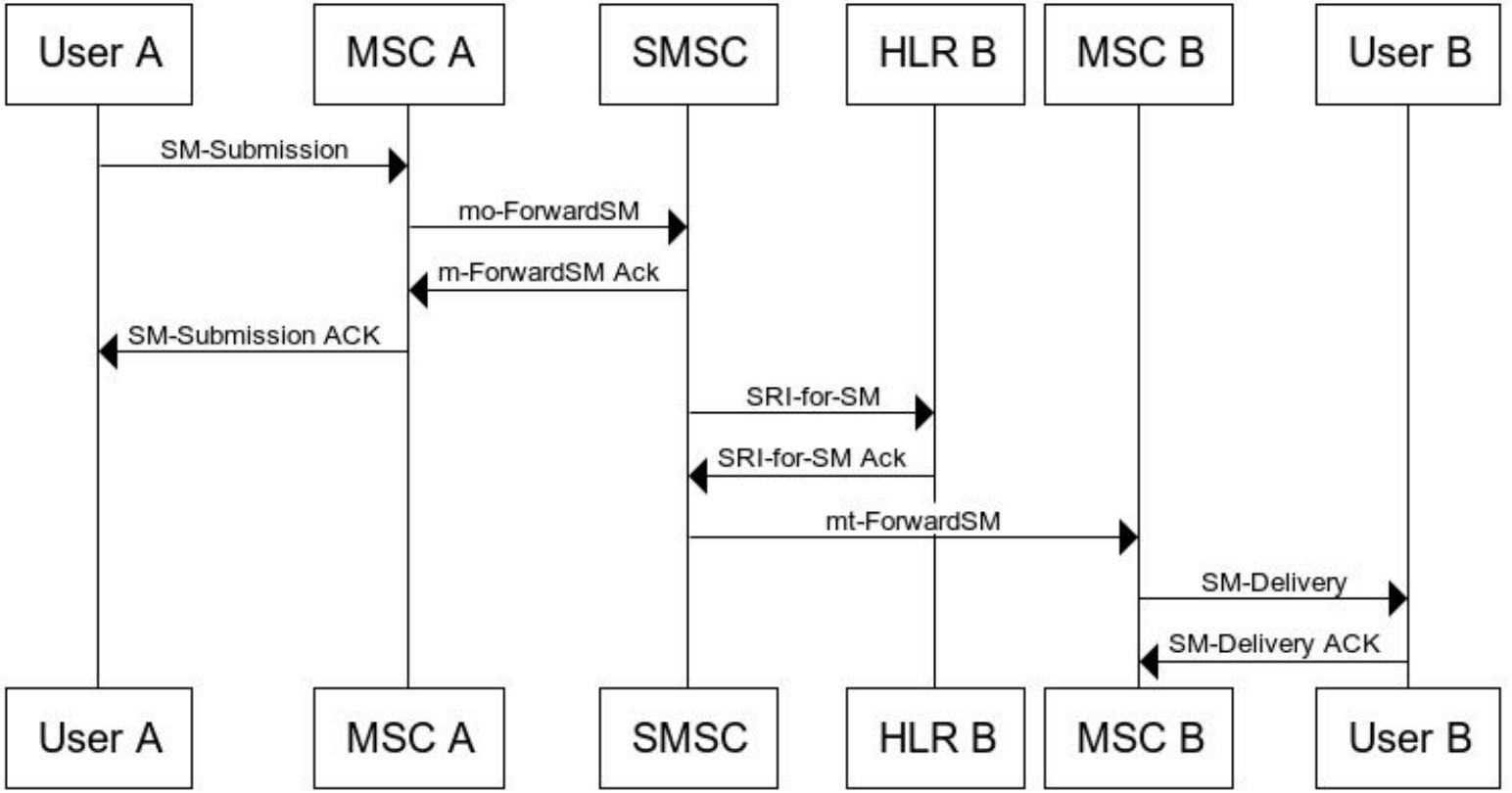
These SMSCs are often contracted out to third parties and do not necessarily run inside the core network, **even though they interact closely with the HLRs and MSC/VLRs**. The security implications here are significant and we will cover them in detail once some other technical background is established.

SMS and the CS core network

Outbound SMS - The mobile sends SMS. (User A to SMSC on previous slide.) User A sends the SMS to the serving MSC (MSC A), which then delivers it to the SMSC. The SMSC address is an E.164 address, just like a telephone number, usually provided by User A's SIM.

Inbound SMS - The network delivers SMS. (SMSC to User B on previous slide.) The final destination address for User B can have many forms, but here we are assuming it is also an E.164 address. The SMSC queries User B's HLR (HLR B) to know the current serving MSC for User B (MSC B). The SMSC then delivers the message to MSC B, which delivers it to User B.

SMS



www.websequencediagrams.com

“Magic” payloads and addresses in SMS

SMS is used for a lot more than just texting, including binary payloads for over-the-air (OTA) updates of the SIM and baseband processor and WAP, a kind of HTTP over SMS.

Some of these SMS payload types present security risks, which we will cover in later sections.

In the figure:

- Yellow highlights the parts that you usually see and control.
- Orange highlights the parts that you never see and usually do not control.