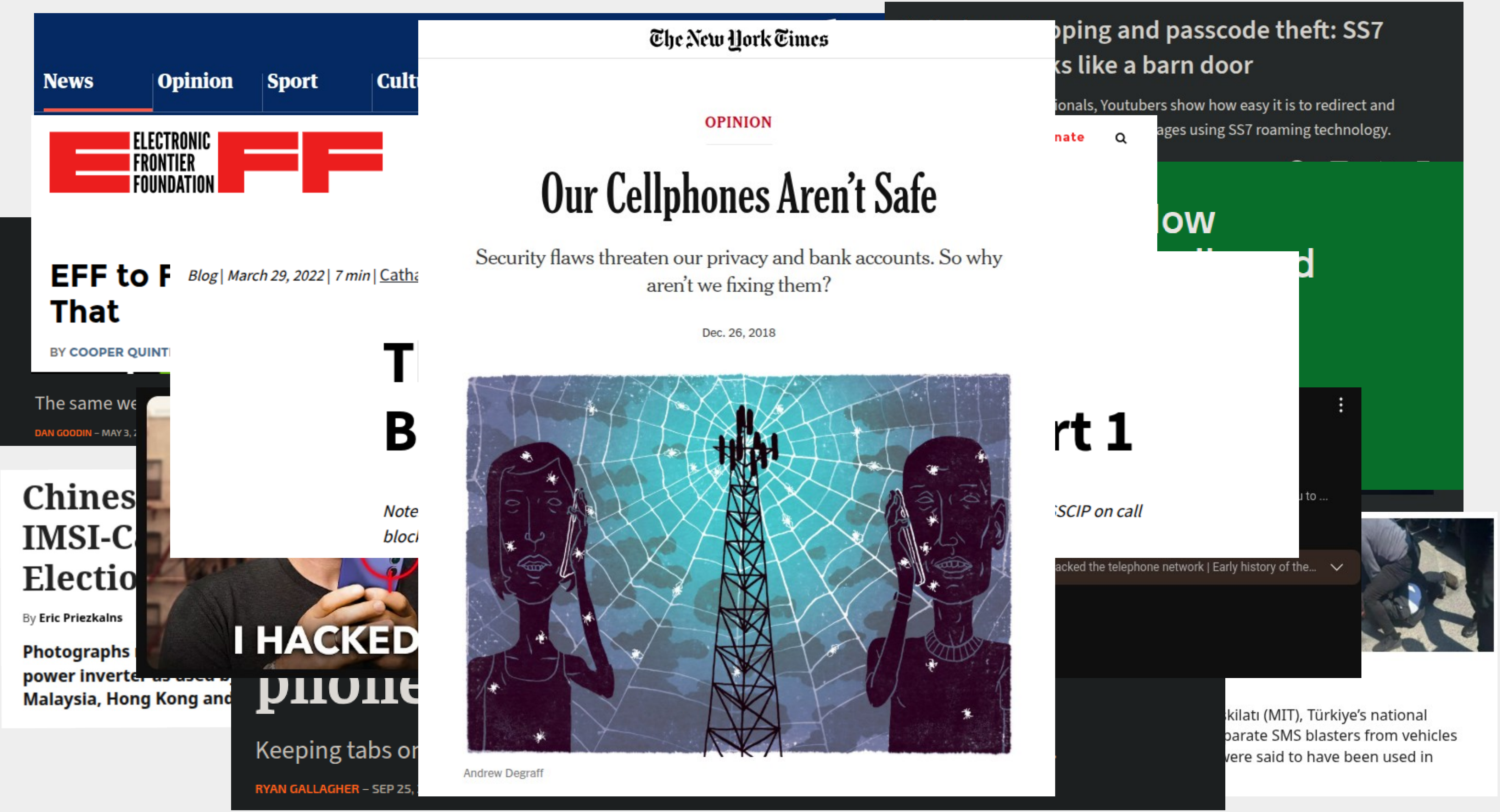
Number of daily placed phone calls	13.5 billion (2021)
Number of daily sent SMS	23-27 billion (2025)
Number of SIM cards that currently exist	9.1 billion (2024)

→ Telecommunication Systems are **very critical infrastructure**

→ But how **secure** are they **really**?

[Sta1],[Sta2],[Sta3]



The New York Times

OPINION

Our Cellphones Aren’t Safe

Security flaws threaten our privacy and bank accounts. So why aren’t we fixing them?

Dec. 26, 2018

Andrew Degraff

News | Opinion | Sport | Cult

ELECTRONIC FRONTIER FOUNDATION

EFF to F

That

Blog | March 29, 2022 | 7 min | Catha

BY COOPER QUINT

The same we

DAN GOODIN – MAY 3, 2

Chines
IMSI-C
Electio

By Eric Priezkalns

Photographs
power inverter
Malaysia, Hong Kong and

I HACKED
phone

Keeping tabs on

RYAN GALLAGHER – SEP 25,

T
B

Note
block

ping and passcode theft: SS7
s like a barn door

ionals, Youtubers show how easy it is to redirect and
ages using SS7 roaming technology.

nate

low
d

rt 1

SCIP on call

u to ...

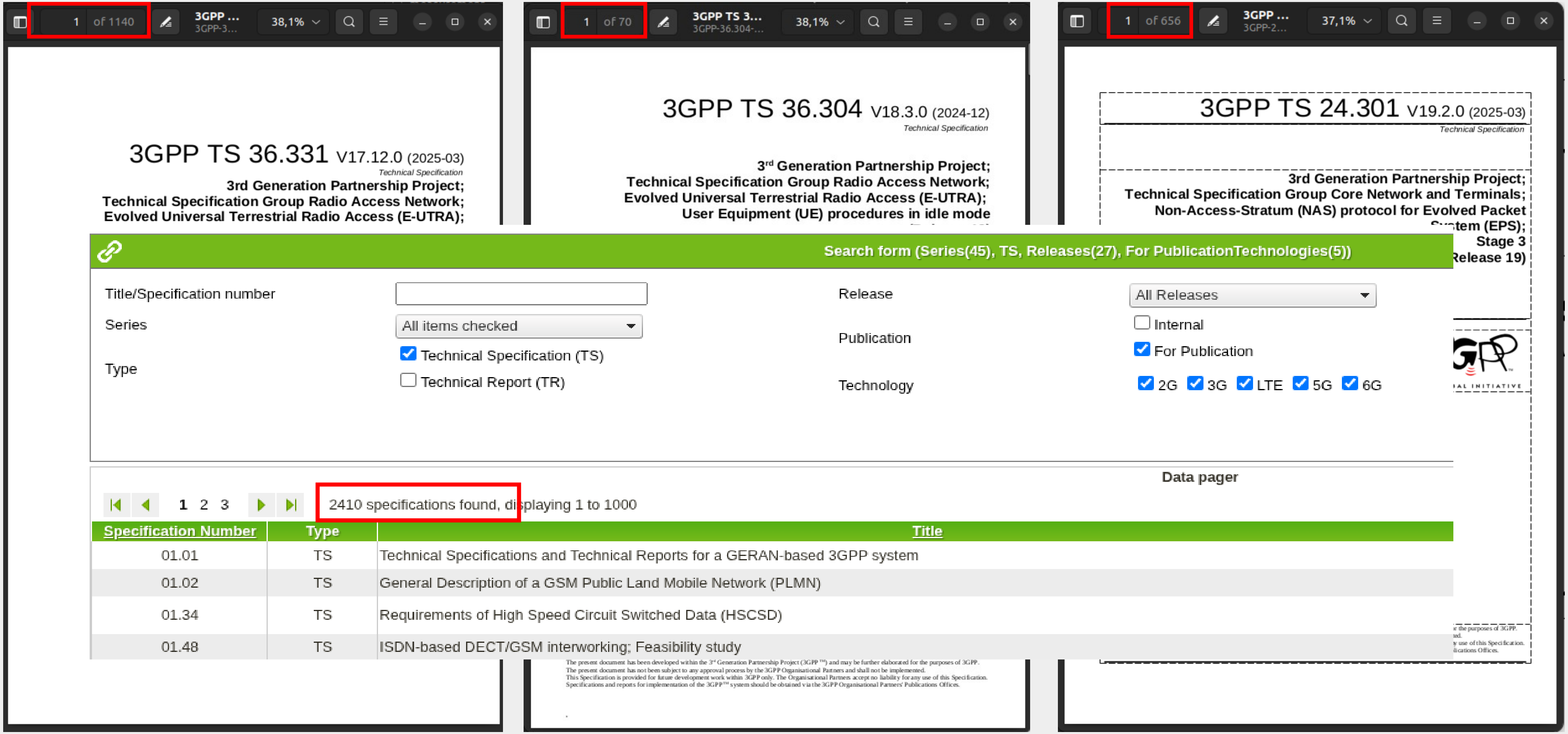
acked the telephone network | Early history of the...

kilatı (MIT), Türkiye’s national
parate SMS blasters from vehicles
were said to have been used in

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Tizian Seehaus

From GSM to 5G: Analyzing the Evolving Security Landscape of Mobile Telecommunication System(s)



3GPP TS 36.331 V17.12.0 (2025-03)
Technical Specification
3rd Generation Partnership Project;
Technical Specification Group Radio Access Network;
Evolved Universal Terrestrial Radio Access (E-UTRA);

3GPP TS 36.304 V18.3.0 (2024-12)
Technical Specification
3rd Generation Partnership Project;
Technical Specification Group Radio Access Network;
Evolved Universal Terrestrial Radio Access (E-UTRA);
User Equipment (UE) procedures in idle mode

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

3GPP TS 24.301 V19.2.0 (2025-03)
Technical Specification
3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
Non-Access-Stratum (NAS) protocol for Evolved Packet
System (EPS);
Stage 3
Release 19)

Search form (Series(45), TS, Releases(27), For PublicationTechnologies(5))

Title/Specification number

Series: All items checked

Type: ☑ Technical Specification (TS) ☐ Technical Report (TR)

Release: All Releases

Publication: ☐ Internal ☑ For Publication

Technology: ☑ 2G ☑ 3G ☑ LTE ☑ 5G ☑ 6G

Data pager

1 2 3 2410 specifications found, displaying 1 to 1000

Specification Number	Type	Title
01.01	TS	Technical Specifications and Technical Reports for a GERAN-based 3GPP system
01.02	TS	General Description of a GSM Public Land Mobile Network (PLMN)
01.34	TS	Requirements of High Speed Circuit Switched Data (HSCSD)
01.48	TS	ISDN-based DECT/GSM interworking; Feasibility study

→ The Mobile Telecommunication Landscape is **huge** and **complex**.

[3GP]

What this Talk is and isn’t

Is	Isn’t
• Overview of Security in Mobile Telecommunication • Simplified version of Key Concepts • Look at higher layers that are important to security	• Full technical walkthrough of Mobile Telecommunication • Fully technically correct • Explanation of physical layers such as radio frequency modulation/demodulation, encoding/decoding of frames/subframes, etc.

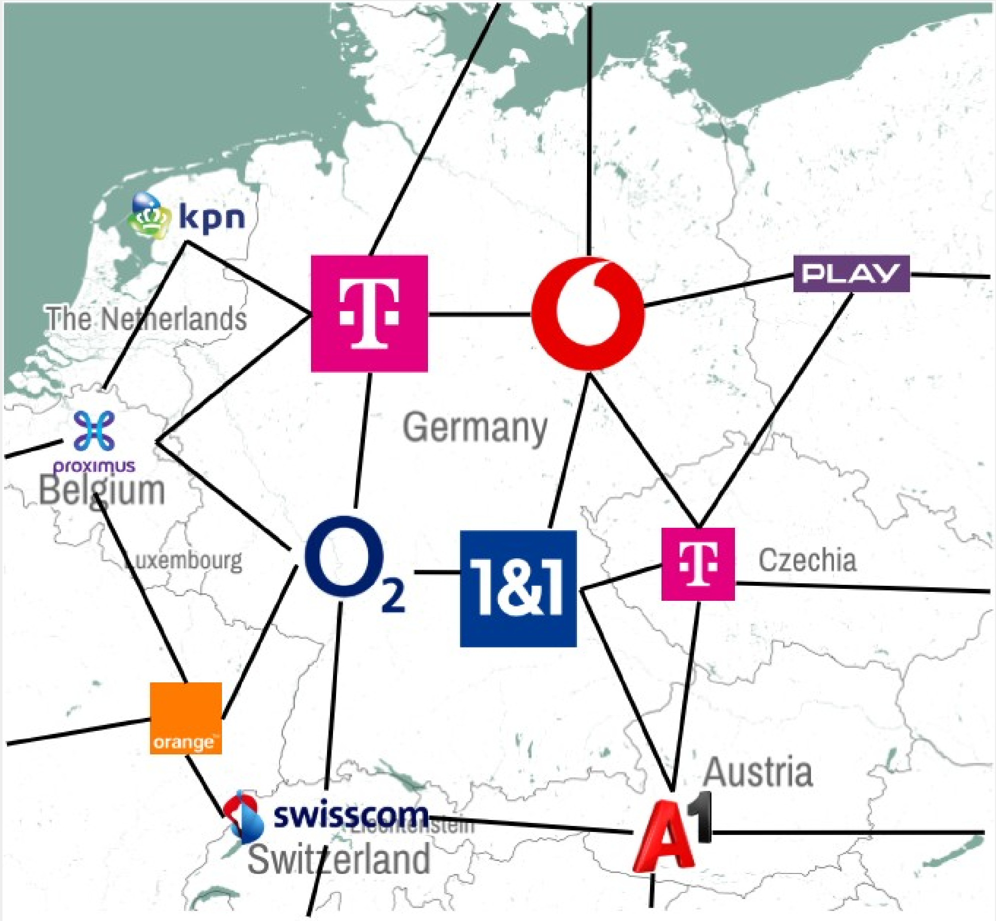
→ This talk should be **fun** and **informative** !

Outline

1. Overview
2. Attack Surface #1: User Equipment
3. Attack Surface #2: RF + Base-Stations
4. Attack Surface #3: Core Network
5. Conclusion

Overview

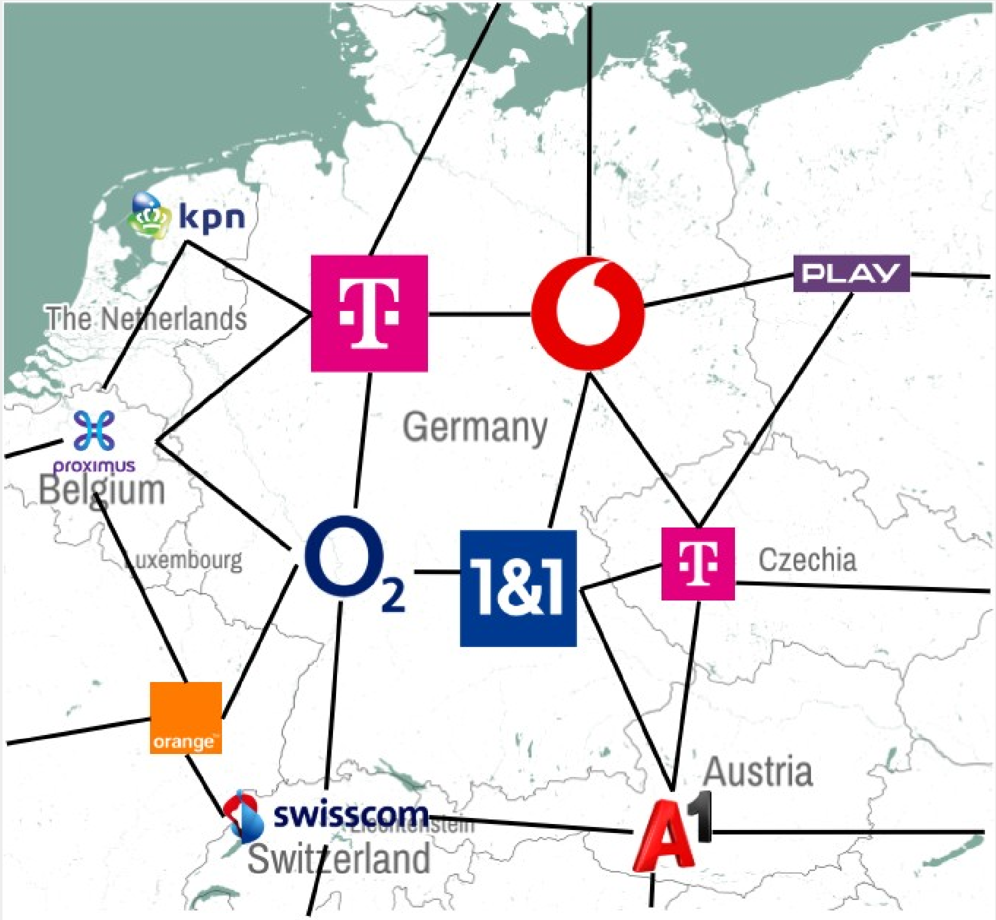
Mobile Telecommunication Landscape



- **Global** Network of Operators/Carrier
- Each operator can host one or more **PLMN** (Public Land Mobile Network)
- Every **PLMN** has it’s own **identifier**.
- **MCC** = “Mobile Country Code”
- **MNC** = “Mobile Network Code”

PLMN	MCC	MNC
Telekom Germany	262	01,06,...
o2 Germany	262	03,05,...
KPN Netherlands	204	08,10,...
Orange France	208	01,02,...
Telekom Czech	230	01,07,...

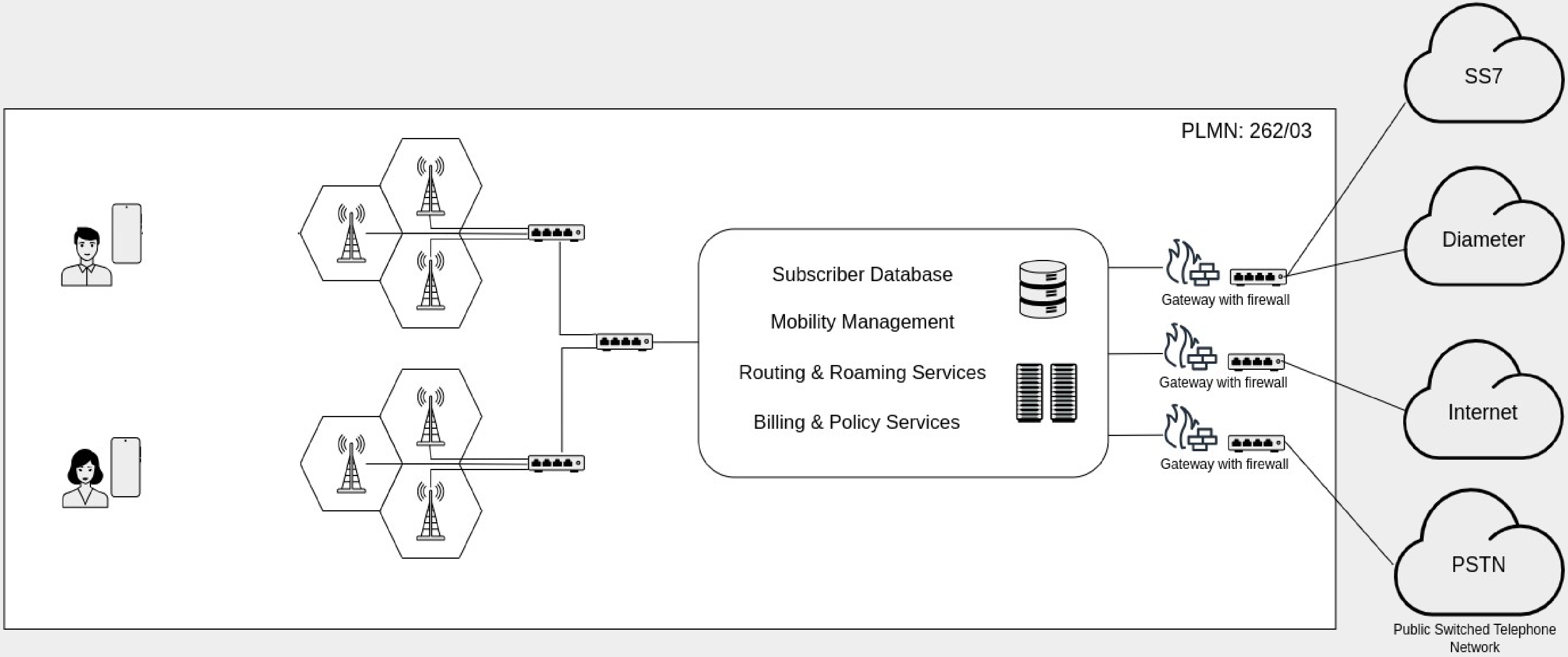
Mobile Telecommunication Landscape



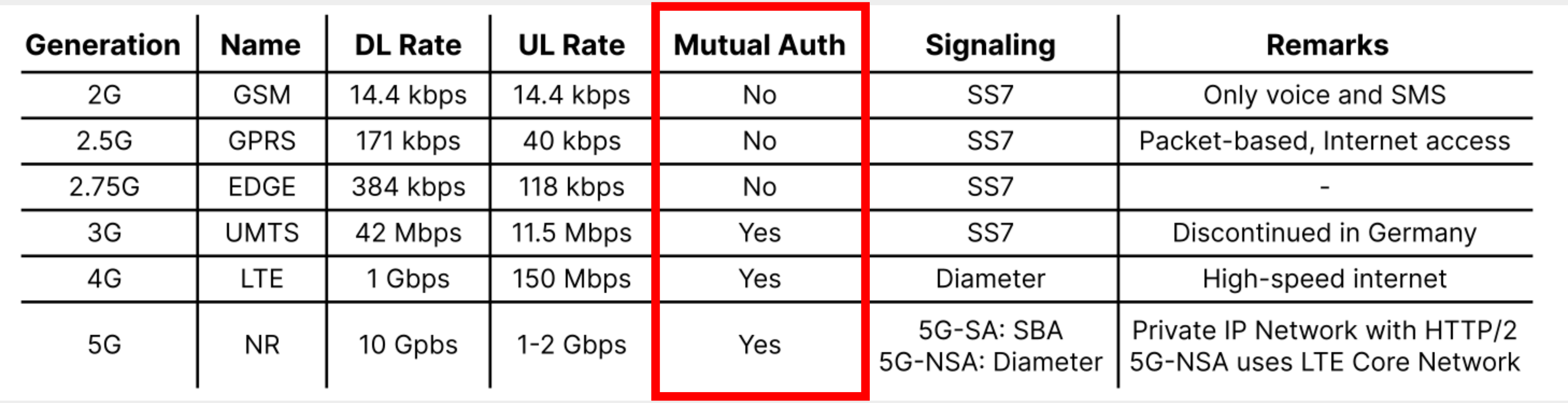
- **PLMNs** are **connected** through **distinct networks**:
  - Data/Voice lines (PSTN)
  - Signaling/Routing lines (SS7,...)

→ PLMNs / operators can **talk to each other** on these networks.

Mobile Telecommunication Landscape

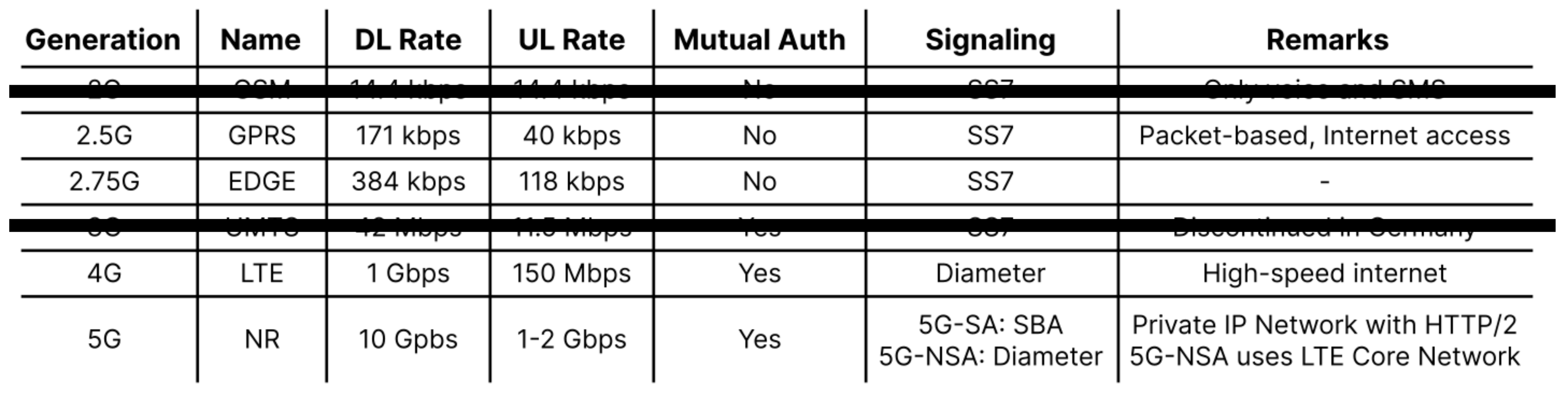


Evolving Mobile Telecommunication Landscape



Generation	Name	DL Rate	UL Rate	Mutual Auth	Signaling	Remarks
2G	GSM	14.4 kbps	14.4 kbps	No	SS7	Only voice and SMS
2.5G	GPRS	171 kbps	40 kbps	No	SS7	Packet-based, Internet access
2.75G	EDGE	384 kbps	118 kbps	No	SS7	-
3G	UMTS	42 Mbps	11.5 Mbps	Yes	SS7	Discontinued in Germany
4G	LTE	1 Gbps	150 Mbps	Yes	Diameter	High-speed internet
5G	NR	10 Gpbs	1-2 Gbps	Yes	5G-SA: SBA 5G-NSA: Diameter	Private IP Network with HTTP/2 5G-NSA uses LTE Core Network

Evolving Mobile Telecommunication Landscape



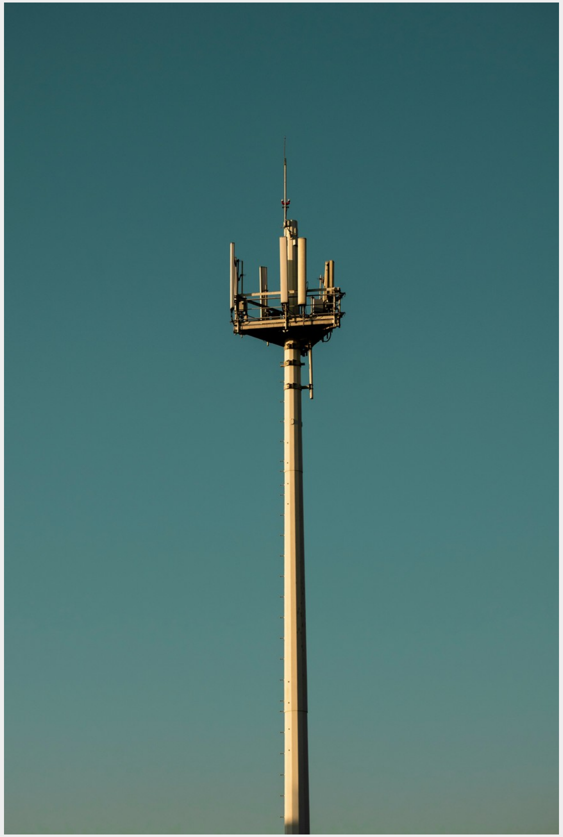
Generation	Name	DL Rate	UL Rate	Mutual Auth	Signaling	Remarks
~~2G~~	~~GSM~~	~~14.4 kbps~~	~~14.4 kbps~~	~~No~~	~~SS7~~	~~Only voice and SMS~~
2.5G	GPRS	171 kbps	40 kbps	No	SS7	Packet-based, Internet access
2.75G	EDGE	384 kbps	118 kbps	No	SS7	-
~~3G~~	~~UMTS~~	~~42 Mbps~~	~~11.5 Mbps~~	~~Yes~~	~~SS7~~	~~Discontinued in Germany~~
4G	LTE	1 Gbps	150 Mbps	Yes	Diameter	High-speed internet
5G	NR	10 Gpbs	1-2 Gbps	Yes	5G-SA: SBA 5G-NSA: Diameter	Private IP Network with HTTP/2 5G-NSA uses LTE Core Network

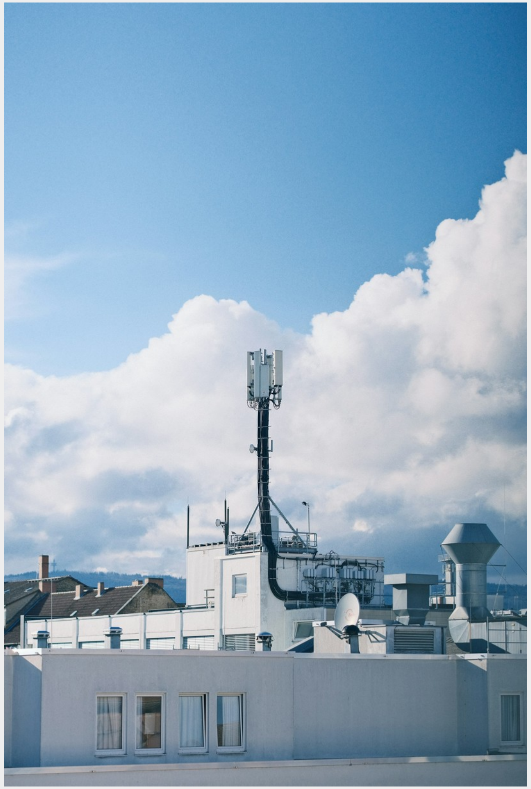
- UMTS is discontinued in Germany. GSM probably as well.

[redacted]

My phone using the GPRS Generation for ~5 seconds before switching to EDGE

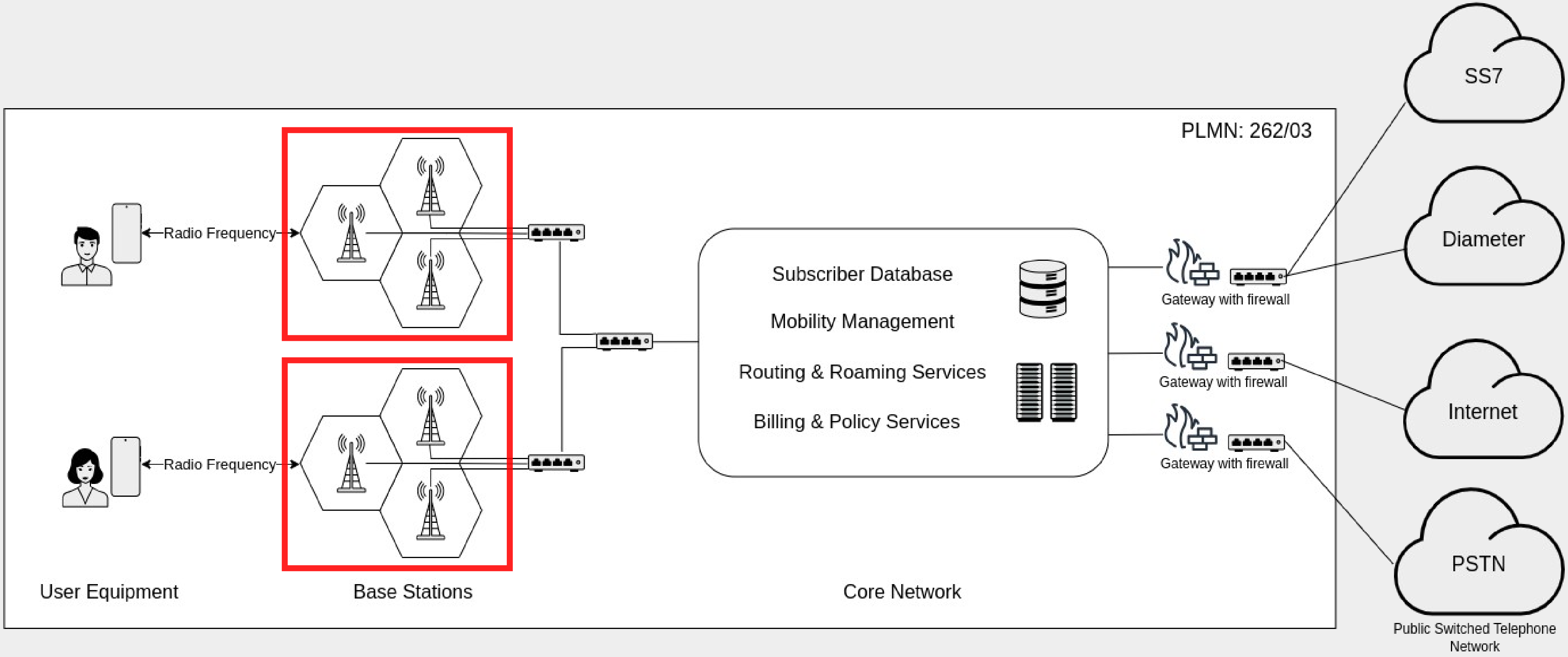
What are Base Stations



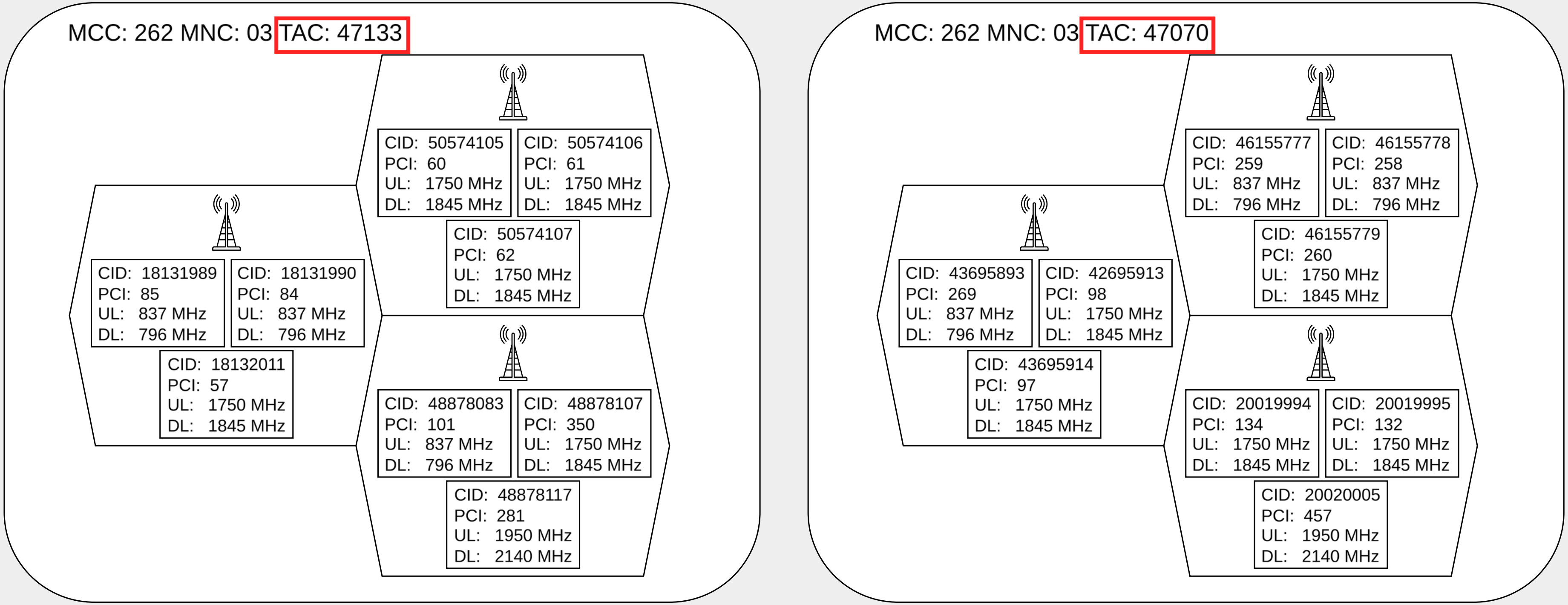


[images from unsplash,freepik]

Tracking Areas



Tracking Areas



MCC: 262 MNC: 03 TAC: 47133

CID: 50574105
PCI: 60
UL: 1750 MHz
DL: 1845 MHz

CID: 50574106
PCI: 61
UL: 1750 MHz
DL: 1845 MHz

CID: 50574107
PCI: 62
UL: 1750 MHz
DL: 1845 MHz

CID: 18131989
PCI: 85
UL: 837 MHz
DL: 796 MHz

CID: 18131990
PCI: 84
UL: 837 MHz
DL: 796 MHz

CID: 18132011
PCI: 57
UL: 1750 MHz
DL: 1845 MHz

CID: 48878083
PCI: 101
UL: 837 MHz
DL: 796 MHz

CID: 48878107
PCI: 350
UL: 1750 MHz
DL: 1845 MHz

CID: 48878117
PCI: 281
UL: 1950 MHz
DL: 2140 MHz

MCC: 262 MNC: 03 TAC: 47070

CID: 46155777
PCI: 259
UL: 837 MHz
DL: 796 MHz

CID: 46155778
PCI: 258
UL: 837 MHz
DL: 796 MHz

CID: 46155779
PCI: 260
UL: 1750 MHz
DL: 1845 MHz

CID: 43695893
PCI: 269
UL: 837 MHz
DL: 796 MHz

CID: 42695913
PCI: 98
UL: 1750 MHz
DL: 1845 MHz

CID: 43695914
PCI: 97
UL: 1750 MHz
DL: 1845 MHz

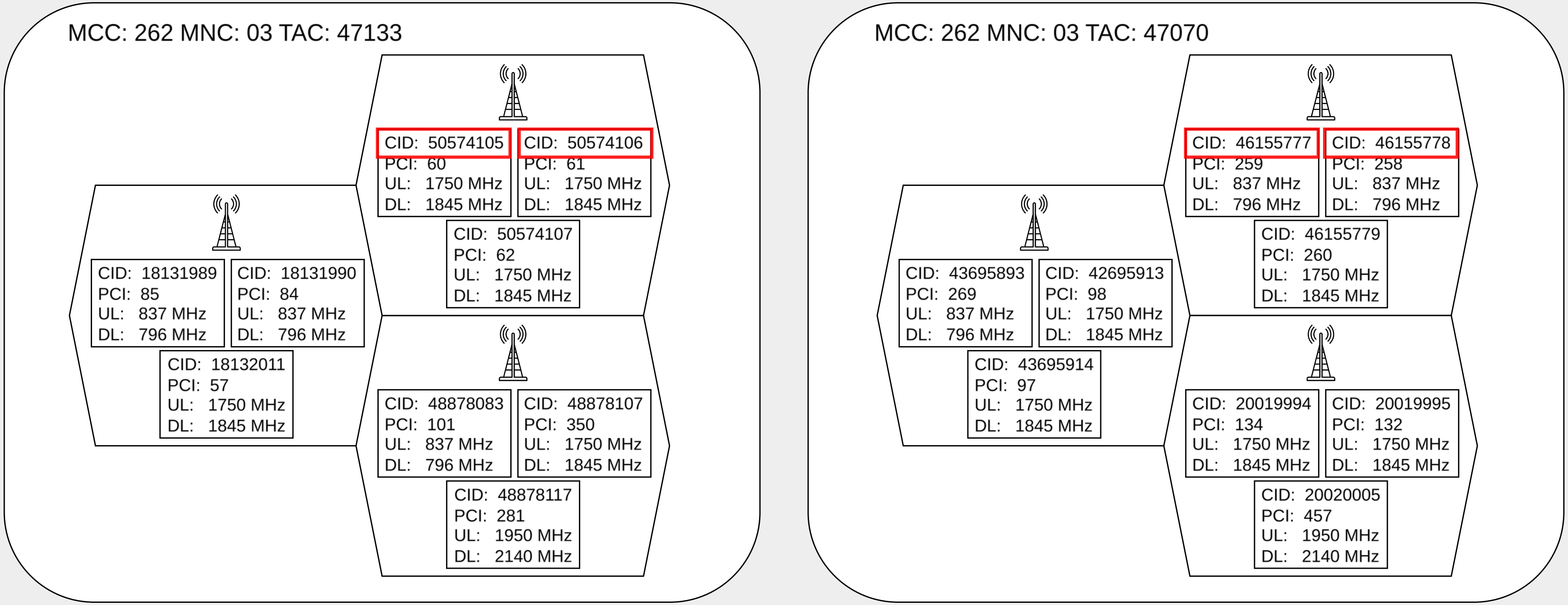
CID: 20019994
PCI: 134
UL: 1750 MHz
DL: 1845 MHz

CID: 20019995
PCI: 132
UL: 1750 MHz
DL: 1845 MHz

CID: 20020005
PCI: 457
UL: 1950 MHz
DL: 2140 MHz

- **Group of cells** inside a geographic location in which the UE does **not need to report** a **location update** to the core network if it’s in **IDLE mode**.
- Reduces radio-frequency and core-network load if UE is in **IDLE mode**.

Cell Identifier (CID)



MCC: 262 MNC: 03 TAC: 47133

CID: 50574105
PCI: 60
UL: 1750 MHz
DL: 1845 MHz

CID: 50574106
PCI: 61
UL: 1750 MHz
DL: 1845 MHz

CID: 50574107
PCI: 62
UL: 1750 MHz
DL: 1845 MHz

CID: 18131989
PCI: 85
UL: 837 MHz
DL: 796 MHz

CID: 18131990
PCI: 84
UL: 837 MHz
DL: 796 MHz

CID: 18132011
PCI: 57
UL: 1750 MHz
DL: 1845 MHz

CID: 48878083
PCI: 101
UL: 837 MHz
DL: 796 MHz

CID: 48878107
PCI: 350
UL: 1750 MHz
DL: 1845 MHz

CID: 48878117
PCI: 281
UL: 1950 MHz
DL: 2140 MHz

MCC: 262 MNC: 03 TAC: 47070

CID: 46155777
PCI: 259
UL: 837 MHz
DL: 796 MHz

CID: 46155778
PCI: 258
UL: 837 MHz
DL: 796 MHz

CID: 46155779
PCI: 260
UL: 1750 MHz
DL: 1845 MHz

CID: 43695893
PCI: 269
UL: 837 MHz
DL: 796 MHz

CID: 42695913
PCI: 98
UL: 1750 MHz
DL: 1845 MHz

CID: 43695914
PCI: 97
UL: 1750 MHz
DL: 1845 MHz

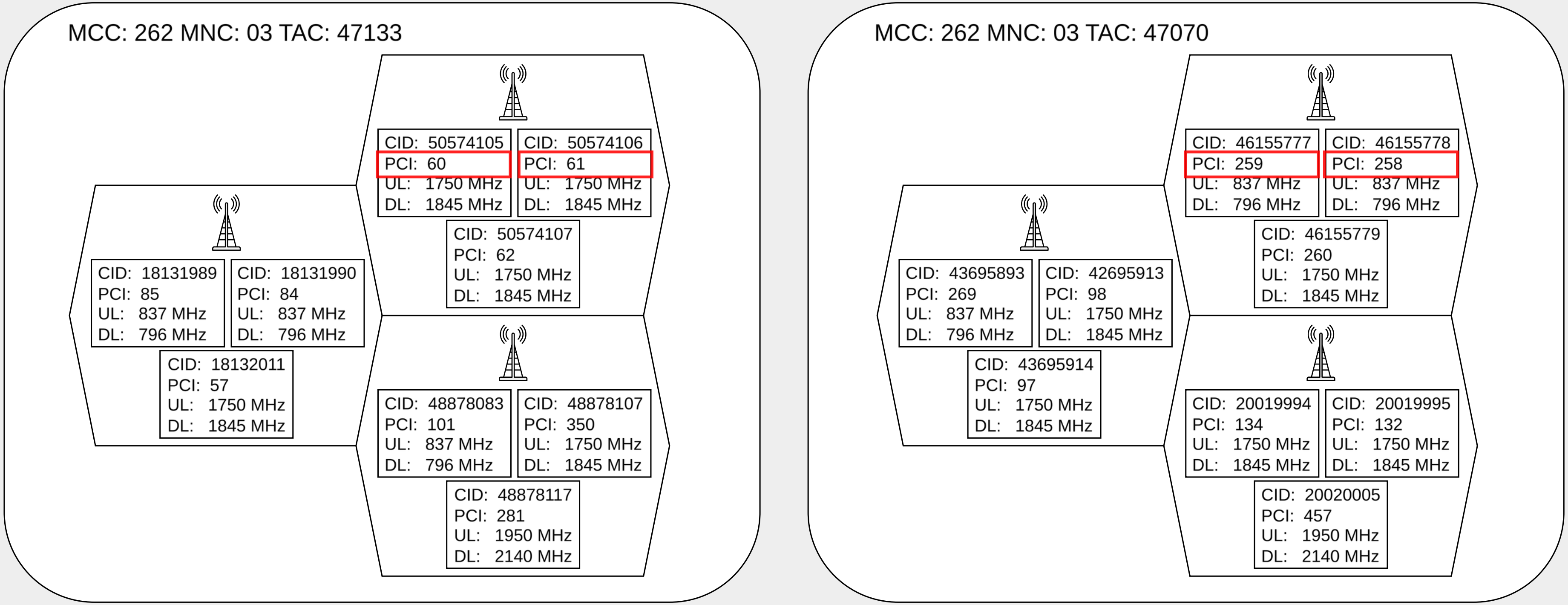
CID: 20019994
PCI: 134
UL: 1750 MHz
DL: 1845 MHz

CID: 20019995
PCI: 132
UL: 1750 MHz
DL: 1845 MHz

CID: 20020005
PCI: 457
UL: 1950 MHz
DL: 2140 MHz

- **PLMN-wide** unique **identifier** for a single cell.
- Used for identification on the **core network layers**.

Physical Cell Identifier (PCI)



MCC: 262 MNC: 03 TAC: 47133

CID: 50574105
PCI: 60
UL: 1750 MHz
DL: 1845 MHz

CID: 50574106
PCI: 61
UL: 1750 MHz
DL: 1845 MHz

CID: 50574107
PCI: 62
UL: 1750 MHz
DL: 1845 MHz

CID: 18131989
PCI: 85
UL: 837 MHz
DL: 796 MHz

CID: 18131990
PCI: 84
UL: 837 MHz
DL: 796 MHz

CID: 18132011
PCI: 57
UL: 1750 MHz
DL: 1845 MHz

CID: 48878083
PCI: 101
UL: 837 MHz
DL: 796 MHz

CID: 48878107
PCI: 350
UL: 1750 MHz
DL: 1845 MHz

CID: 48878117
PCI: 281
UL: 1950 MHz
DL: 2140 MHz

MCC: 262 MNC: 03 TAC: 47070

CID: 46155777
PCI: 259
UL: 837 MHz
DL: 796 MHz

CID: 46155778
PCI: 258
UL: 837 MHz
DL: 796 MHz

CID: 46155779
PCI: 260
UL: 1750 MHz
DL: 1845 MHz

CID: 43695893
PCI: 269
UL: 837 MHz
DL: 796 MHz

CID: 42695913
PCI: 98
UL: 1750 MHz
DL: 1845 MHz

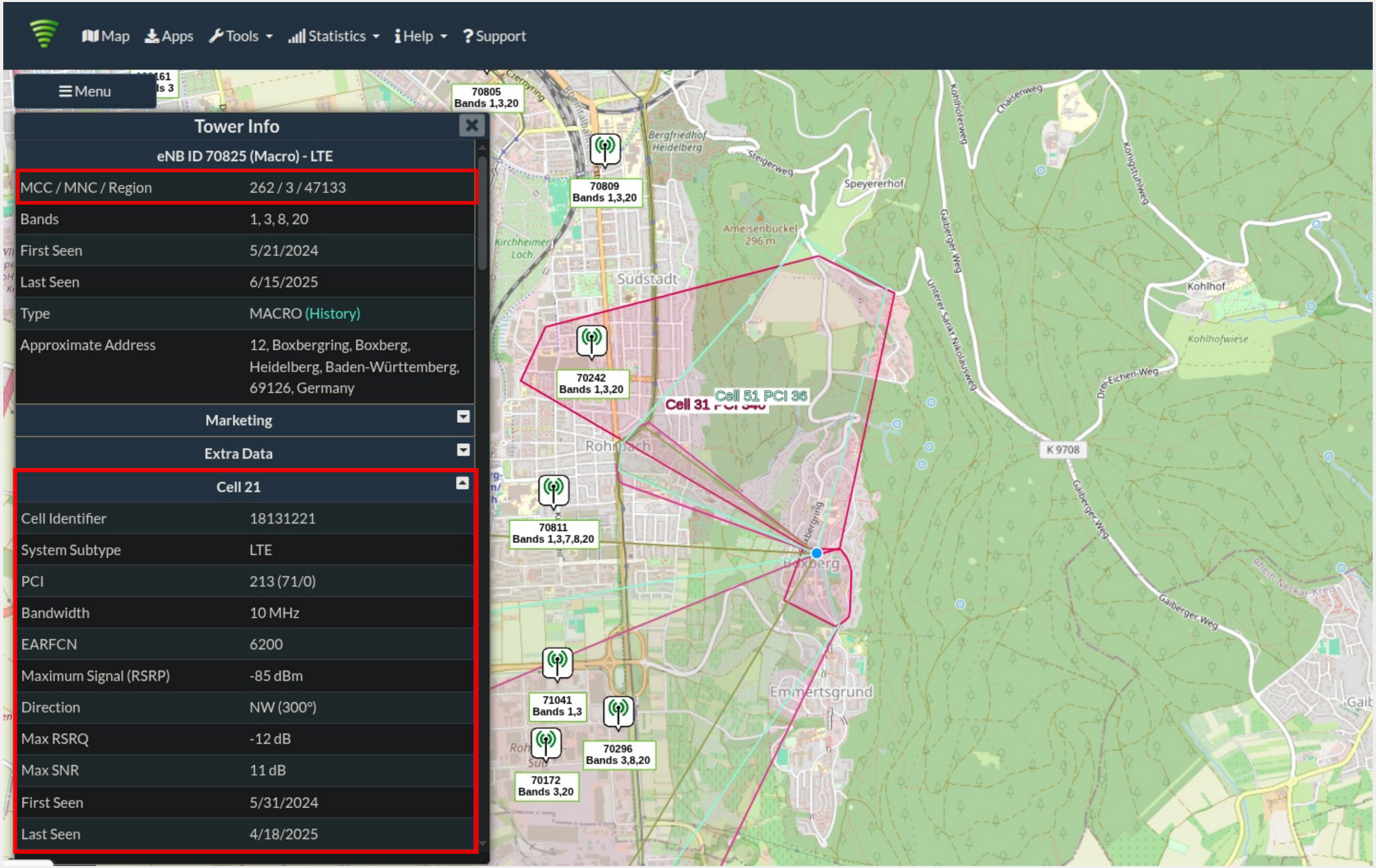
CID: 43695914
PCI: 97
UL: 1750 MHz
DL: 1845 MHz

CID: 20019994
PCI: 134
UL: 1750 MHz
DL: 1845 MHz

CID: 20019995
PCI: 132
UL: 1750 MHz
DL: 1845 MHz

CID: 20020005
PCI: 457
UL: 1950 MHz
DL: 2140 MHz

- Identifier for a single cell that is **unique** within a **limited geographic area**.
- Can be **reused** inside the same PLMN.
- Used for identification on the **physical/radio-frequency layers**.



Tower Info

eNB ID 70825 (Macro) - LTE

MCC / MNC / Region	262 / 3 / 47133
Bands	1, 3, 8, 20
First Seen	5/21/2024
Last Seen	6/15/2025
Type	MACRO (History)
Approximate Address	12, Boxbergring, Boxberg, Heidelberg, Baden-Württemberg, 69126, Germany

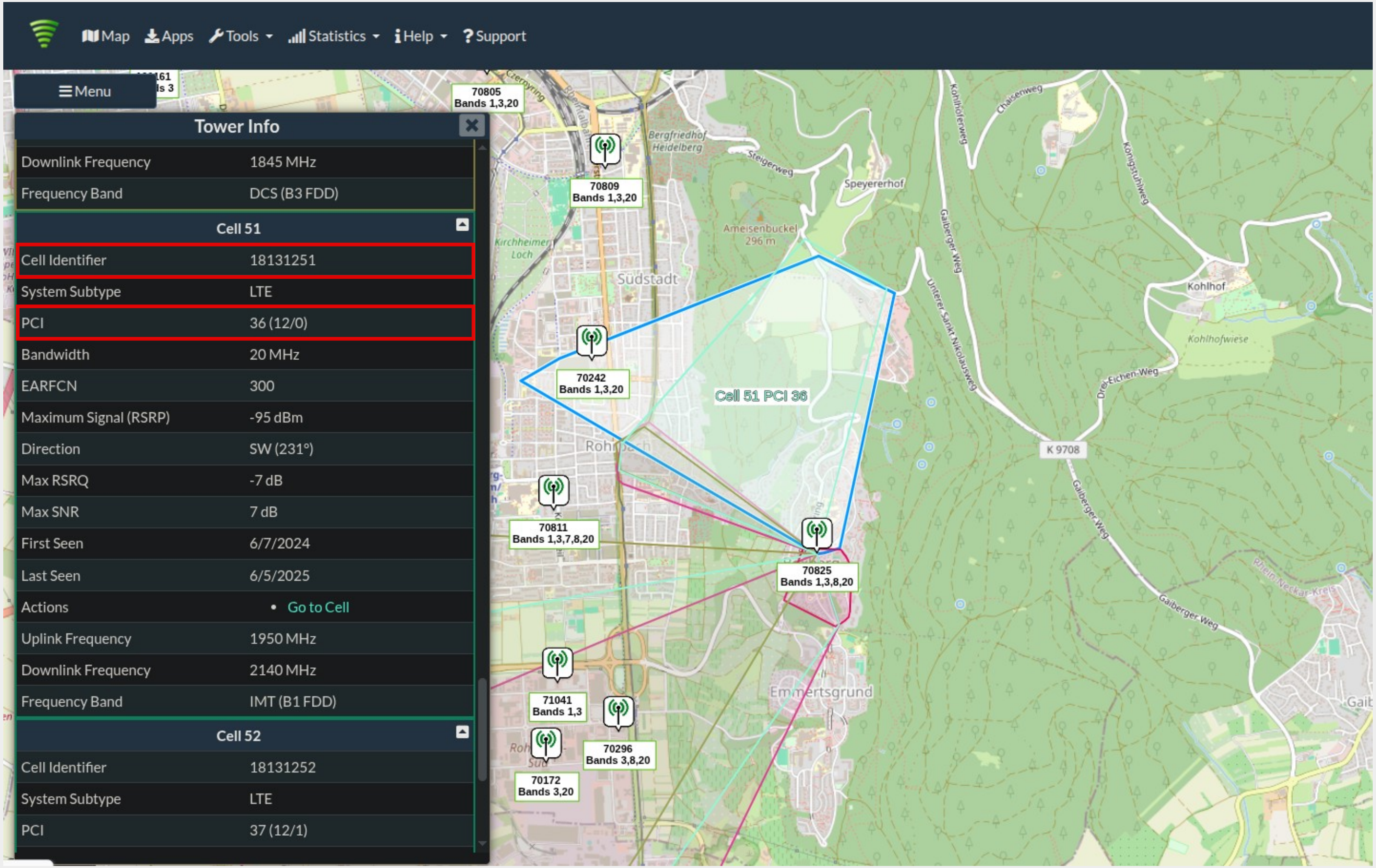
Marketing

Extra Data

Cell 21

Cell Identifier	18131221
System Subtype	LTE
PCI	213 (71/0)
Bandwidth	10 MHz
EARFCN	6200
Maximum Signal (RSRP)	-85 dBm
Direction	NW (300°)
Max RSRQ	-12 dB
Max SNR	11 dB
First Seen	5/31/2024
Last Seen	4/18/2025

[cellmapper.net]



Tower Info

Downlink Frequency	1845 MHz
Frequency Band	DCS (B3 FDD)

Cell 51

Cell Identifier	18131251
System Subtype	LTE
PCI	36 (12/0)
Bandwidth	20 MHz
EARFCN	300
Maximum Signal (RSRP)	-95 dBm
Direction	SW (231°)
Max RSRQ	-7 dB
Max SNR	7 dB
First Seen	6/7/2024
Last Seen	6/5/2025
Actions	• Go to Cell
Uplink Frequency	1950 MHz
Downlink Frequency	2140 MHz
Frequency Band	IMT (B1 FDD)

Cell 52

Cell Identifier	18131252
System Subtype	LTE
PCI	37 (12/1)

[cellmapper.net]

Threat Model

Impersonation	Interception	Location Tracking	Deanonymization
• Spoof SMS sender-id • Spoof caller-id • Transfer victims prepaid balance to my SIM	• Call Interception/Redirection • SMS Interception • MitM Attacks	• Country based tracking • Location Area based tracking • Cell-level based tracking • Exact GPS measurement tracking	• Detect presence of individual in area

Threat Model

Impersonation	Interception	Location Tracking	Deanonymization
• Spoof SMS sender-id • Spoof caller-id • Transfer victims prepaid balance to my SIM	• Call Interception/Redirection • SMS Interception • MitM Attacks	• Country based tracking • Location Area based tracking • Cell-level based tracking • Exact GPS measurement tracking	• Detect presence of individual in area

Demo: Driving Home

Mobile Station International Subscriber Directory Number

MSISDN

$$\underbrace{+49}_{\text{Country Code}}\ \underbrace{176}_{\text{National Destination Code}}\ \underbrace{12345678}_{\text{Subscriber Number}}$$

MSISDN – What does it reveal?

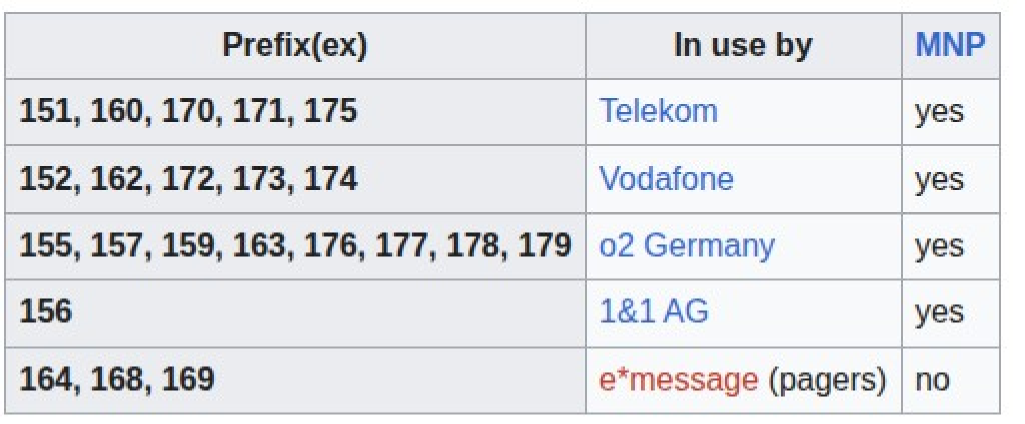
- National Destination Code reveals **original PLMN** this number was registered for.

$$\underbrace{+49}_{\text{Country Code}}\ \underbrace{176}_{\text{National Destination Code}}\ \underbrace{12345678}_{\text{Subscriber Number}}$$

MSISDN – What does it reveal?

- National Destination Code reveals **original PLMN** this number was registered for.
- Nowadays with **mobile-number-portability** (MNP) this information source might be **outdated**.

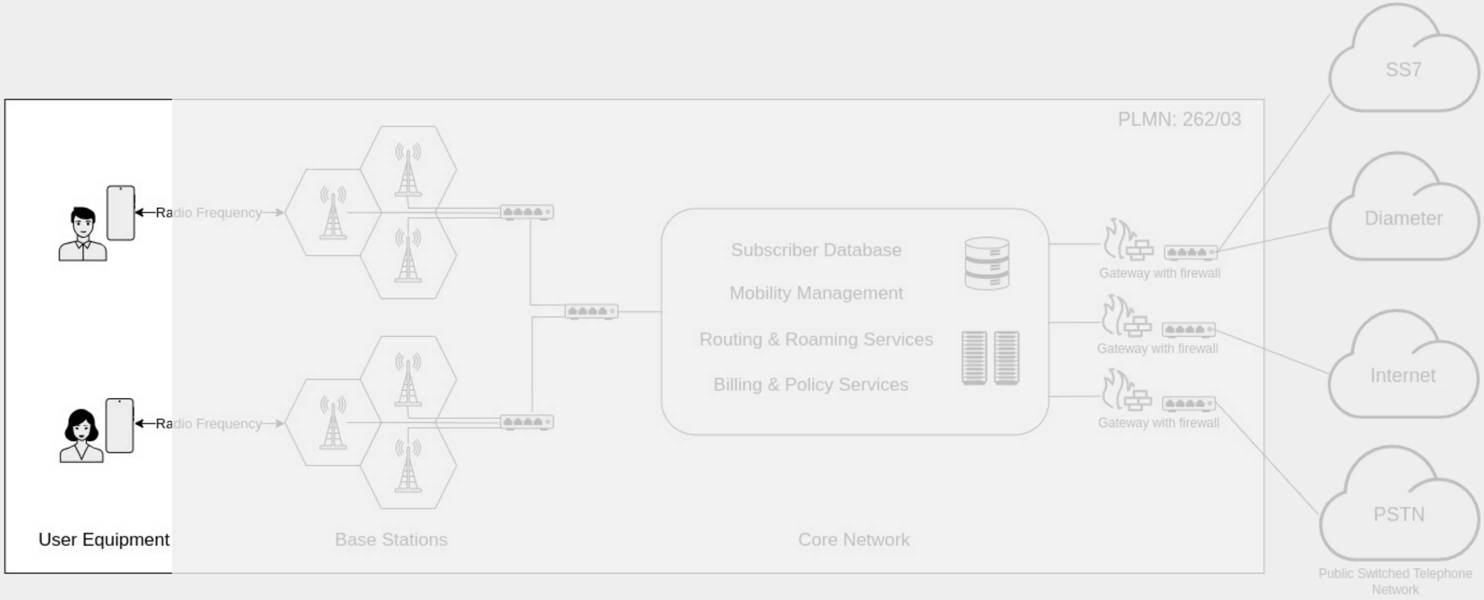
→ But there is **another** open **method** to obtain accurate information. (We'll see later).



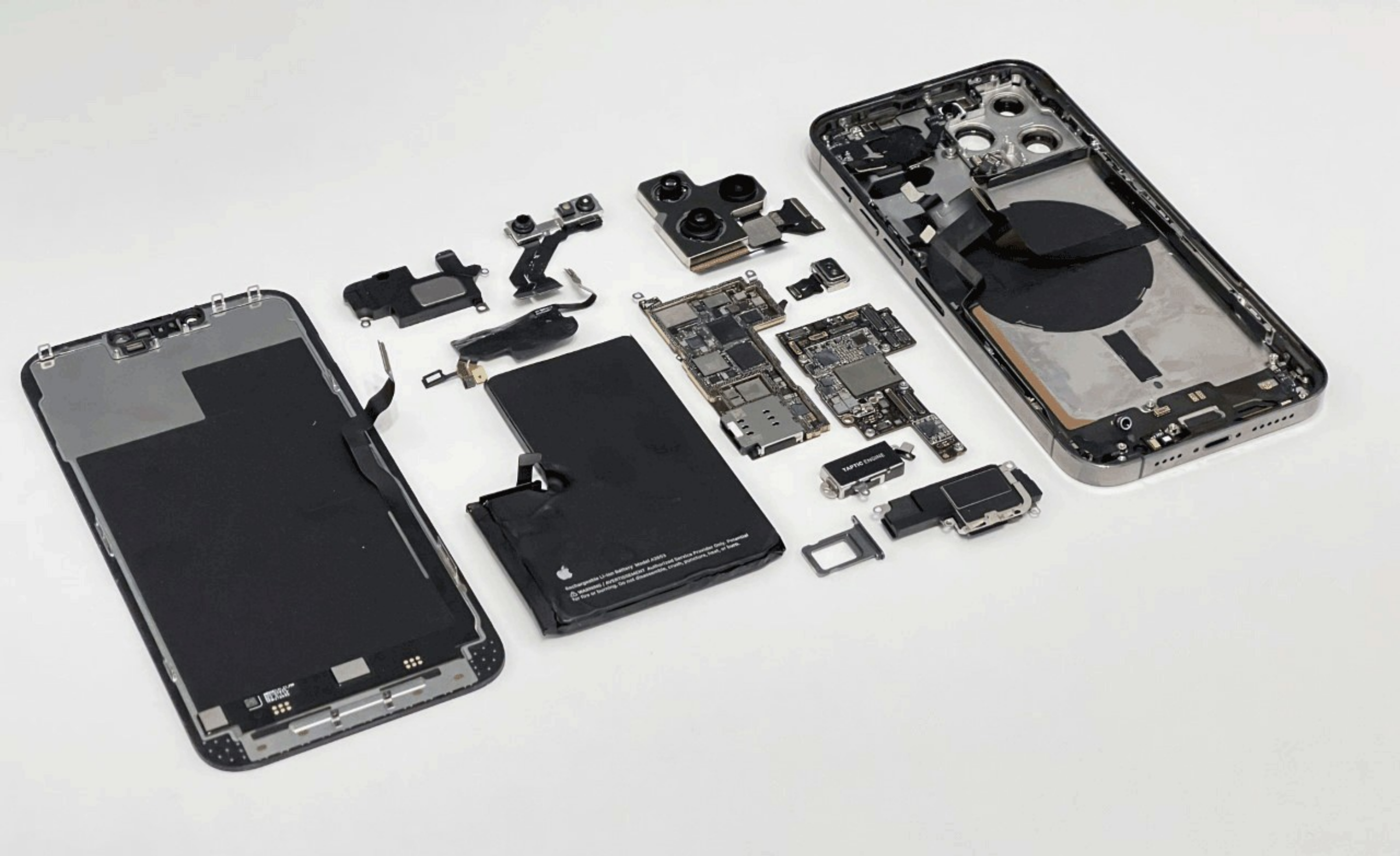
Prefix(ex)	In use by	MNP
151, 160, 170, 171, 175	Telekom	yes
152, 162, 172, 173, 174	Vodafone	yes
155, 157, 159, 163, 176, 177, 178, 179	o2 Germany	yes
156	1&1 AG	yes
164, 168, 169	e*message (pagers)	no

National Destination Code to PLMN mapping [WiK]

Attack Surface #1: User Equipment

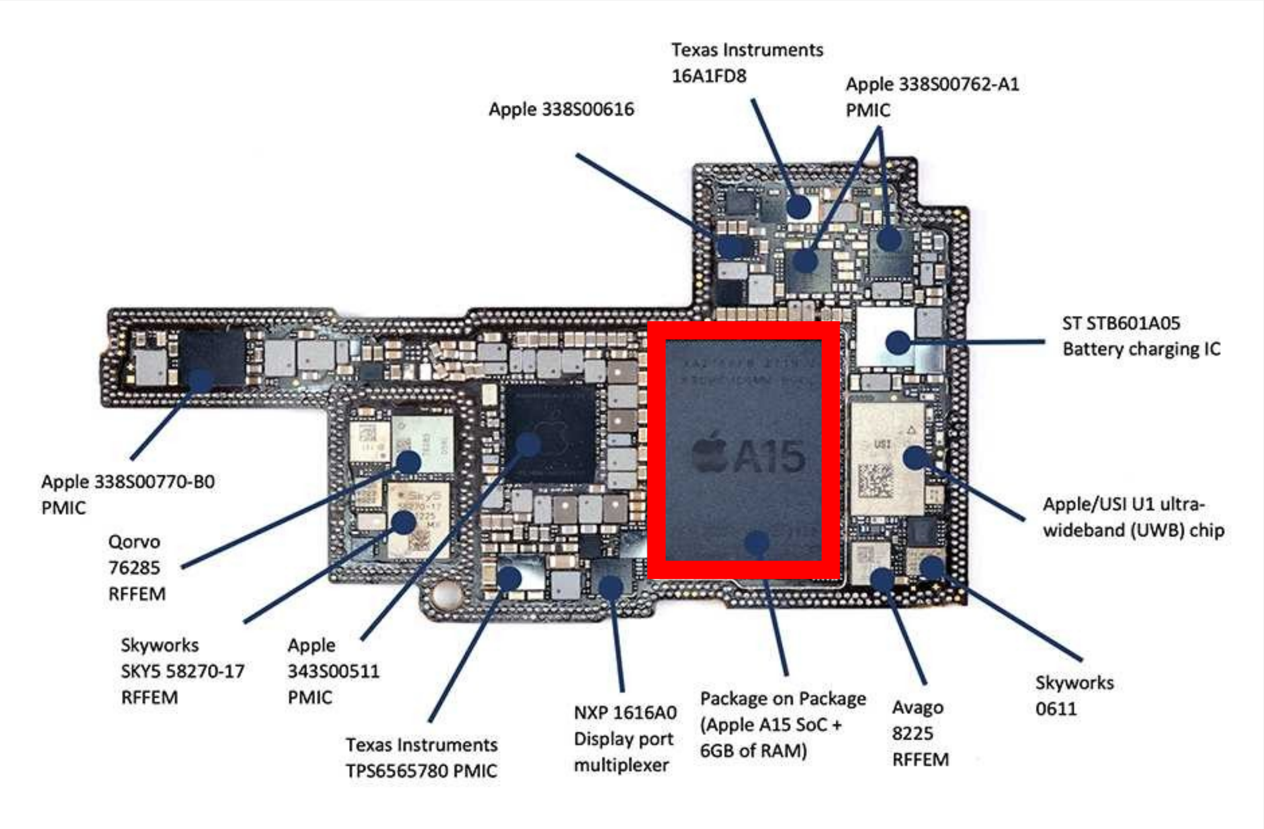


How many Processors are in your Phone?



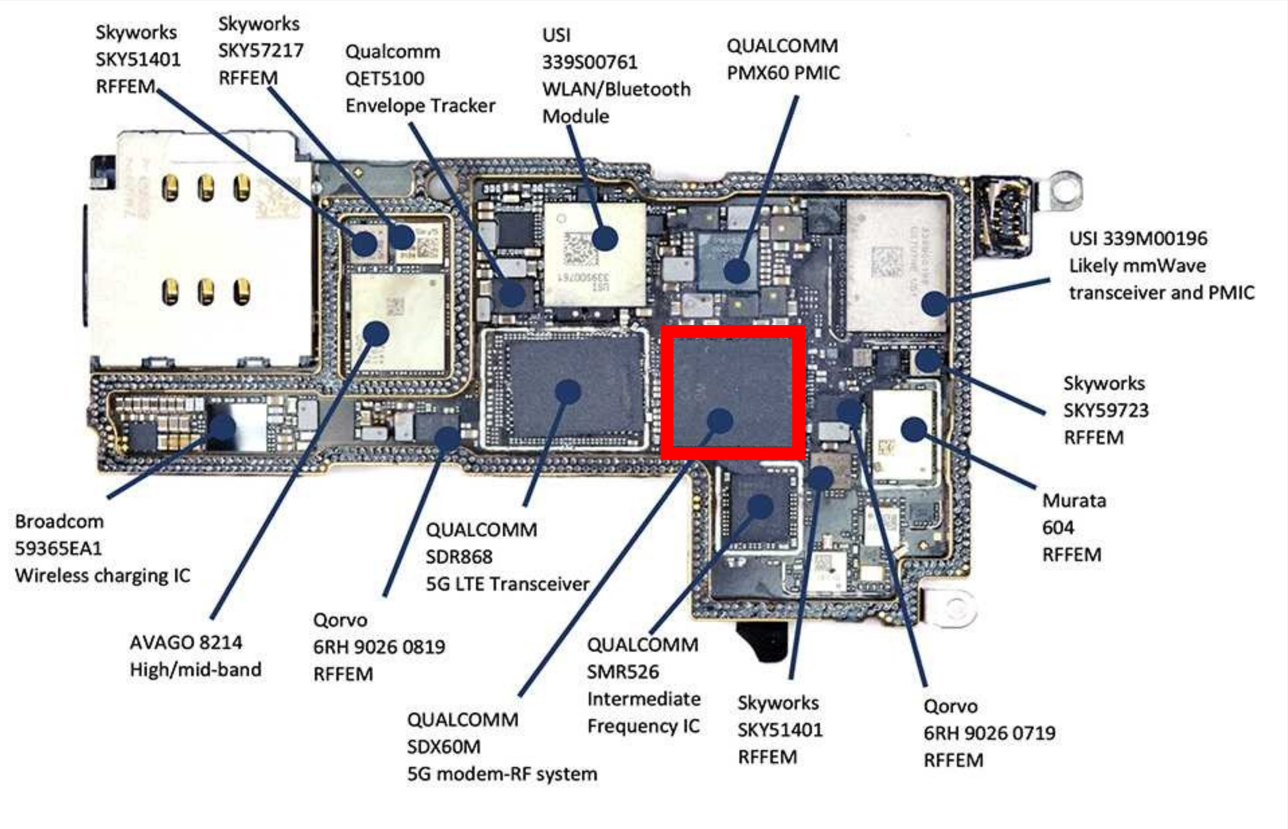
IPhone13 Pro Max Teardown [TeA]

The Application Processor



[TeA]

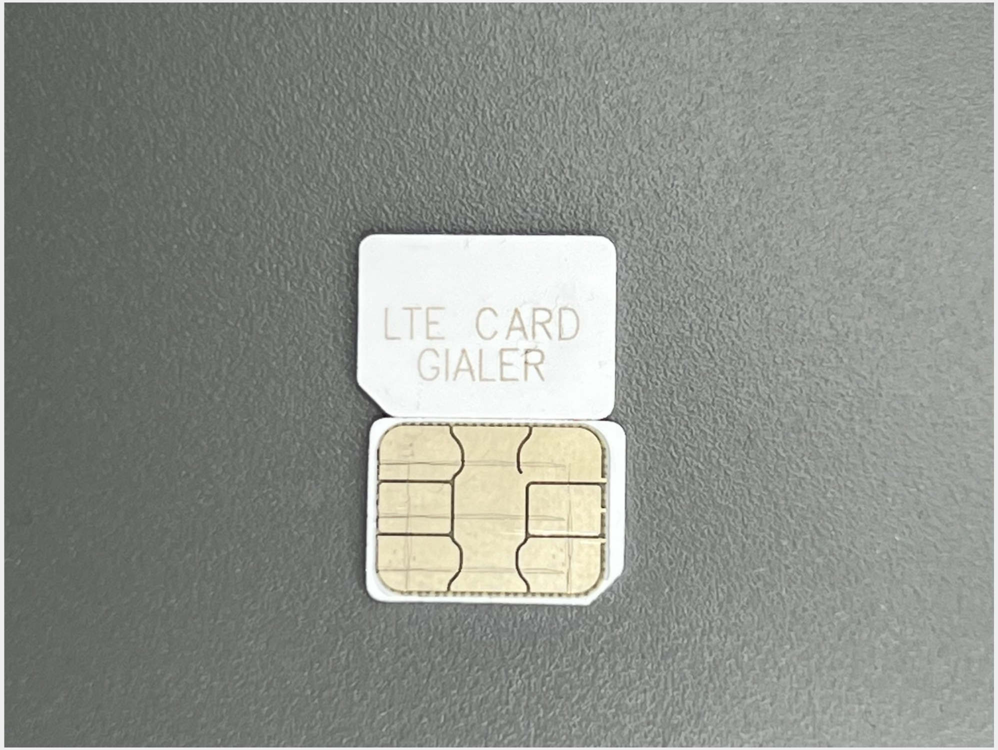
The Baseband Processor



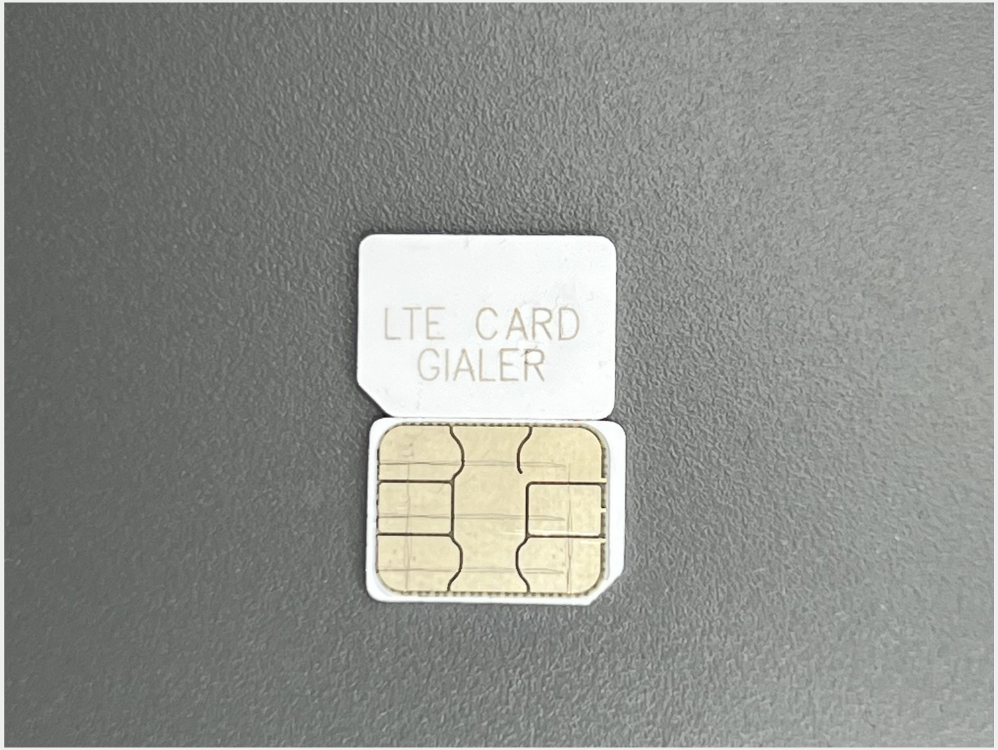
- Runs the **Modem** firmware.
- Implements all RF logic and specs.
- Exposes **API** for Application Processor.
- Has hard-coded **unique identifier** called **IMEI**

[TeA]

The Subscriber Identity Module card

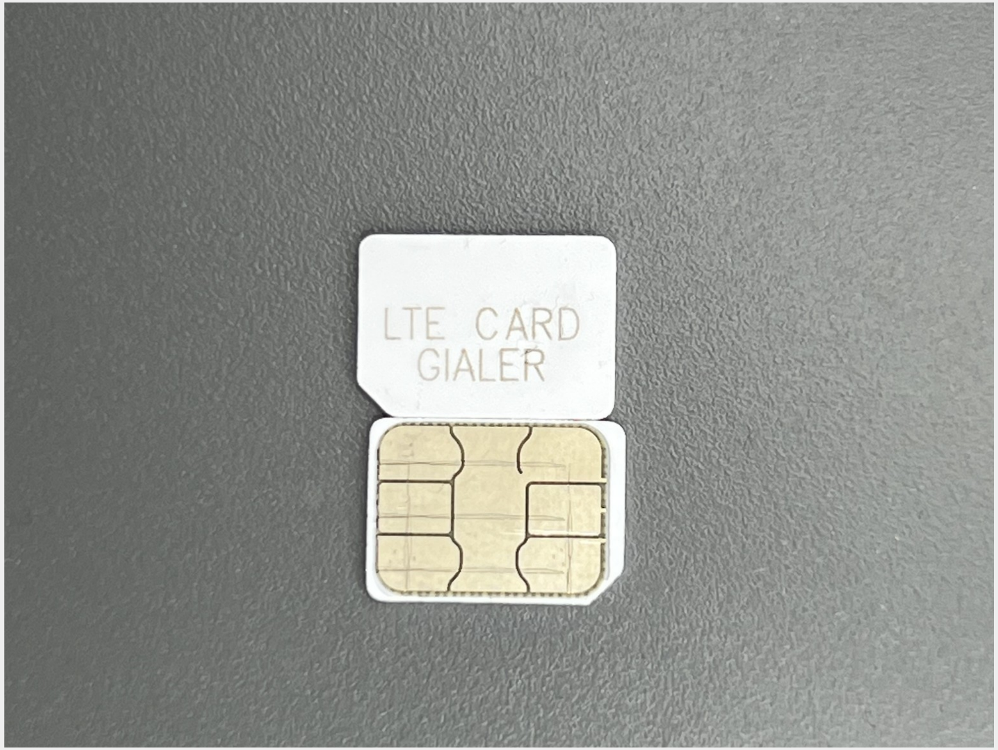


The SIM card


LTE CARD
GIALER

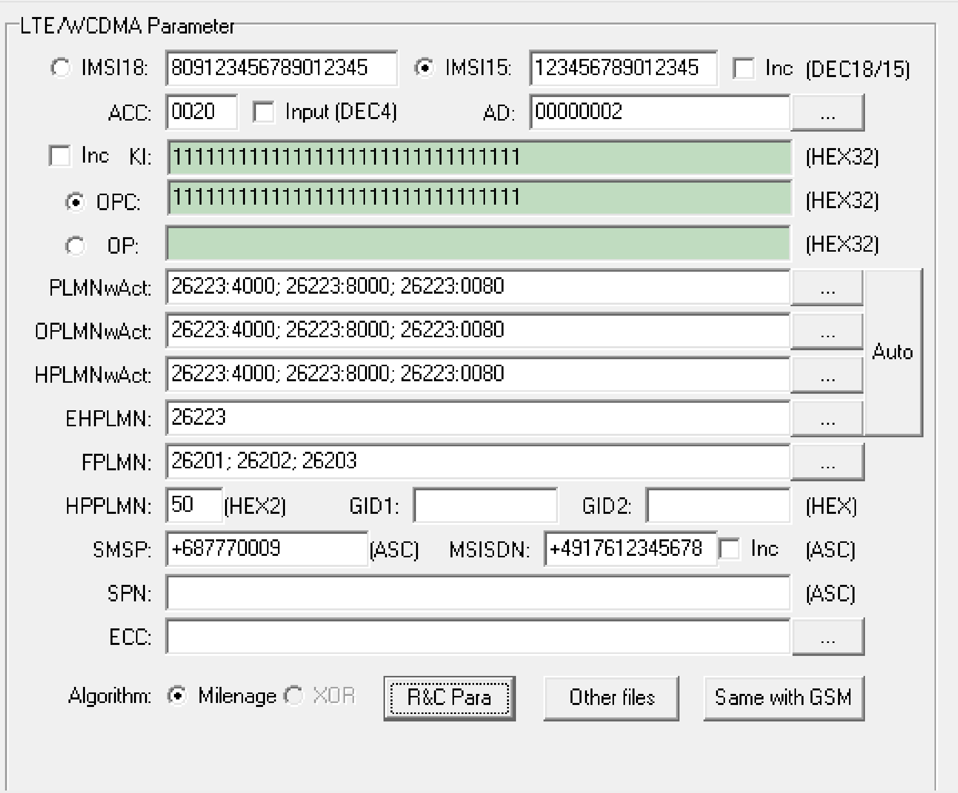
Kreissparkasse
[redacted]
Debit
[redacted]
[redacted]
IBAN
(BLZ)
(Konto-Nr.
[redacted]

The SIM card



- Is a **Smartcard**.
- Has its own non-volatile **Filesystem**.
- Has hardcoded **unique identifier** called **IMSI** (“International Mobile Subscriber Identity”).

What’s stored on your SIM card?



LTE/WCDMA Parameter

○ IMSI18: 809123456789012345 ● IMSI15: 123456789012345 □ Inc (DEC18/15)

ACC: 0020 □ Input (DEC4) AD: 00000002

□ Inc KI: 11111111111111111111111111111111 (HEX32)

● OPC: 11111111111111111111111111111111 (HEX32)

○ OP: (HEX32)

PLMNwAct: 26223:4000; 26223:8000; 26223:0080

OPLMNwAct: 26223:4000; 26223:8000; 26223:0080

HPLMNwAct: 26223:4000; 26223:8000; 26223:0080

EHPLMN: 26223

FPLMN: 26201; 26202; 26203

HPPLMN: 50 (HEX2) GID1: GID2: (HEX)

SMSP: +687770009 (ASC) MSISDN: +4917612345678 □ Inc (ASC)

SPN: (ASC)

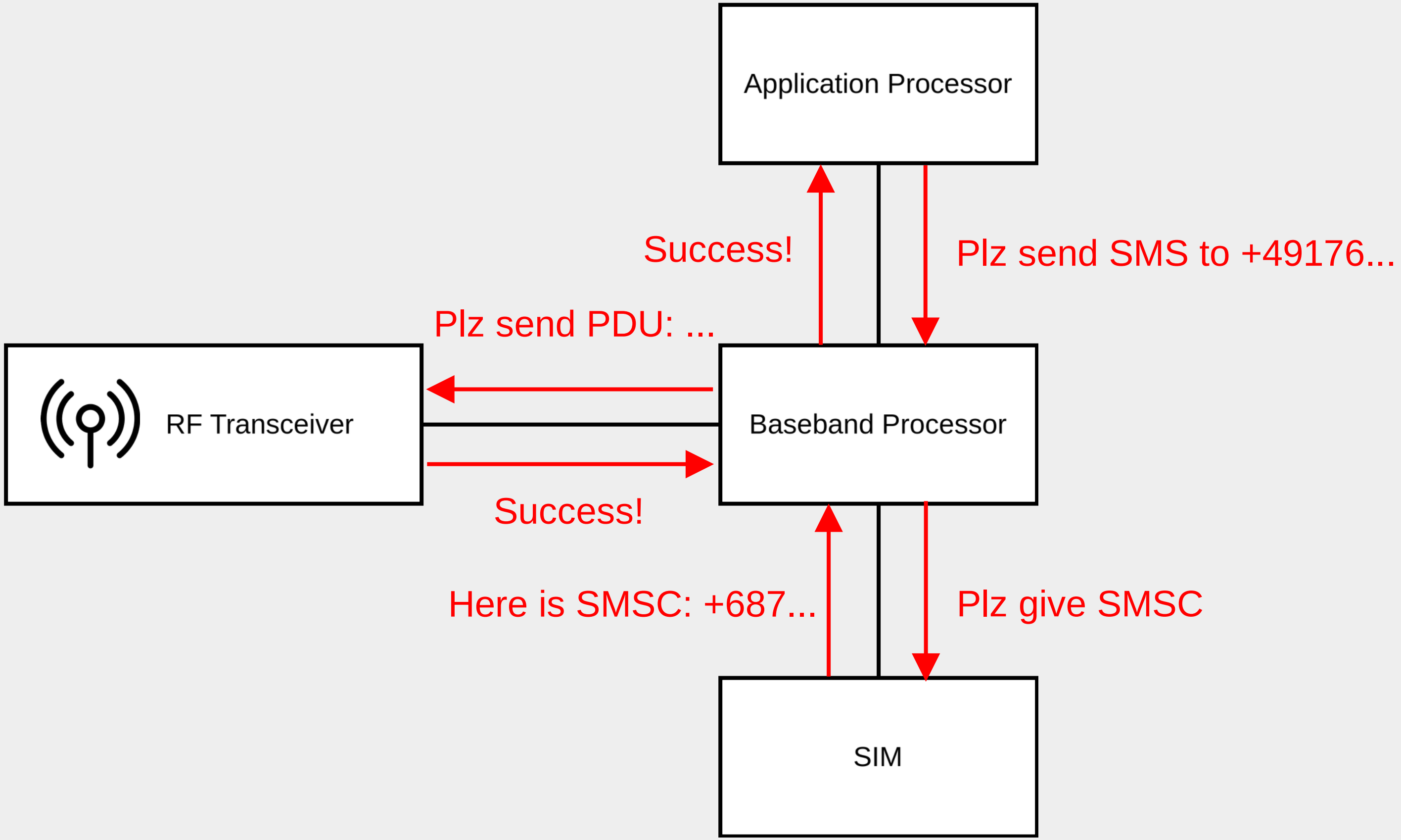
ECC:

Algorithm: ● Milenage ○ XOR

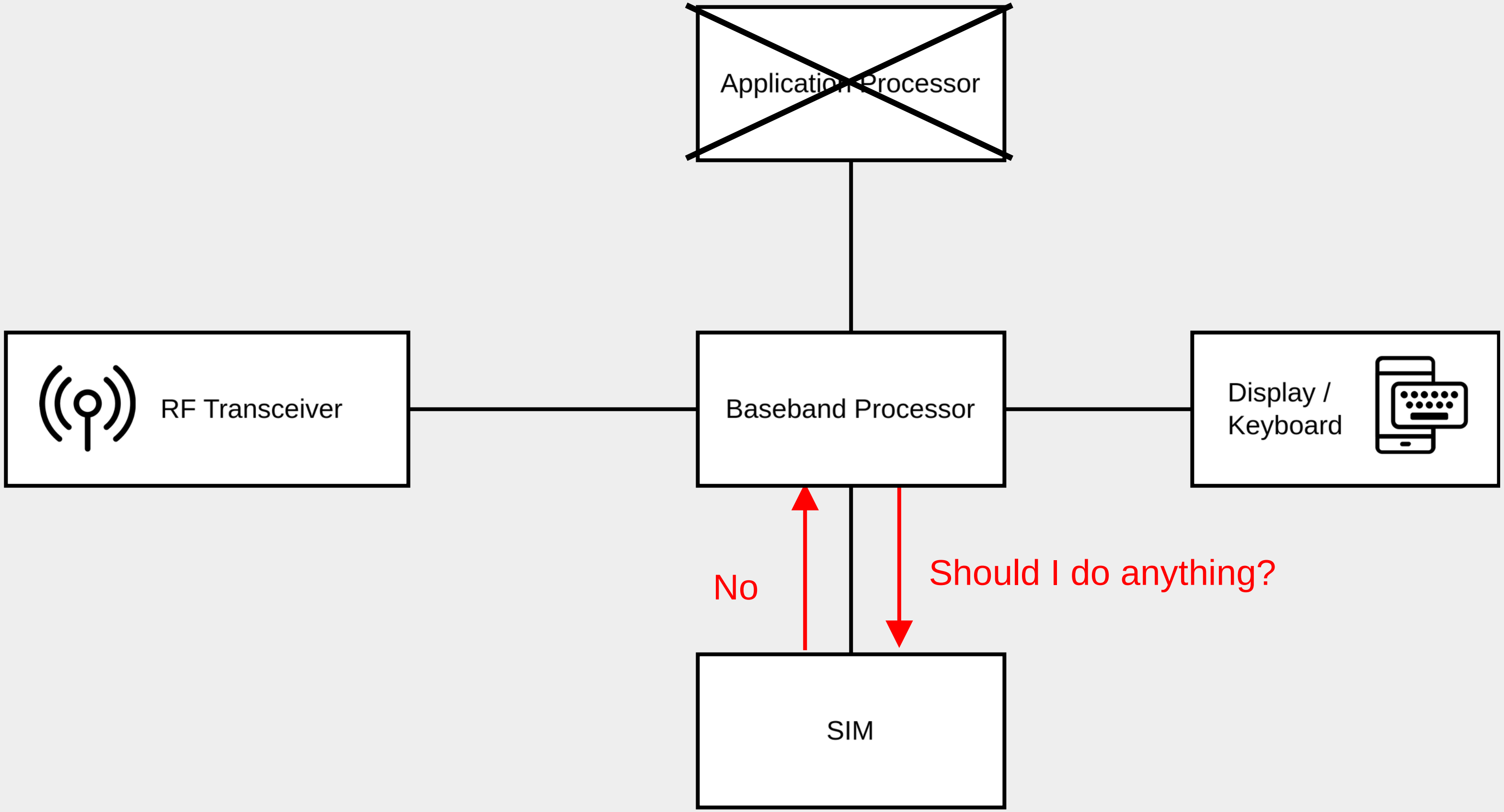
Snippet of SIM-Personalize Tools for a programmable SIM-card

- **IMSI**
- SIM **Ki**
- **OPc** (not present in < 3G)
- **SMSC** (“SMS Center”)
- **MSISDN**
- Other files with arbitrary data
- ...

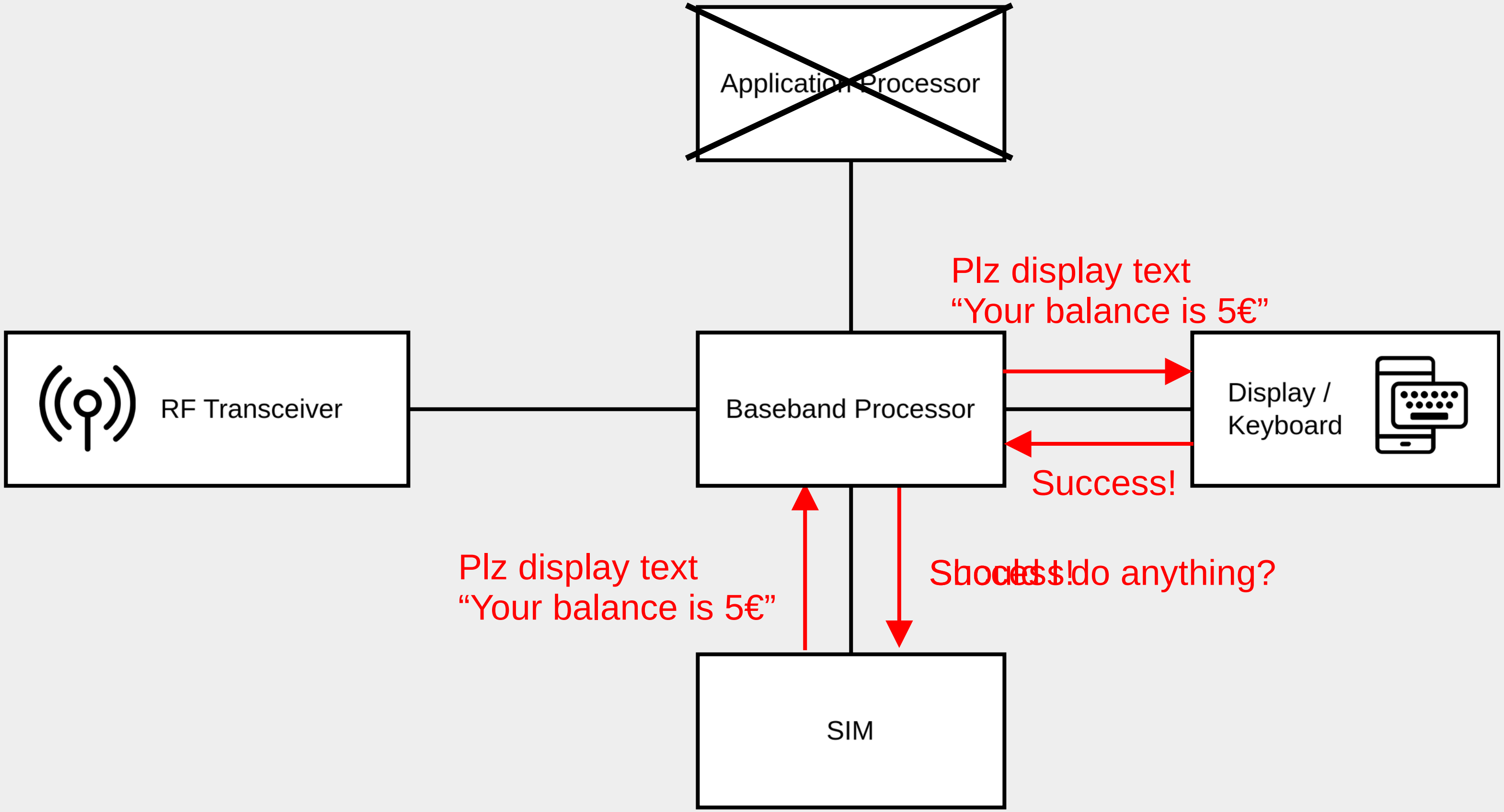
Processor Communication



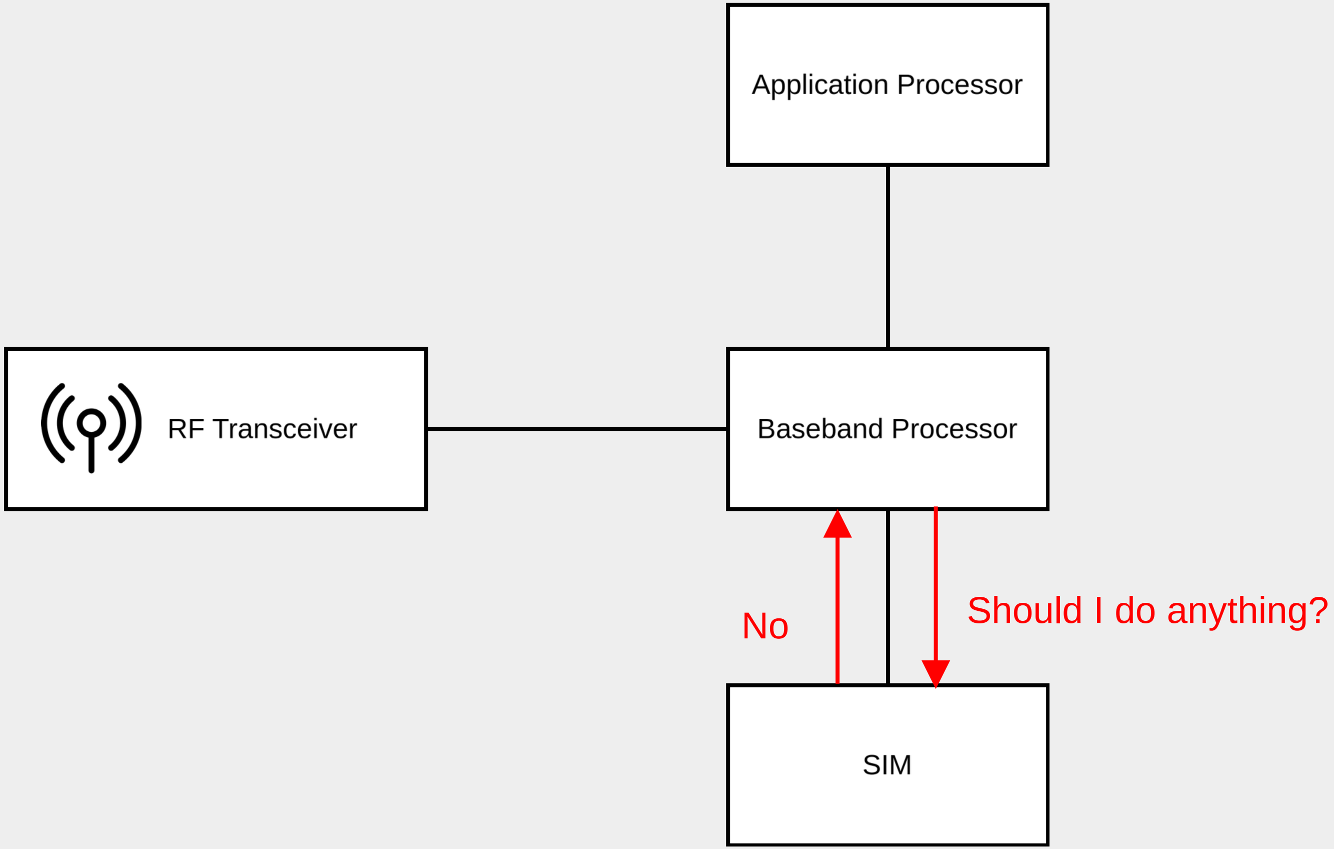
SIM Application Toolkit



SIM Application Toolkit

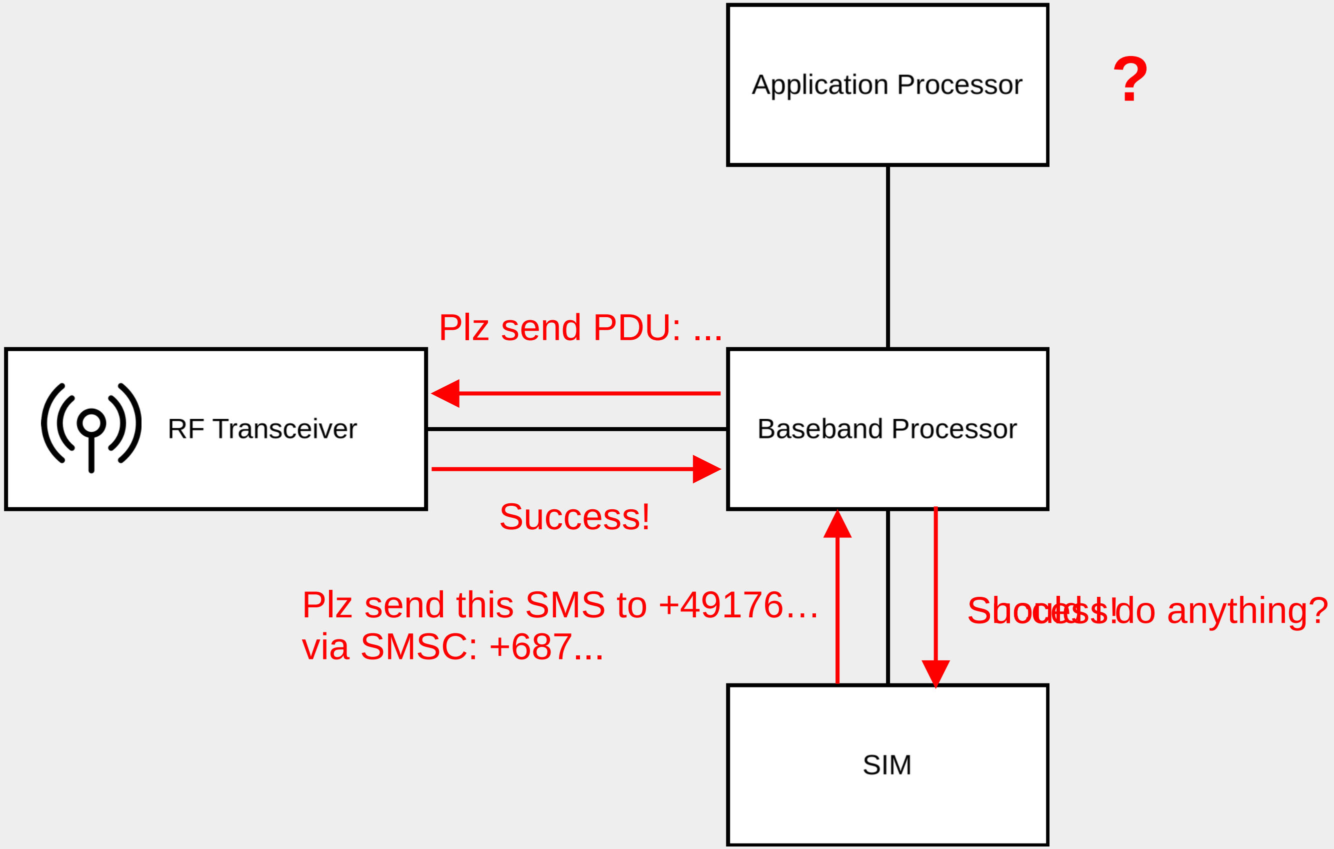


Attack 1.1: Proactive SIMs



[PaS]

Attack 1.1: Proactive SIMs



[PaS]

Attack 1.1: Proactive SIMs – What can a SIM do?

Get event Notifications

- Service Changes
- Location Updates
- Periodic Timers
- Call and SMS event
- User active, IDLE changes

Request Data

- IMEI
- PLMN / LAC / Cell-ID
- Neighbour cells with signal strength
- Current time / time zone
- WLAN SSID and status *
- Battery Level *
- GPS Location *

Communicate

- Initiate SMS
- Initiate Phone call
- Open TCP/UDP/HTTP channel *

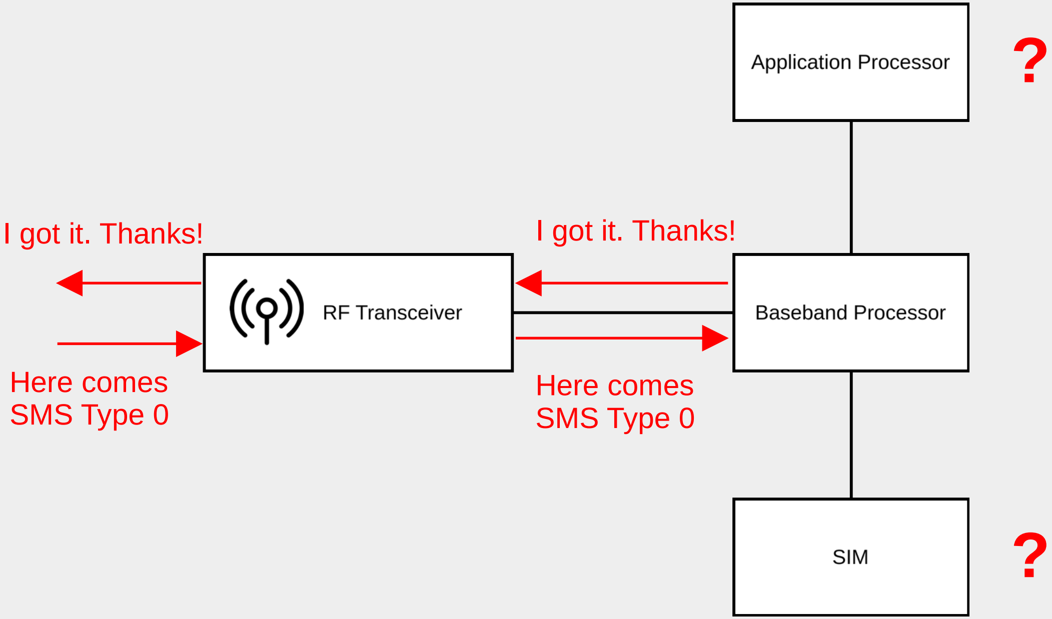
* only with help of Application Processor

[3GPP TS 31.311 Sec6]

Attack 1.2: Silent SMS

From 3GPP TS 23.040 Section 9.2.3.9:

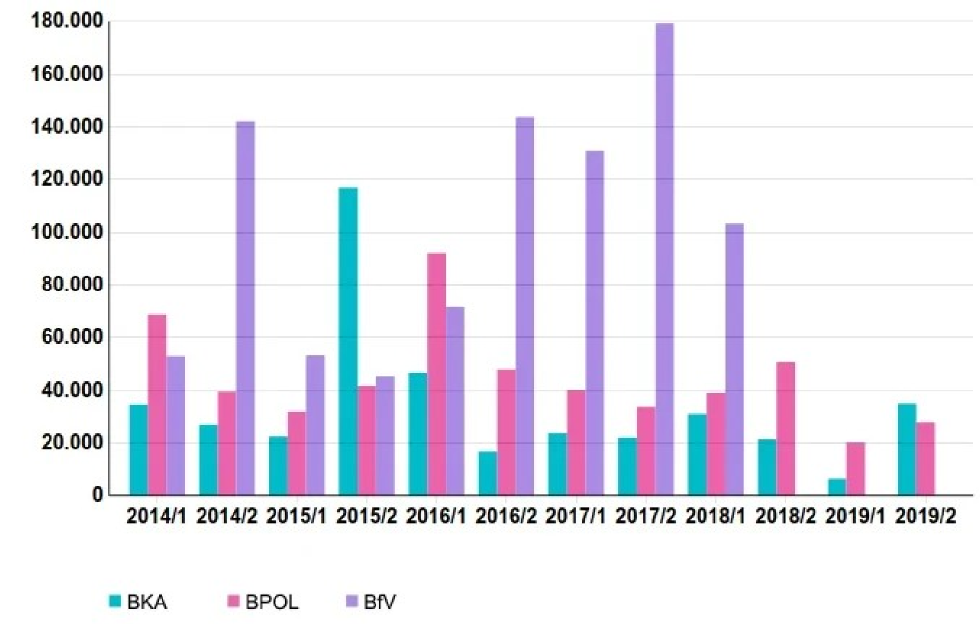
> A short message type 0 indicates that the ME **must acknowledge** receipt of the short message but shall **discard its contents**. This means that
>
> - [...]
> - the MS shall **not indicate** the receipt of the type 0 short message **to the user**,
> - the short message shall **neither be stored** in the **(U)SIM** nor **ME**.



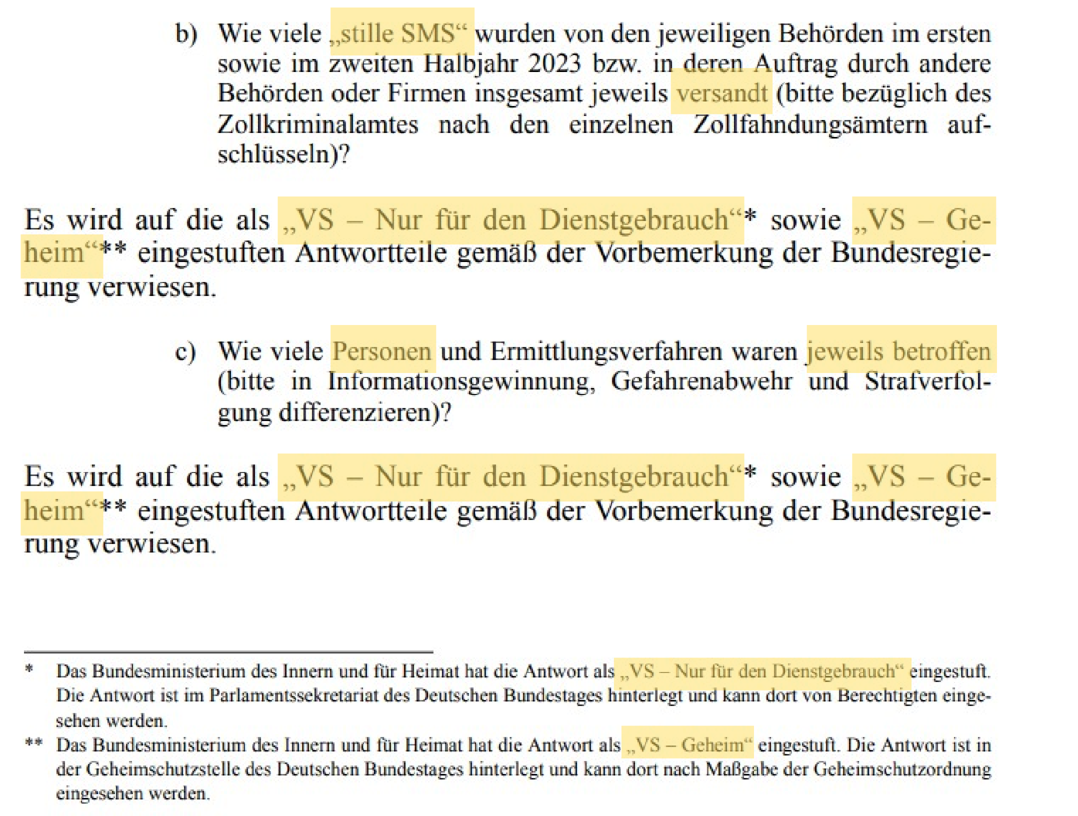
"Silent SMS are SMS that are not shown to the user."

Law Enforcement Agencies:

Attack 1.2: Silent SMS – Usage by Law Enforcement Agencies



Number of Silent SMSs sent by German Law Enforcement Agencies [SiS]



b) Wie viele „stille SMS“ wurden von den jeweiligen Behörden im ersten sowie im zweiten Halbjahr 2023 bzw. in deren Auftrag durch andere Behörden oder Firmen insgesamt jeweils versandt (bitte bezüglich des Zollkriminalamtes nach den einzelnen Zollfahndungsämtern aufschlüsseln)?

Es wird auf die als „VS – Nur für den Dienstgebrauch“* sowie „VS – Geheim“** eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

c) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

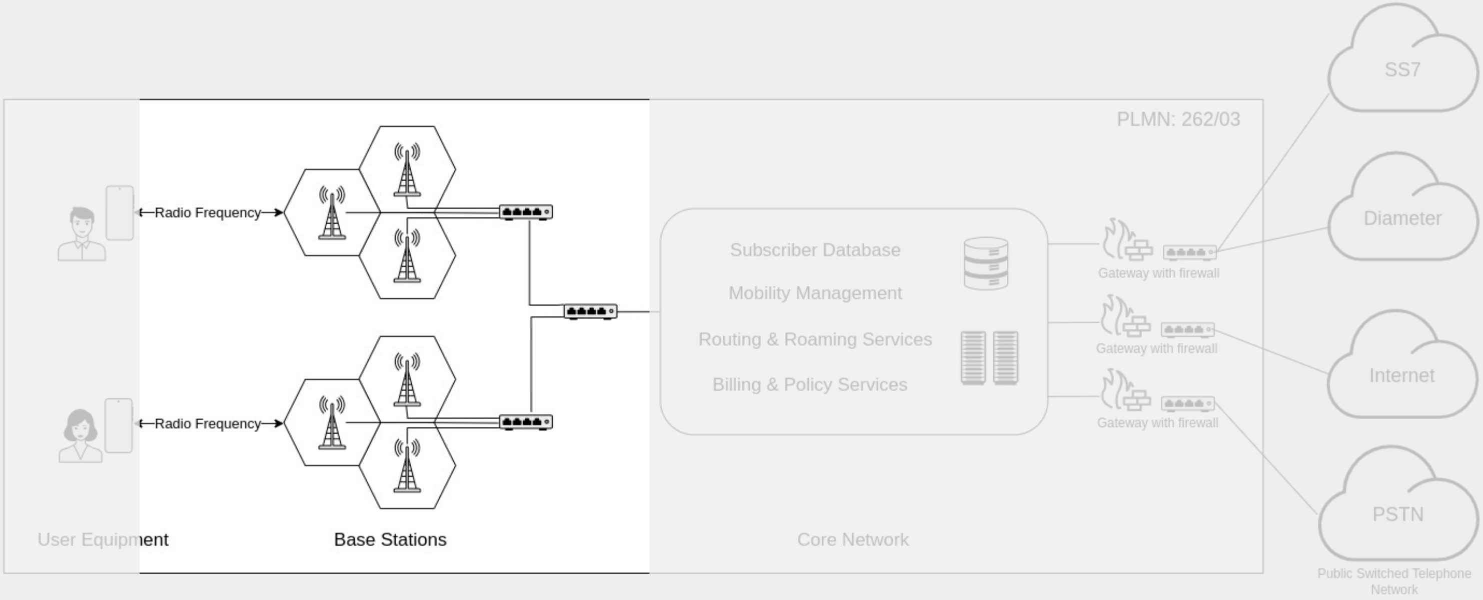
Es wird auf die als „VS – Nur für den Dienstgebrauch“* sowie „VS – Geheim“** eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

** Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

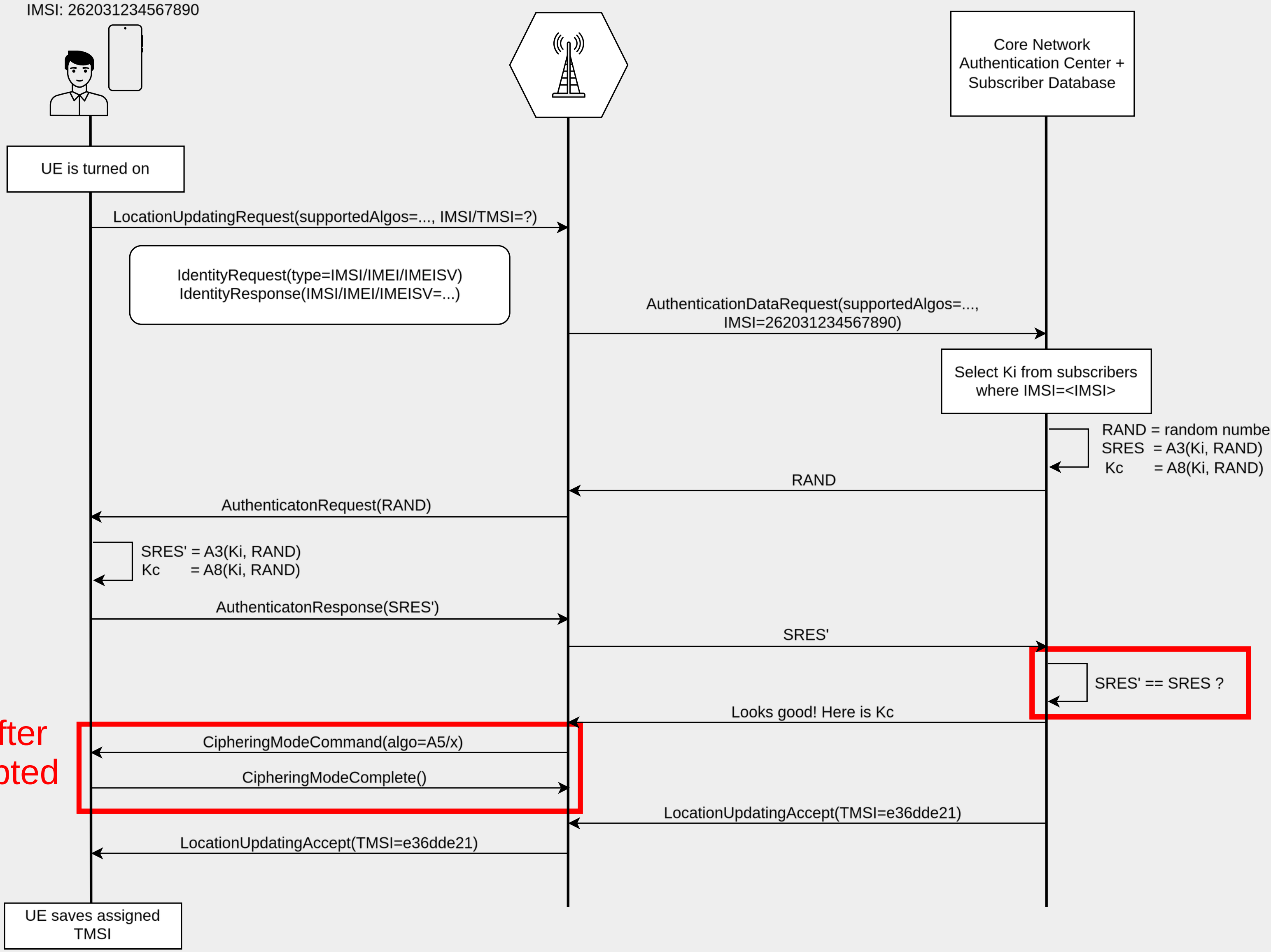
Answer to “Kleine Frage”: Use of so-called silent SMS, Wi-Fi catchers, IMSI catchers, and cell tower dumps (2023) [SmQ]

Attack Surface #2: RF + Base Stations



What happens when you turn on your phone? (2G)

2G



IMSI: 262031234567890

Core Network
Authentication Center +
Subscriber Database

UE is turned on

LocationUpdatingRequest(supportedAlgos=..., IMSI/TMSI=?)

IdentityRequest(type=IMSI/IMEI/IMEISV)
IdentityResponse(IMSI/IMEI/IMEISV=...)

AuthenticationDataRequest(supportedAlgos=...,
IMSI=262031234567890)

Select Ki from subscribers
where IMSI=<IMSI>

RAND = random number
SRES = A3(Ki, RAND)
Kc = A8(Ki, RAND)

RAND

AuthenticatonRequest(RAND)

SRES' = A3(Ki, RAND)
Kc = A8(Ki, RAND)

AuthenticatonResponse(SRES')

SRES'

SRES' == SRES ?

Looks good! Here is Kc

CipheringModeCommand(algo=A5/x)

CipheringModeComplete()

LocationUpdatingAccept(TMSI=e36dde21)

LocationUpdatingAccept(TMSI=e36dde21)

UE saves assigned
TMSI

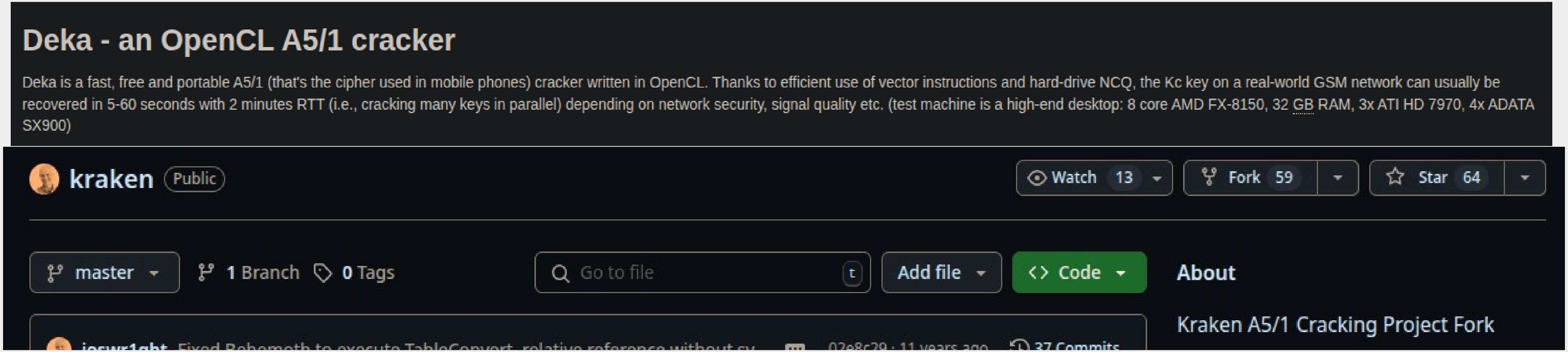
No mutual
authentication

Everything after
that is encrypted
with A5/x

Attack 2.1: Decrypt SMS / Phone Calls

In the 2G variants there are various encryption algorithms available to encrypt user data:

- A5/0: No Encryption. Insecure.
- A5/1: Can be cracked with 2TB rainbow tables in a few seconds. Insecure. [Noh10]
- A5/2: Is fundamentally broken. Can be cracked within milliseconds. Insecure.
- A5/3: Uses KASUMI cipher with 96bit key. Secure enough for practice.
- A5/4: Uses KASUMI cipher with 128bit key length. Secure enough for practice.



Deka - an OpenCL A5/1 cracker

Deka is a fast, free and portable A5/1 (that's the cipher used in mobile phones) cracker written in OpenCL. Thanks to efficient use of vector instructions and hard-drive NCQ, the Kc key on a real-world GSM network can usually be recovered in 5-60 seconds with 2 minutes RTT (i.e., cracking many keys in parallel) depending on network security, signal quality etc. (test machine is a high-end desktop: 8 core AMD FX-8150, 32 GB RAM, 3x ATI HD 7970, 4x ADATA SX900)

kraken Public

About

Kraken A5/1 Cracking Project Fork

joswr1ght Fixed Behemoth to execute TableConvert, relative reference without sy 02e8c29 · 11 years ago 37 Commits

Two Open-Source A5/1 cracking tools. [Dek],[KrK]

Sidenote: Man-in-the-Middle Attacks in 2G

- The **Base-Station decides** the **final** ciphering **algorithm** used for SMS/Calls.
- Rouge Base-Station could **force** UE into using **no** or **weak** **encryption** (A5/0 or A5/1).

→ Together with no mutual authentication in 2G this opens door to various MitM Attacks.

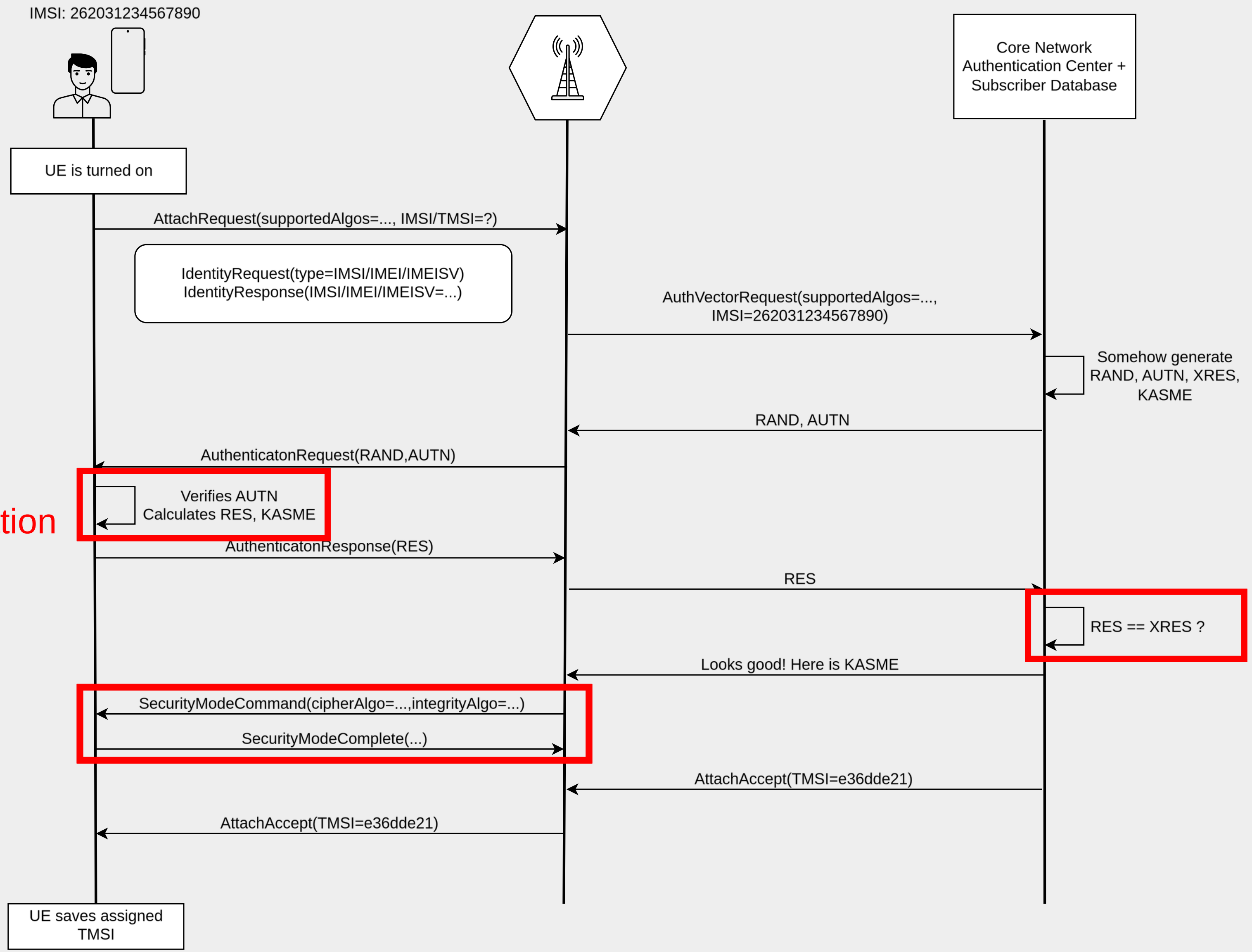
"PHONE CALLS/SMS MESSAGES CAN BE INTERCEPTED IN 2G."
YOUR MOBILE OPERATOR STILL SUPPORTING 2G.

What happens when you turn on your phone? (3G)

- Very **similar** to how **4G** works.
- 3G is **discontinued** in Germany.

→ Let’s see how 4G works then.

What happens when you turn on your phone? (4G)



4G

IMSI: 262031234567890

Core Network
Authentication Center +
Subscriber Database

UE is turned on

AttachRequest(supportedAlgos=..., IMSI/TMSI=?)

IdentityRequest(type=IMSI/IMEI/IMEISV)
IdentityResponse(IMSI/IMEI/IMEISV=...)

AuthVectorRequest(supportedAlgos=...,
IMSI=262031234567890)

Somehow generate
RAND, AUTN, XRES,
KASME

RAND, AUTN

AuthenticatonRequest(RAND,AUTN)

Mutual
authentication

Verifies AUTN
Calculates RES, KASME

AuthenticatonResponse(RES)

RES

RES == XRES ?

Looks good! Here is KASME

SecurityModeCommand(cipherAlgo=...,integrityAlgo=...)

SecurityModeComplete(...)

AttachAccept(TMSI=e36dde21)

AttachAccept(TMSI=e36dde21)

UE saves assigned
TMSI

Key Concept: Temporary Mobile Subscriber Identity

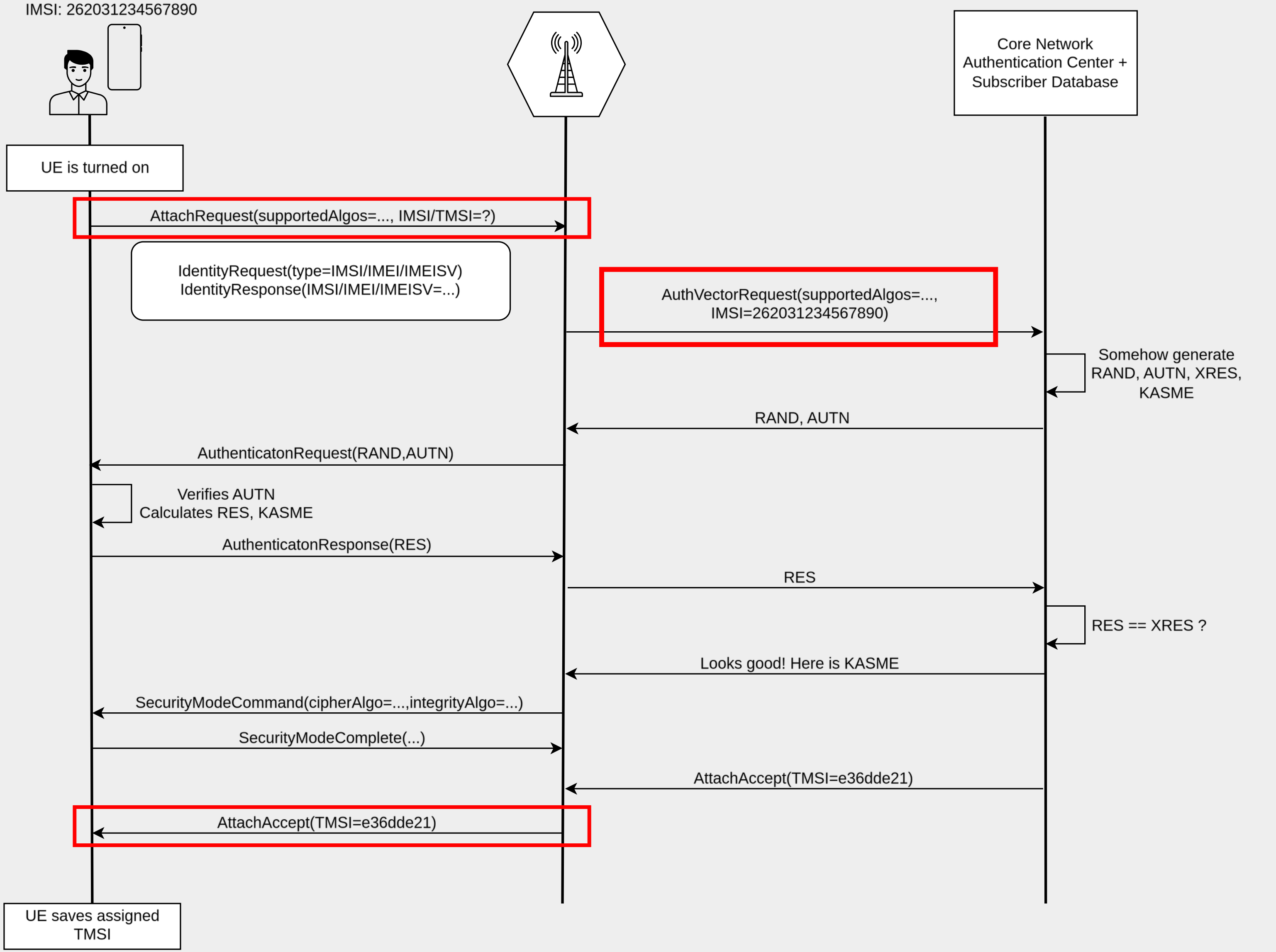
Key Concept: TMSI

Used to **pseudonymize IMSI**. It is obtained/rotated on several configurable occasions.

Obtained on:

- **Initial registration** in PLMN Core Network.

4G



IMSI: 262031234567890

Core Network
Authentication Center +
Subscriber Database

UE is turned on

AttachRequest(supportedAlgos=..., IMSI/TMSI=?)

IdentityRequest(type=IMSI/IMEI/IMEISV)
IdentityResponse(IMSI/IMEI/IMEISV=...)

AuthVectorRequest(supportedAlgos=...,
IMSI=262031234567890)

Somehow generate
RAND, AUTN, XRES,
KASME

RAND, AUTN

AuthenticatonRequest(RAND,AUTN)

Verifies AUTN
Calculates RES, KASME

AuthenticatonResponse(RES)

RES

RES == XRES ?

Looks good! Here is KASME

SecurityModeCommand(cipherAlgo=...,integrityAlgo=...)

SecurityModeComplete(...)

AttachAccept(TMSI=e36dde21)

AttachAccept(TMSI=e36dde21)

UE saves assigned
TMSI

Key Concept: TMSI

- Used to **pseudonymize IMSI**. It is obtained/rotated on several configurable occasions.

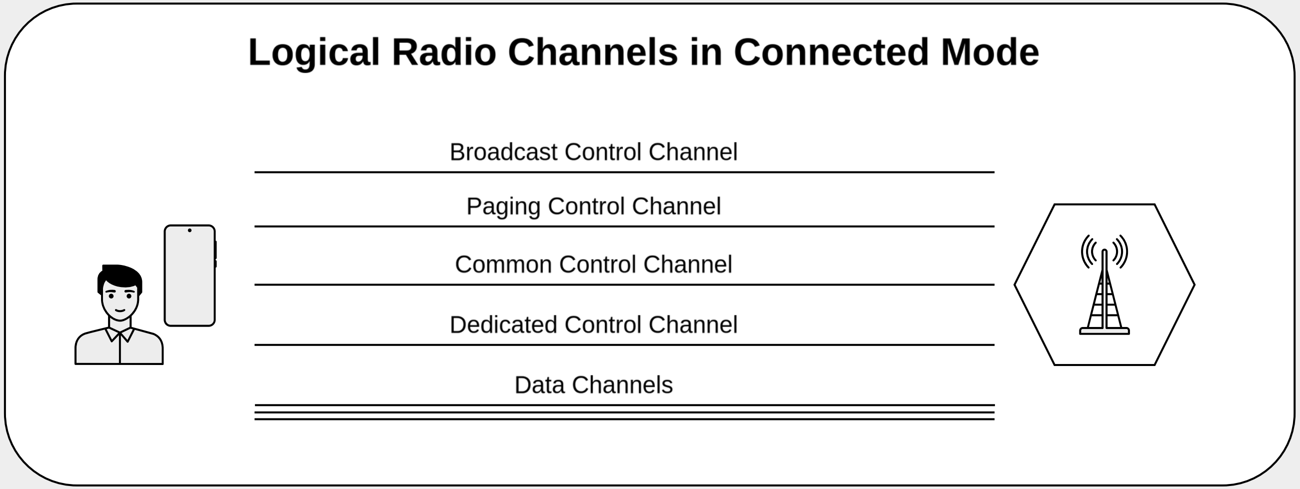
Obtained on:

- **Initial registration** in PLMN Core Network.

Rotated on:

- Registering in a new **Tracking/Location Area**.
- **Invalid** old TMSI (via TMSIReallocationCommand).
- ...

Key Concept: Paging



Logical Radio Channels in Connected Mode

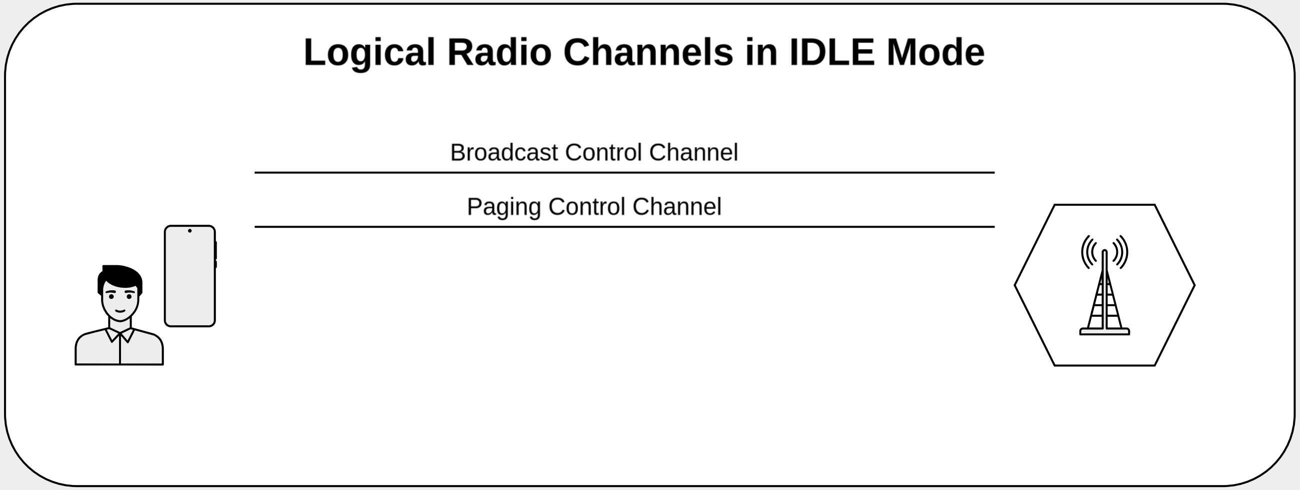
Broadcast Control Channel

Paging Control Channel

Common Control Channel

Dedicated Control Channel

Data Channels

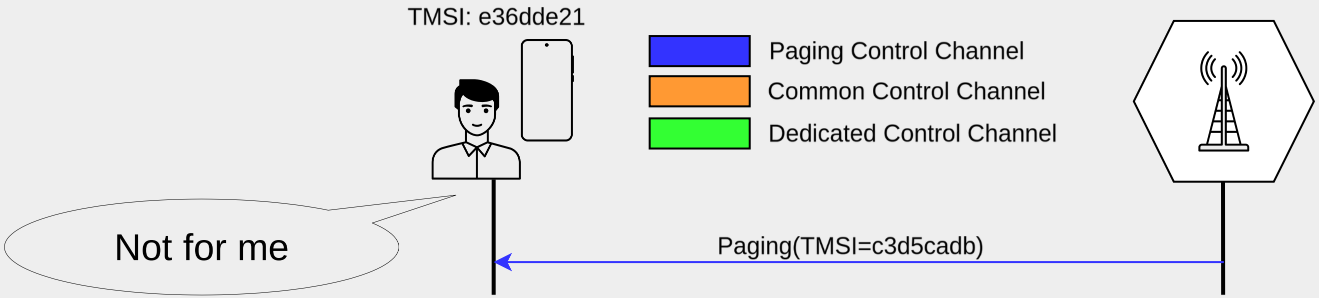


Logical Radio Channels in IDLE Mode

Broadcast Control Channel

Paging Control Channel

Key Concept: Paging



TMSI: e36dde21

🟦 Paging Control Channel

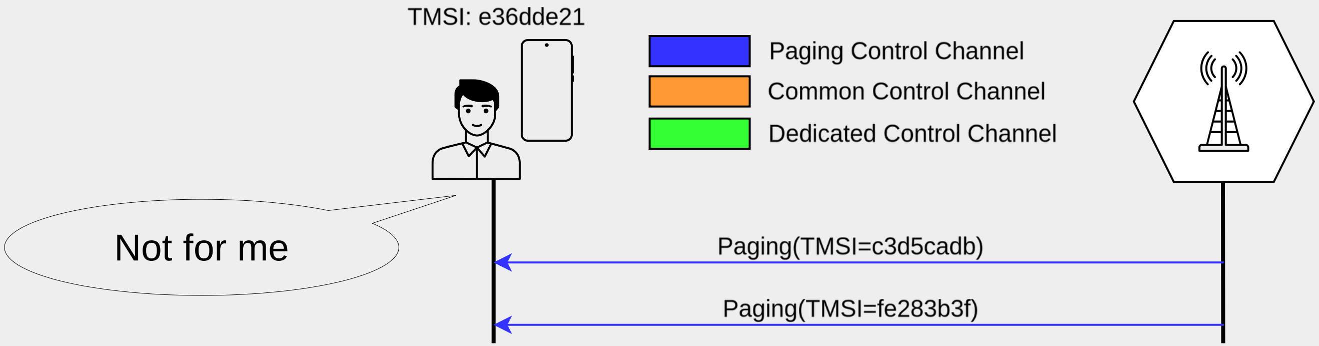
🟧 Common Control Channel

🟩 Dedicated Control Channel

Paging(TMSI=c3d5cadb)

Not for me

Key Concept: Paging



TMSI: e36dde21

🟦 Paging Control Channel

🟧 Common Control Channel

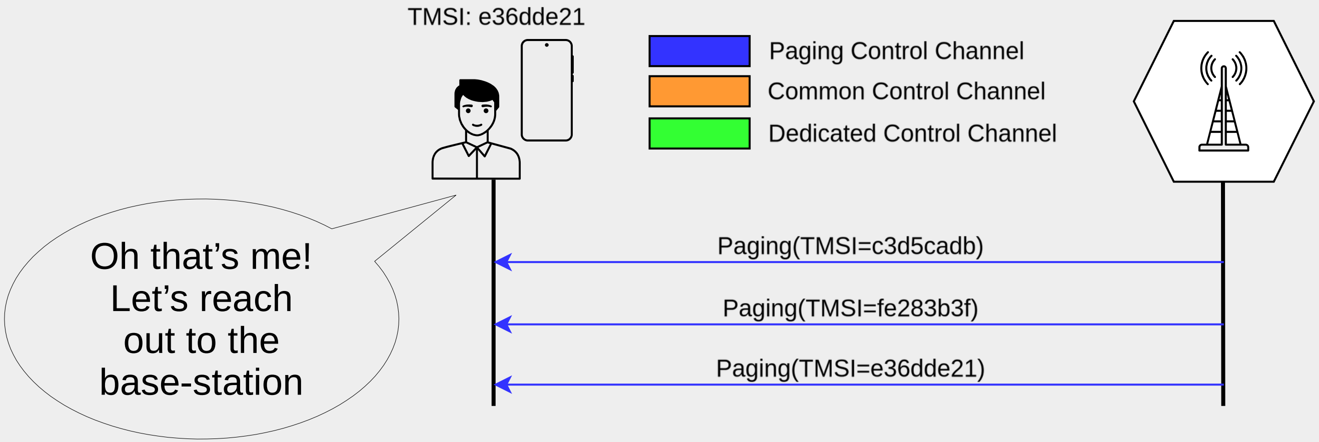
🟩 Dedicated Control Channel

Not for me

Paging(TMSI=c3d5cadb)

Paging(TMSI=fe283b3f)

Key Concept: Paging



TMSI: e36dde21

🟦 Paging Control Channel

🟧 Common Control Channel

🟩 Dedicated Control Channel

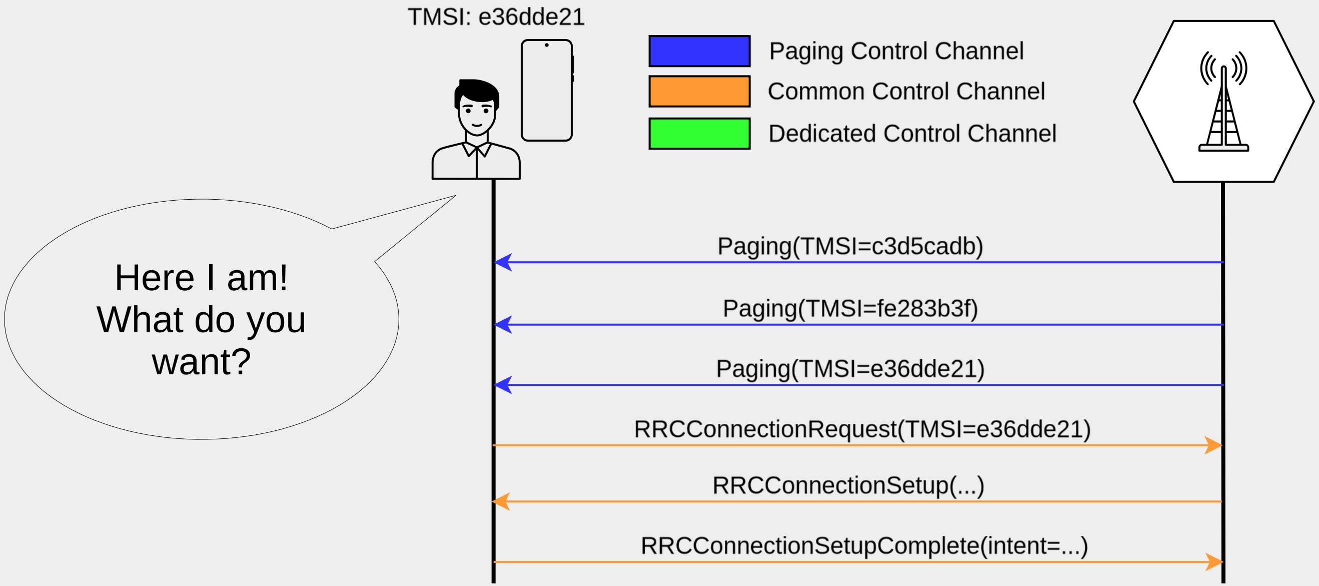
Paging(TMSI=c3d5cadb)

Paging(TMSI=fe283b3f)

Paging(TMSI=e36dde21)

Oh that’s me! Let’s reach out to the base-station

Key Concept: Paging



TMSI: e36dde21

🟦 Paging Control Channel

🟧 Common Control Channel

🟩 Dedicated Control Channel

Here I am!
What do you
want?

Paging(TMSI=c3d5cadb)

Paging(TMSI=fe283b3f)

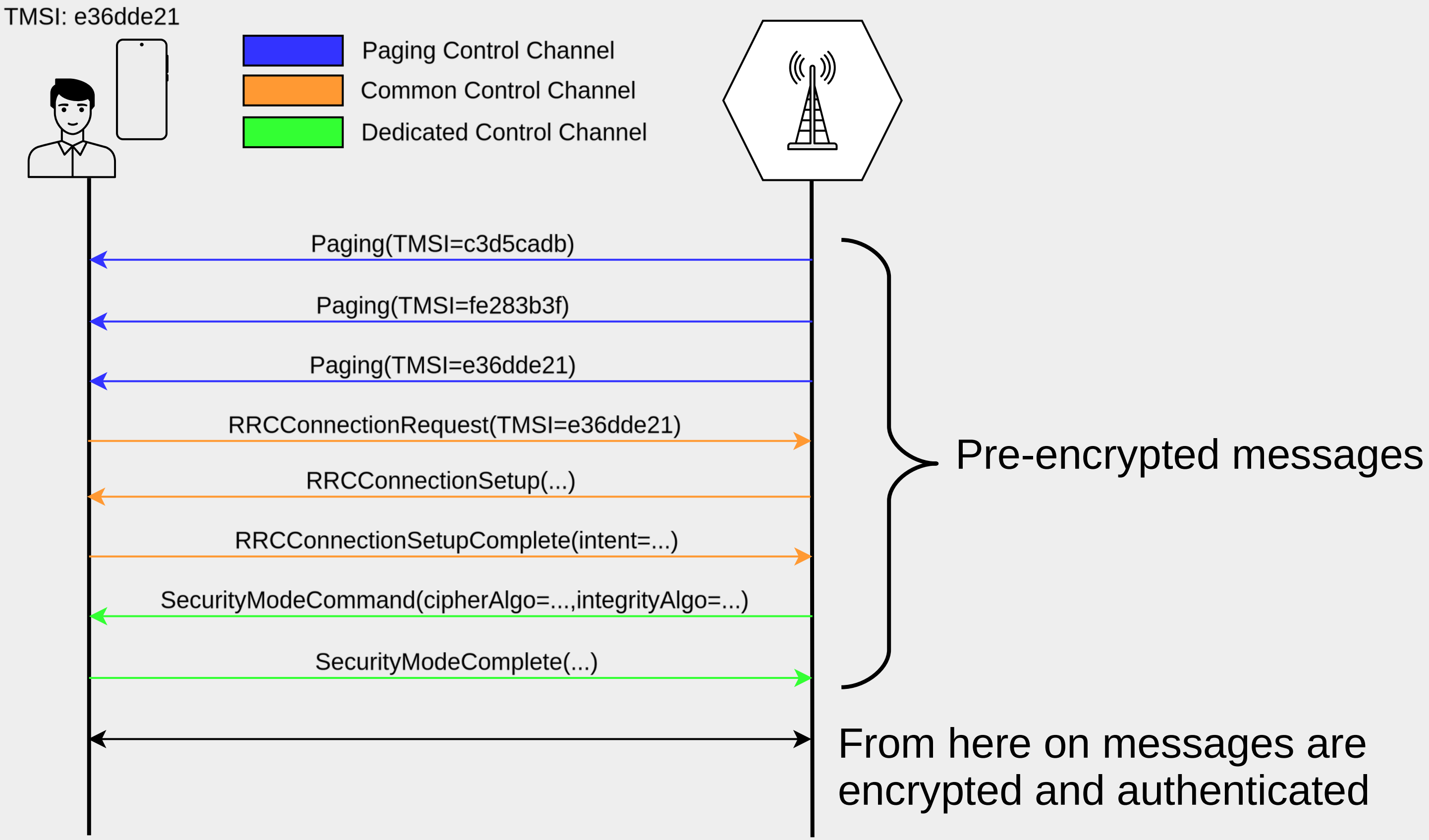
Paging(TMSI=e36dde21)

RRCConnectionRequest(TMSI=e36dde21)

RRCConnectionSetup(...)

RRCConnectionSetupComplete(intent=...)

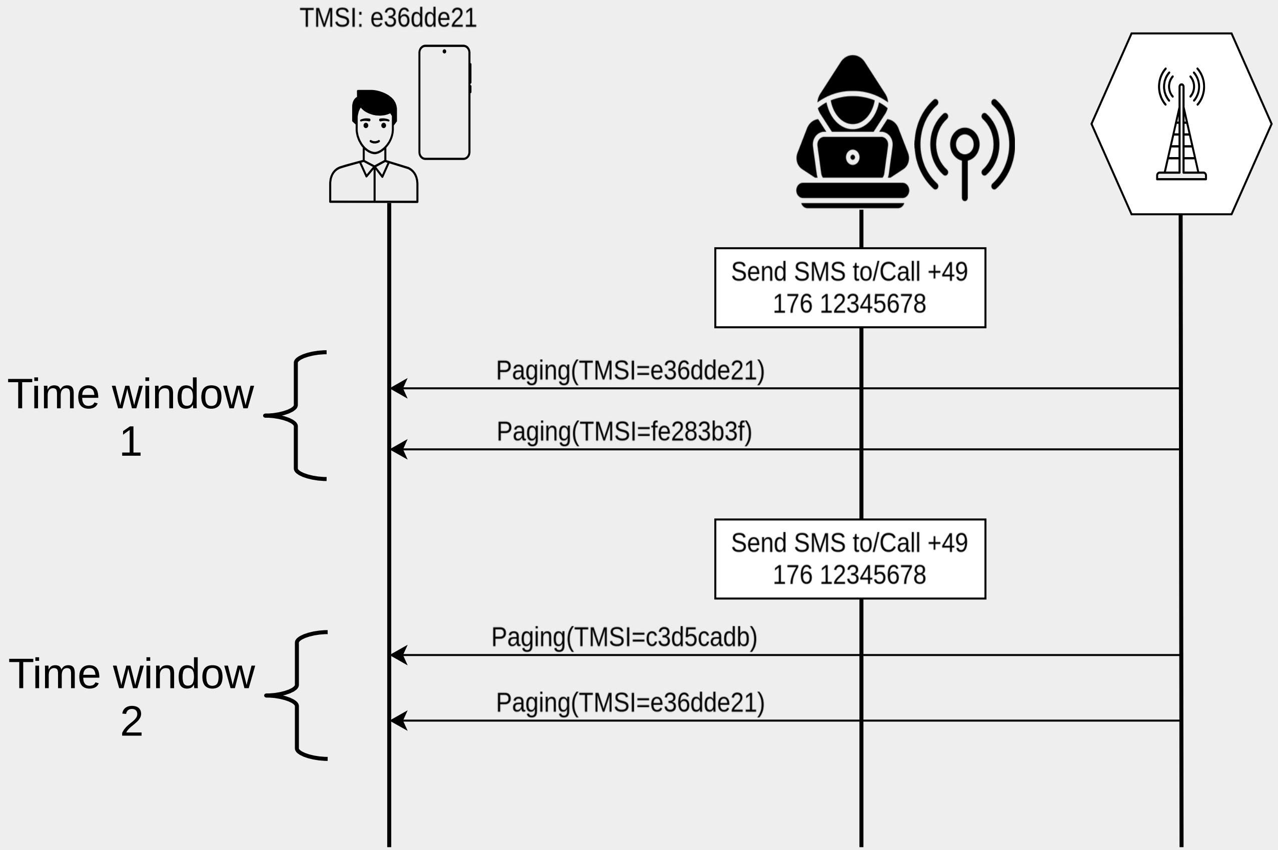
Key Concept: Paging



TMSI: e36dde21
🟦 Paging Control Channel
🟧 Common Control Channel
🟩 Dedicated Control Channel
Paging(TMSI=c3d5cadb)
Paging(TMSI=fe283b3f)
Paging(TMSI=e36dde21)
RRCConnectionRequest(TMSI=e36dde21)
RRCConnectionSetup(...)
RRCConnectionSetupComplete(intent=...)
SecurityModeCommand(cipherAlgo=...,integrityAlgo=...)
SecurityModeComplete(...)
Pre-encrypted messages
From here on messages are encrypted and authenticated

→ Paging messages are sent in cleartext from **all base-stations** in current **TAU** of UE (for calls) **or** the **last registered** single **cell** (for SMS/WhatsApp Messages/etc.). Thats called “Smart Paging”.

Attack 2.2: Presence Testing



TMSI: e36dde21

Send SMS to/Call +49 176 12345678

Time window 1

Paging(TMSI=e36dde21)

Paging(TMSI=fe283b3f)

Send SMS to/Call +49 176 12345678

Time window 2

Paging(TMSI=c3d5cadb)

Paging(TMSI=e36dde21)

{e36dde21, fe283b3f}

∩

{c3d5cadb, e36dde21}
=
{e36dde21}

→ Obtains **MSISDN** to **TMSI** mapping as a byproduct.

[Sha17],[Got19]

Sidenote: Flash Calls

- Initiate a call but then **hang up directly** afterwards.
- Good **timing** is key! Can be **scripted** using VoIP/Modem API.

→ Creates **Paging messages** in current TAU of UE, **without notifying** the victim.

→ Good legal alternative to Silent SMSs.

[Sha17],[Got19]

Live Demo: Presence Testing

IMSI-Catcher

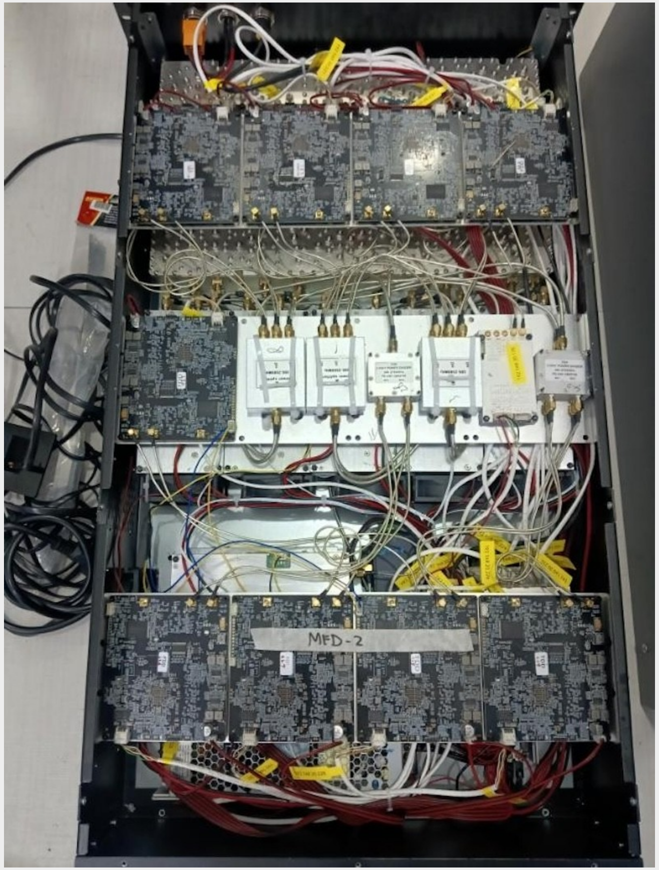
How it started:

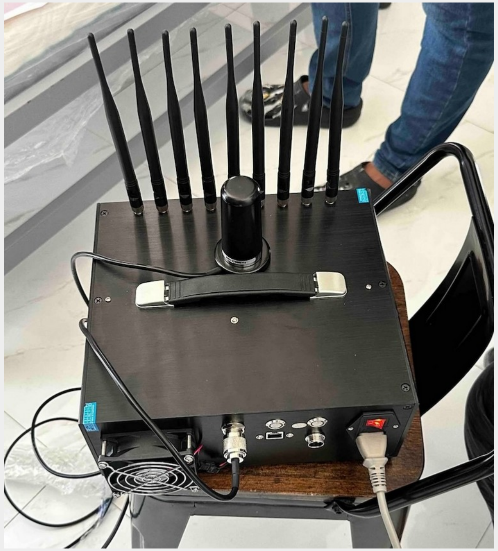
- Devices used to **catch IMSIs**.
- Mostly **passive**. Just listens to UL/DL and catch plaintext IMSIs.

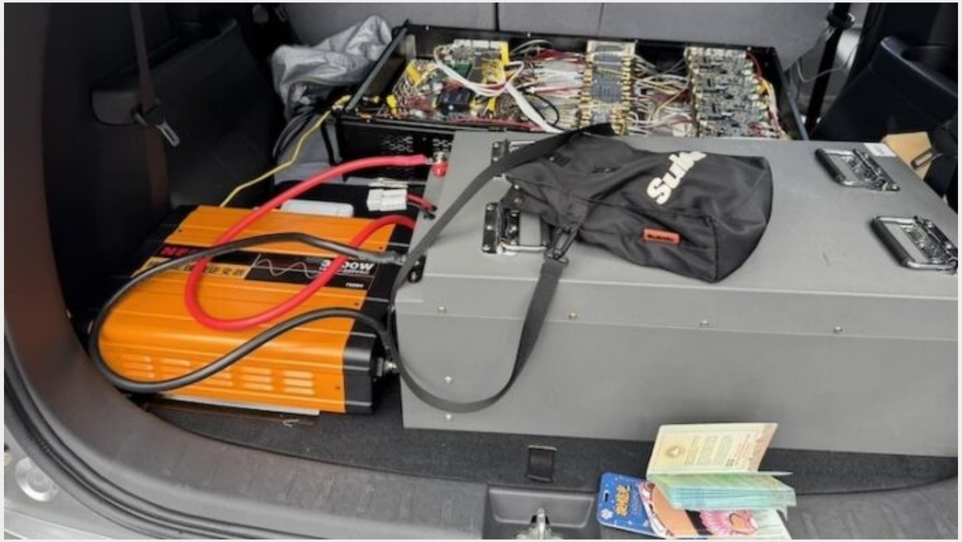
How it's now:

- General term for all kinds of rouge base-stations.
- Can perform much more sophisticated attacks such as Call/SMS Interception, active downgrade attacks, SMS-Blasting, etc.
- Mostly **active**. Emulates a legit base-station to lure UEs into connecting to it.

IMSI-Catcher







Attack 2.3a: IMSI-Catching (Passive)

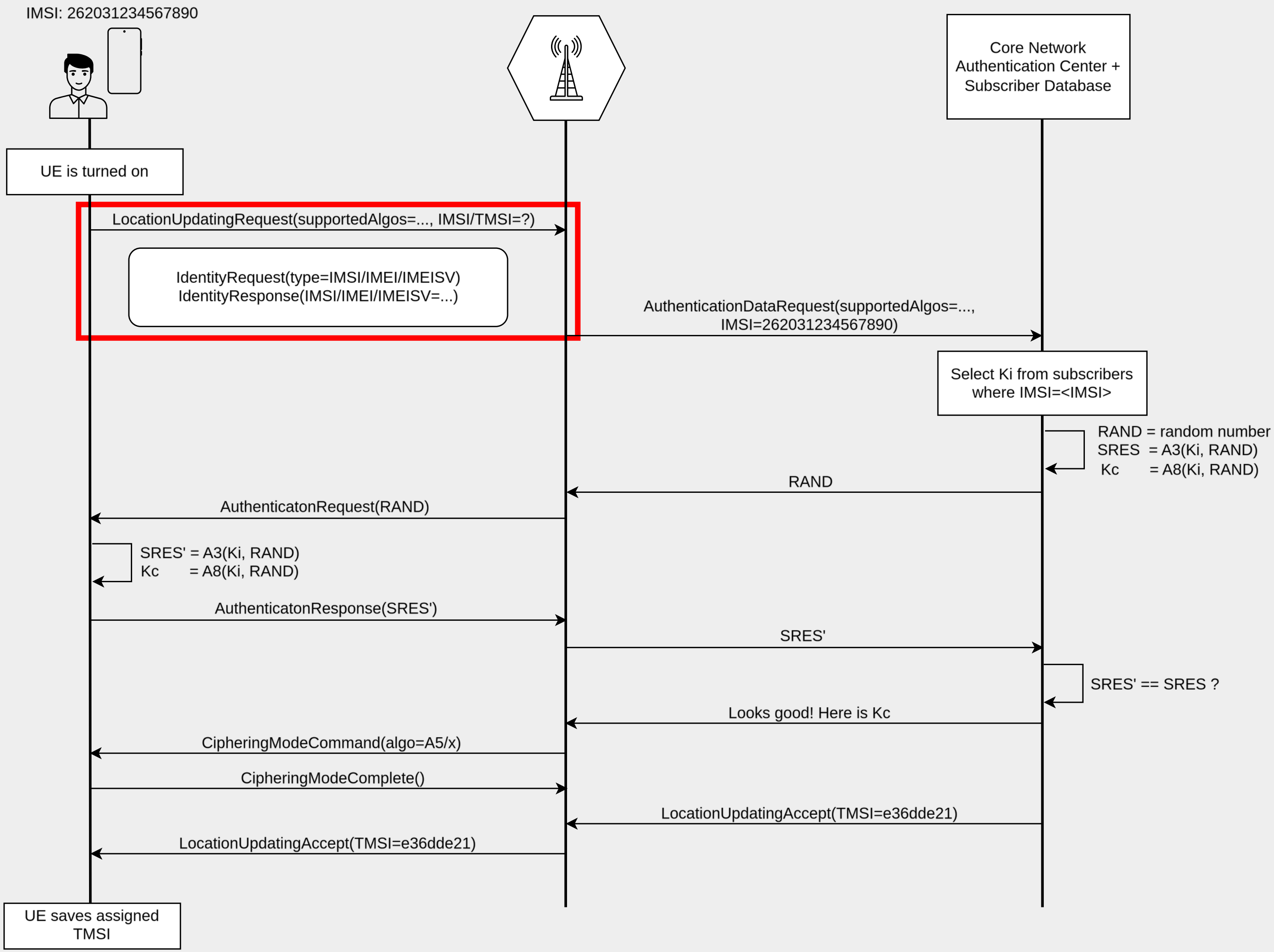
There are several occasions where IMSIs might be sent in **cleartext** over RF.

2G:

- Location Updating Request (if no TMSI is known to UE).
- Paging Request (if no TMSI is known or paging with TMSI does not yield Paging Response).
- Paging Response (if Paging Request included IMSI).
- Identity Response (type=IMSI).

[Fei19],[Jov16]

2G



IMSI: 262031234567890

Core Network
Authentication Center +
Subscriber Database

UE is turned on

LocationUpdatingRequest(supportedAlgos=..., IMSI/TMSI=?)

IdentityRequest(type=IMSI/IMEI/IMEISV)
IdentityResponse(IMSI/IMEI/IMEISV=...)

AuthenticationDataRequest(supportedAlgos=...,
IMSI=262031234567890)

Select Ki from subscribers
where IMSI=<IMSI>

RAND = random number
SRES = A3(Ki, RAND)
Kc = A8(Ki, RAND)

RAND

AuthenticatonRequest(RAND)

SRES' = A3(Ki, RAND)
Kc = A8(Ki, RAND)

AuthenticatonResponse(SRES')

SRES'

SRES' == SRES ?

Looks good! Here is Kc

CipheringModeCommand(algo=A5/x)

CipheringModeComplete()

LocationUpdatingAccept(TMSI=e36dde21)

LocationUpdatingAccept(TMSI=e36dde21)

UE saves assigned
TMSI

Attack 2.3a: IMSI-Catching (Passive)

There are several occasions where IMSIs might be sent in **cleartext** over RF.

2G:

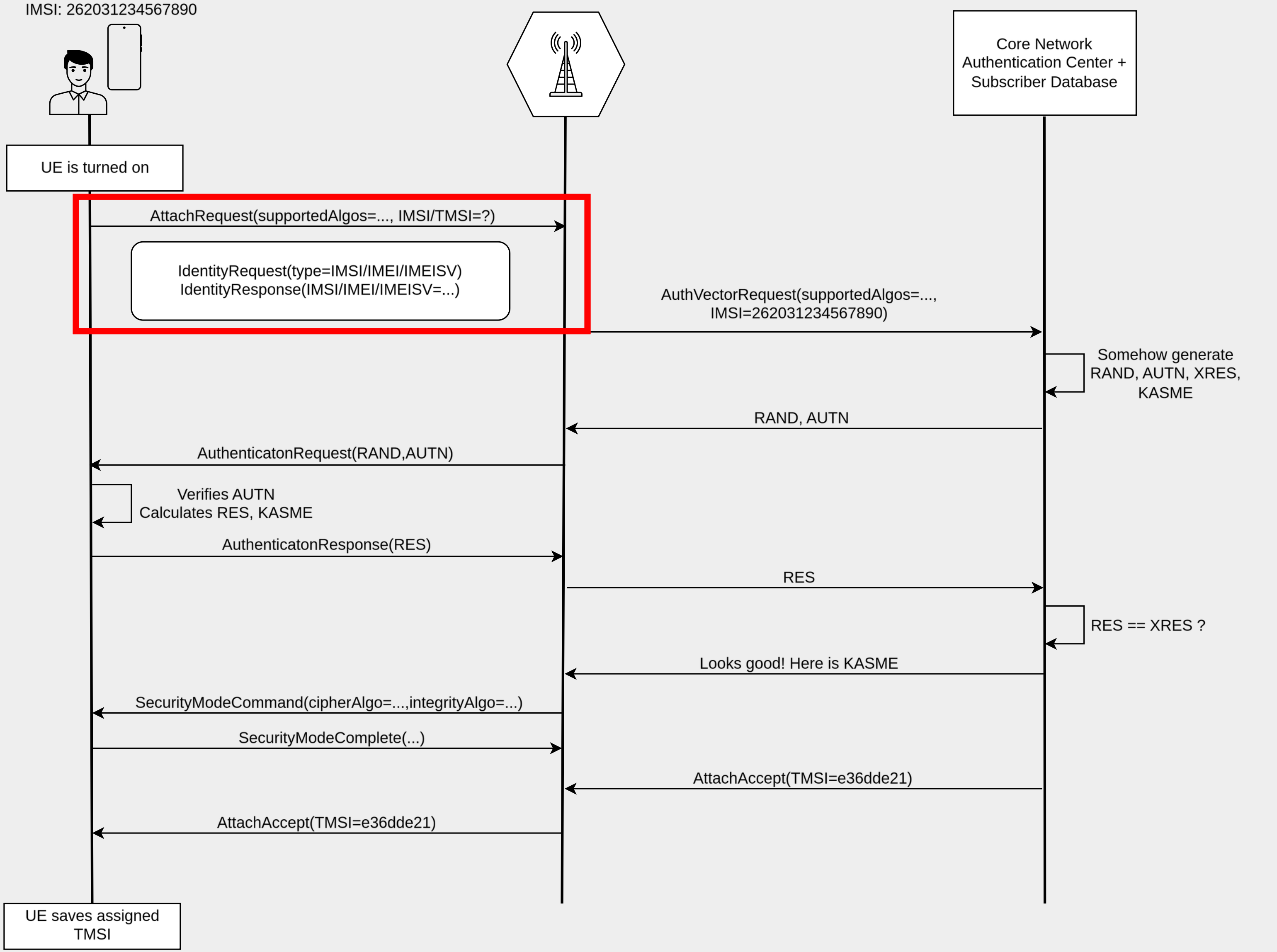
- Location Updating Request (if no TMSI is known to UE).
- Paging Request (if no TMSI is known or paging with TMSI does not yield Paging Response).
- Paging Response (if Paging Request included IMSI).
- Identity Response (type=IMSI).

4G:

- Initial AttachRequest (if no TMSI is known to UE).
- Paging Request (if no TMSI is known or paging with TMSI does not yield Paging Response).
- RRCConnectionRequest (if Paging Request included IMSI).
- Identity Response (type=IMSI).

[Fei19],[Jov16]

4G



IMSI: 262031234567890

Core Network
Authentication Center +
Subscriber Database

UE is turned on

AttachRequest(supportedAlgos=..., IMSI/TMSI=?)

IdentityRequest(type=IMSI/IMEI/IMEISV)
IdentityResponse(IMSI/IMEI/IMEISV=...)

AuthVectorRequest(supportedAlgos=...,
IMSI=262031234567890)

Somehow generate
RAND, AUTN, XRES,
KASME

RAND, AUTN

AuthenticatonRequest(RAND,AUTN)

Verifies AUTN
Calculates RES, KASME

AuthenticatonResponse(RES)

RES

RES == XRES ?

Looks good! Here is KASME

SecurityModeCommand(cipherAlgo=...,integrityAlgo=...)

SecurityModeComplete(...)

AttachAccept(TMSI=e36dde21)

AttachAccept(TMSI=e36dde21)

UE saves assigned
TMSI

Attack 2.3a: IMSI-Catching (Passive)

There are several occasions where IMSIs might be sent in **cleartext** over RF.

5G-NSA:

- Non-Standalone-Mode uses LTE Core Network.
- Also the Authentication Procedure is the **same as in 4G**.
- Only improvement is faster speed through improved RF specifications in 5G.

→ Same Attacks as in 4G possible.

5G-SA:

- Has its own Core Network called “5GC” (5G Core).
- IMSI is **never** sent in **cleartext** over RF.
- SUPI = IMSI equivalent
- SUCI = ECIES_encrypt(SUPI, public_key_of_operator)

→ No passive IMSI-Catching possible.

[Fei19],[Jov16]

Attack 2.3b: IMSI-Catching (Active)

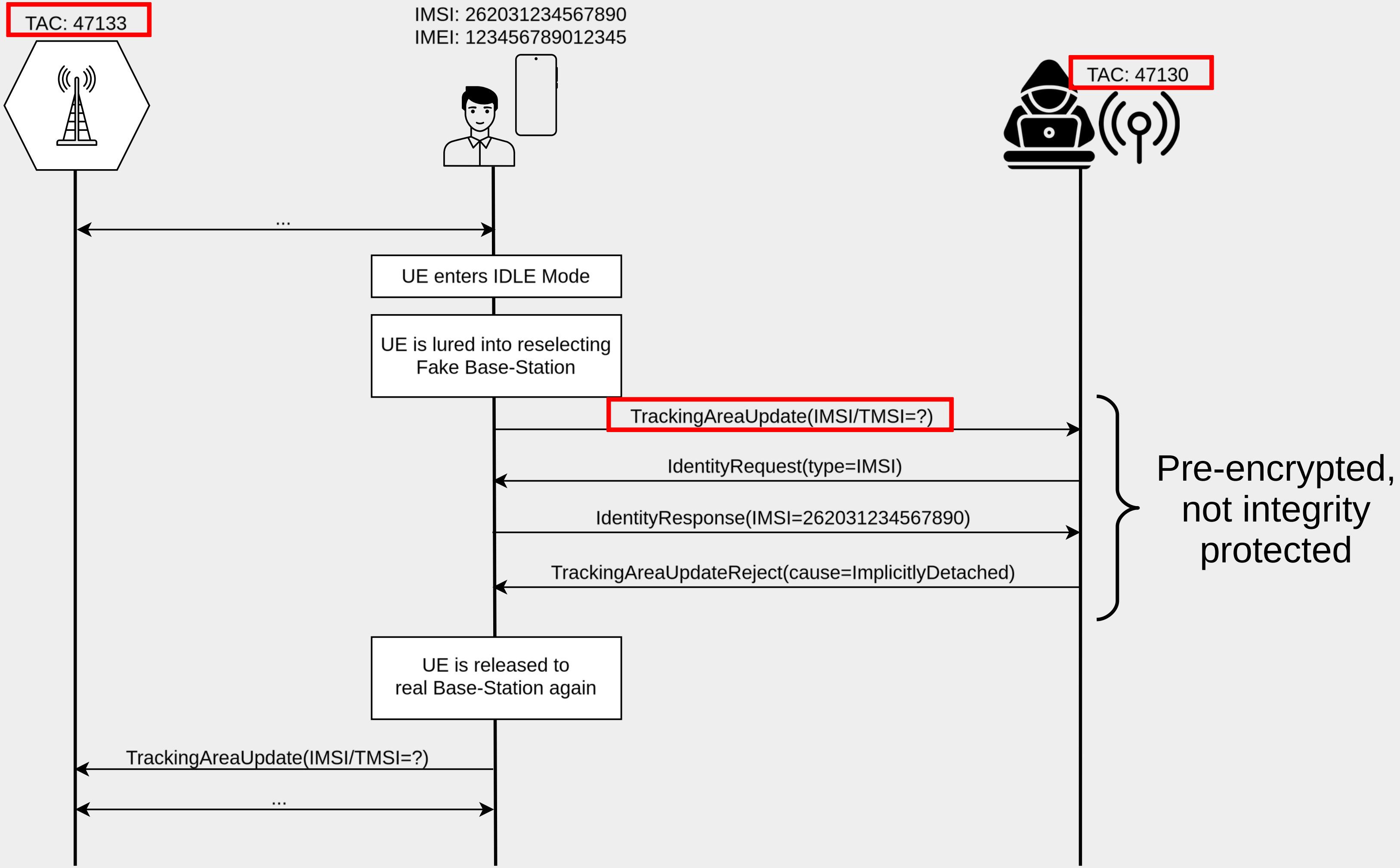
- Exploits the fact that **IdentityRequest**/**IdentityResponse** messages can be exchanged **pre-authenticated**.
- Requires UE to **reselect** from current legitimate cell to our fake Base-Station (we'll see how that works later).
- We can then initiate an **IdentityRequest** to get the IMSI.
- After IMSI leak, UE is released as quickly as possible to avoid detection. This can be done via:
  - TrackingAreaUpdate Reject Message
  - Changing Frequencies / shutting IMSI-Catcher down.
  - RRCConnectionRelease
  - ...

→ All that happens in **less than a second**!

[Fei19],[Jov16],[Got19]

Attack 2.3b: IMSI-Catching (Active)

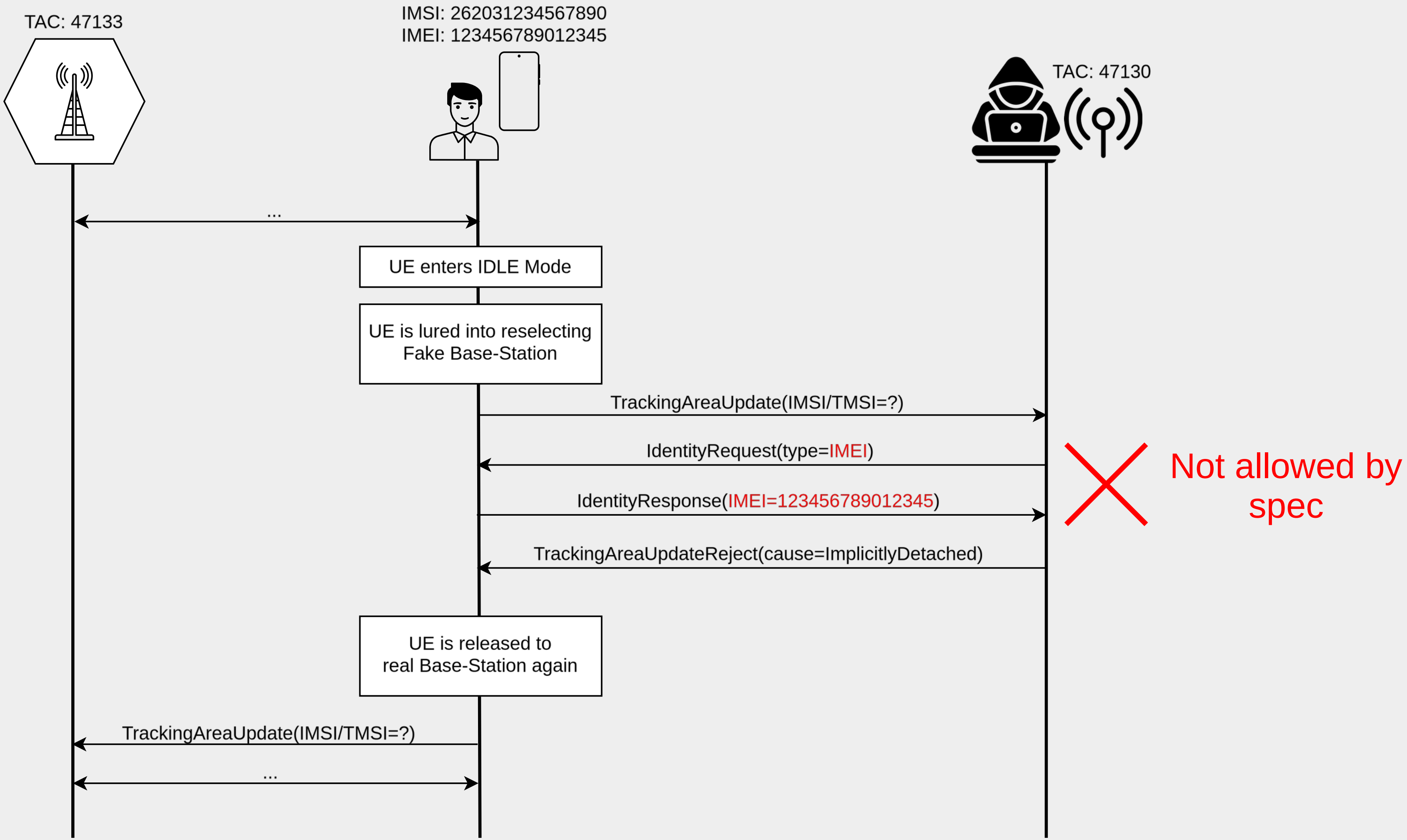
4G



TAC: 47133
IMSI: 262031234567890
IMEI: 123456789012345
TAC: 47130
...
UE enters IDLE Mode
UE is lured into reselecting Fake Base-Station
TrackingAreaUpdate(IMSI/TMSI=?)
IdentityRequest(type=IMSI)
IdentityResponse(IMSI=262031234567890)
TrackingAreaUpdateReject(cause=ImplicitlyDetached)
Pre-encrypted, not integrity protected
UE is released to real Base-Station again
TrackingAreaUpdate(IMSI/TMSI=?)
...

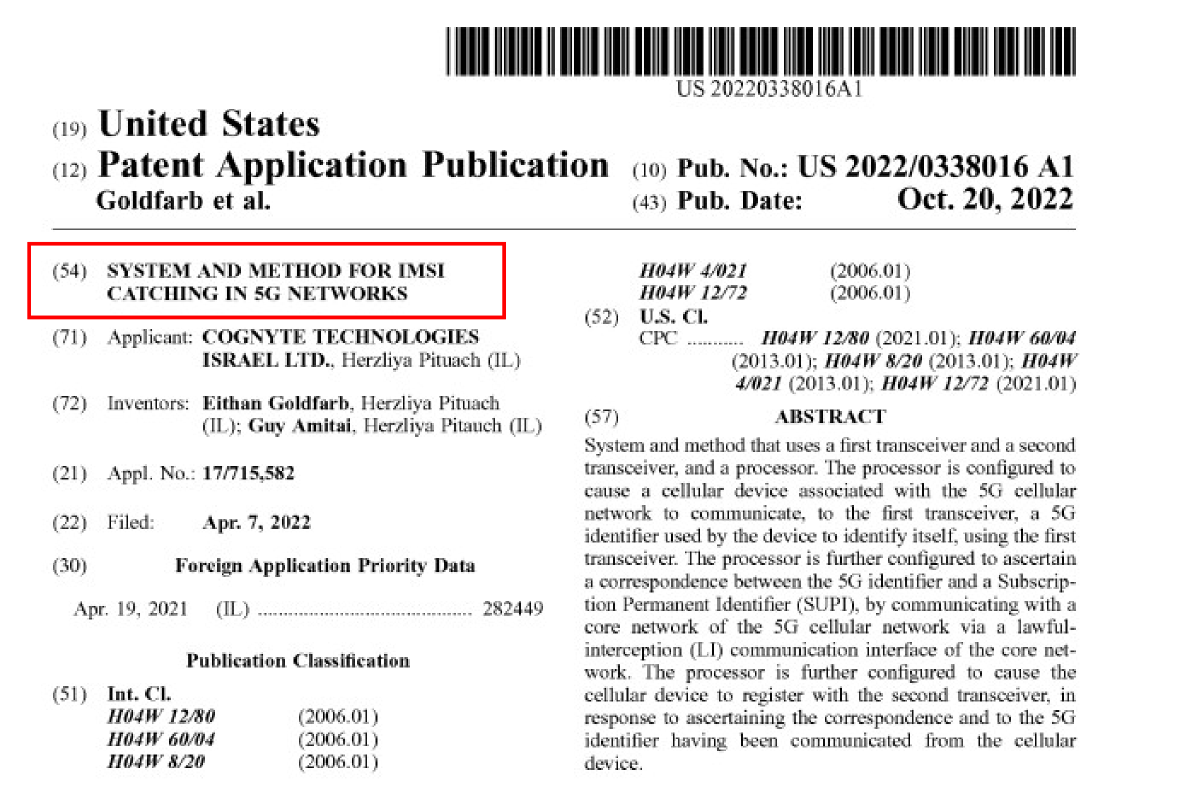
Attack 2.3b: IMSI-Catching (Active)

4G


TAC: 47133
IMSI: 262031234567890
IMEI: 123456789012345
TAC: 47130
...
UE enters IDLE Mode
UE is lured into reselecting Fake Base-Station
TrackingAreaUpdate(IMSI/TMSI=?)
IdentityRequest(type=IMEI)
IdentityResponse(IMEI=123456789012345)
Not allowed by spec
TrackingAreaUpdateReject(cause=ImplicitlyDetached)
UE is released to real Base-Station again
TrackingAreaUpdate(IMSI/TMSI=?)
...

Attack 2.3c: IMSI-Catching in 5G-SA (Active)

- Is substantially **harder** because of **encrypted SUCI**. May require additional capabilities such as Core Network Access.



US 20220338016A1

(19) **United States**

(12) **Patent Application Publication**
Goldfarb et al.

(10) **Pub. No.: US 2022/0338016 A1**

(43) **Pub. Date: Oct. 20, 2022**

(54) **SYSTEM AND METHOD FOR IMSI CATCHING IN 5G NETWORKS**

(71) Applicant: **COGNYTE TECHNOLOGIES ISRAEL LTD.**, Herzliya Pituach (IL)

(72) Inventors: **Eithan Goldfarb**, Herzliya Pituach (IL); **Guy Amitai**, Herzliya Pitauch (IL)

(21) Appl. No.: **17/715,582**

(22) Filed: **Apr. 7, 2022**

(30) **Foreign Application Priority Data**

Apr. 19, 2021 (IL) 282449

Publication Classification

(51) **Int. Cl.**

H04W 12/80	(2006.01)
H04W 60/04	(2006.01)
H04W 8/20	(2006.01)
H04W 4/021	(2006.01)
H04W 12/72	(2006.01)

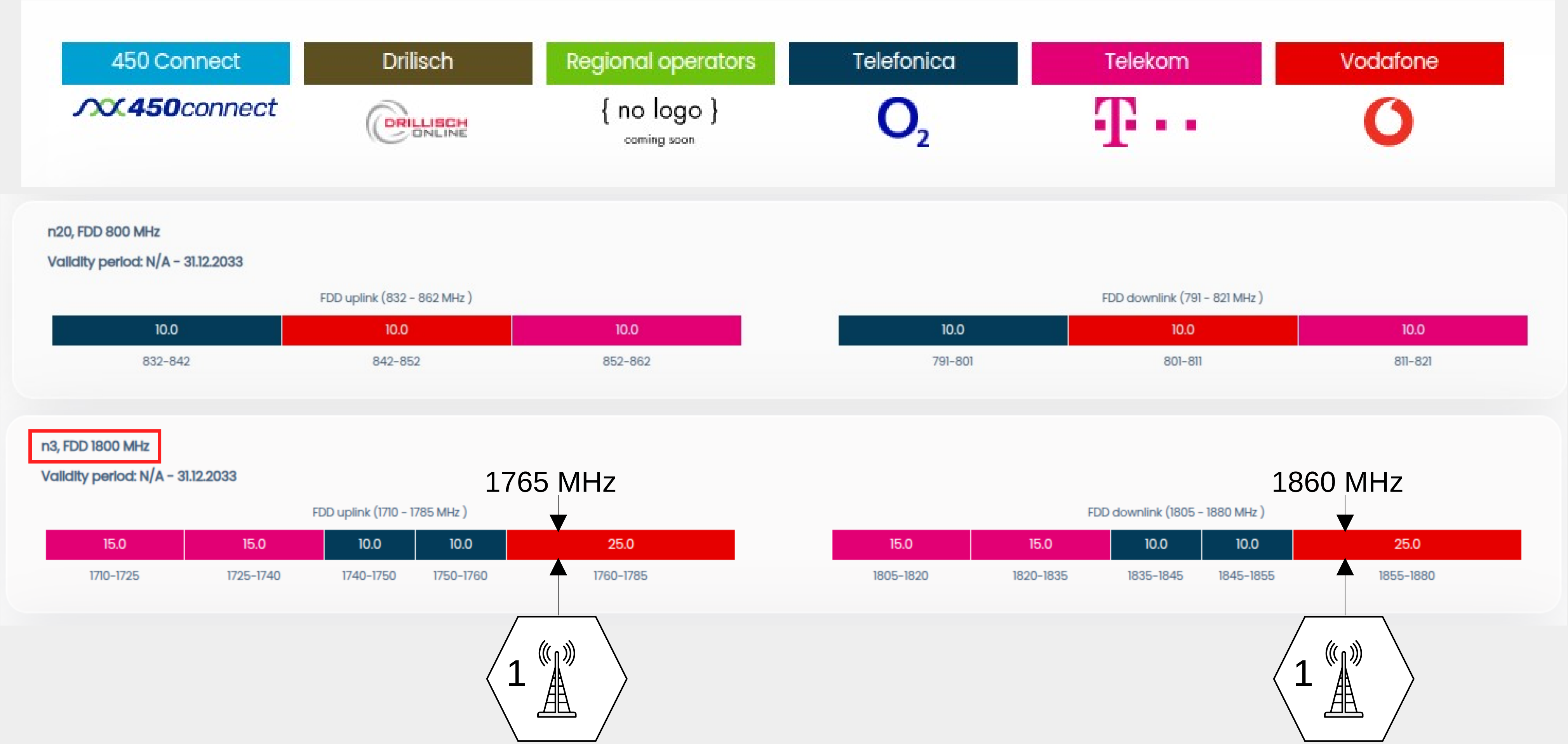
(52) **U.S. Cl.**
CPC ***H04W 12/80*** (2021.01); ***H04W 60/04*** (2013.01); ***H04W 8/20*** (2013.01); ***H04W 4/021*** (2013.01); ***H04W 12/72*** (2021.01)

(57) **ABSTRACT**

System and method that uses a first transceiver and a second transceiver, and a processor. The processor is configured to cause a cellular device associated with the 5G cellular network to communicate, to the first transceiver, a 5G identifier used by the device to identify itself, using the first transceiver. The processor is further configured to ascertain a correspondence between the 5G identifier and a Subscription Permanent Identifier (SUPI), by communicating with a core network of the 5G cellular network via a lawful-interception (LI) communication interface of the core network. The processor is further configured to cause the cellular device to register with the second transceiver, in response to ascertaining the correspondence and to the 5G identifier having been communicated from the cellular device.

US Patent for IMSI-Catching in 5G-SA Networks [PaT]

Key Concept: Frequency Bands



450 Connect	Drilisch	Regional operators	Telefonica	Telekom	Vodafone
450connect	DRILLISCH ONLINE	{ no logo } coming soon	O2	T · ·	

n20, FDD 800 MHz

Validity period: N/A - 31.12.2033

FDD uplink (832 - 862 MHz)

10.0	10.0	10.0
832-842	842-852	852-862

FDD downlink (791 - 821 MHz)

10.0	10.0	10.0
791-801	801-811	811-821

n3, FDD 1800 MHz

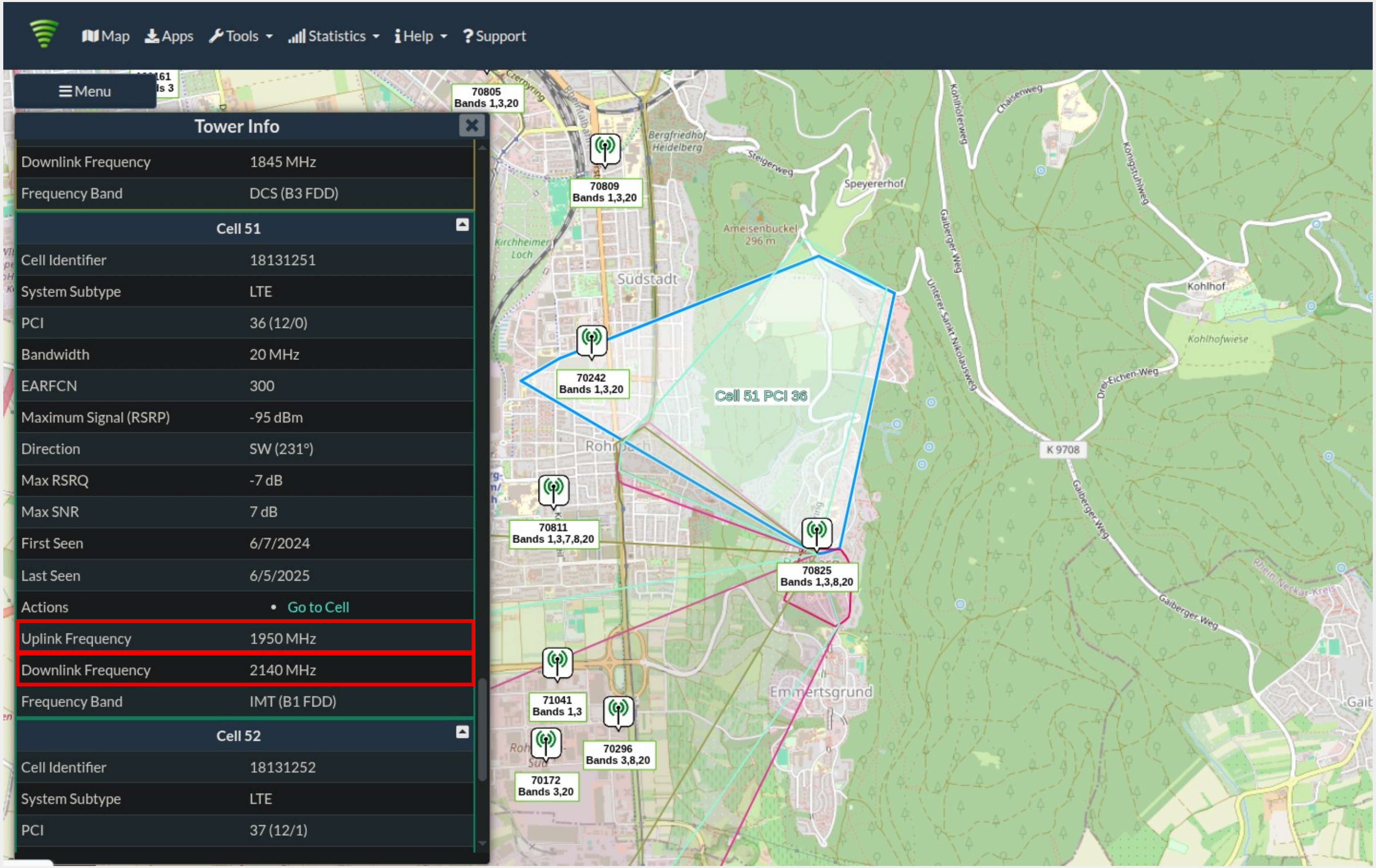
Validity period: N/A - 31.12.2033

FDD uplink (1710 - 1785 MHz)

15.0	15.0	10.0	10.0	25.0
1710-1725	1725-1740	1740-1750	1750-1760	1760-1785

FDD downlink (1805 - 1880 MHz)

15.0	15.0	10.0	10.0	25.0
1805-1820	1820-1835	1835-1845	1845-1855	1855-1880



Downlink Frequency	1845 MHz
Frequency Band	DCS (B3 FDD)
Cell 51	
Cell Identifier	18131251
System Subtype	LTE
PCI	36 (12/0)
Bandwidth	20 MHz
EARFCN	300
Maximum Signal (RSRP)	-95 dBm
Direction	SW (231°)
Max RSRQ	-7 dB
Max SNR	7 dB
First Seen	6/7/2024
Last Seen	6/5/2025
Actions	- Go to Cell
Uplink Frequency	1950 MHz
Downlink Frequency	2140 MHz
Frequency Band	IMT (B1 FDD)
Cell 52	
Cell Identifier	18131252
System Subtype	LTE
PCI	37 (12/1)

[cellmapper.net]

Attack 2.4: Cell Reselection

Generally UEs prefer **faster** generations.

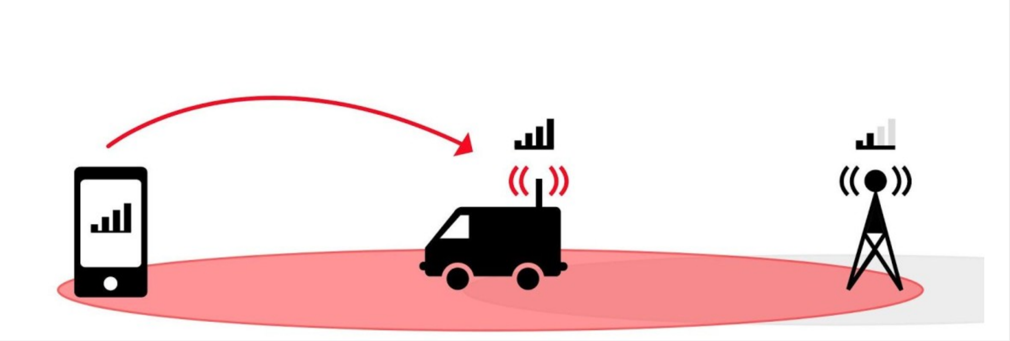
Intra-RAT, inter-frequency cell reselection behavior in ...

...2G:

- strongest signal wins.

How to force reselection:

- Open a fake base-station on an empty frequency band with stronger signal than real base-stations.
- The closer you are to an UE the stronger the signal.



[Got19]

Attack 2.4: Cell Reselection

Generally UEs prefer **faster** generations.

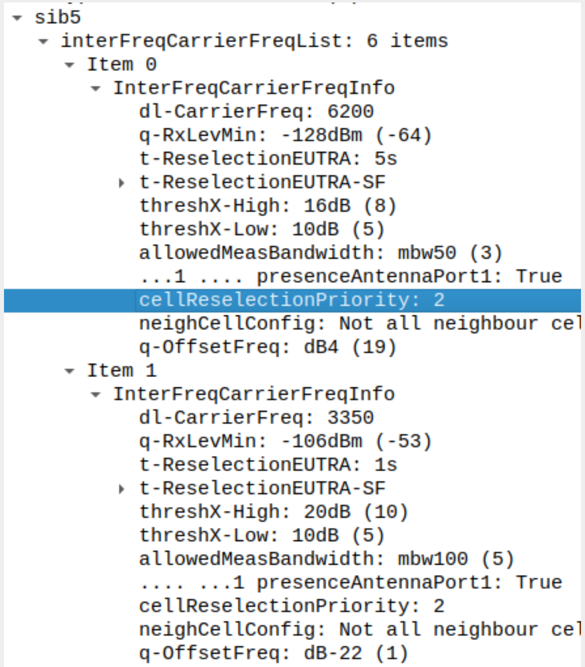
Intra-RAT, inter-frequency cell reselection behavior in ...

...3G/4G/5G:

- Base-Stations broadcast “nearest neighbor cells” list with priorities for each neighbor cell,
- if neighbor cell with higher priority gives better signal strength, reselect to it.
- Cell reselection is only performed in IDLE mode.

How to force reselection:

- Pick a victim Base-Station, extract its neighbor list
- Pick a higher priority cell from this list whose signal strength is also very poor.
- Open a fake Base-Station on the frequency band of that high priority cell, and make your signal better than that of real Base-Station.
- UEs in IDLE mode will now reselect to you.



```
▾ sib5
  ▾ interFreqCarrierFreqList: 6 items
    ▾ Item 0
      ▾ InterFreqCarrierFreqInfo
          dl-CarrierFreq: 6200
          q-RxLevMin: -128dBm (-64)
          t-ReselectionEUTRA: 5s
        ▸ t-ReselectionEUTRA-SF
          threshX-High: 16dB (8)
          threshX-Low: 10dB (5)
          allowedMeasBandwidth: mbw50 (3)
          ...1 .... presenceAntennaPort1: True
          cellReselectionPriority: 2
          neighCellConfig: Not all neighbour cel
          q-OffsetFreq: dB4 (19)
    ▾ Item 1
      ▾ InterFreqCarrierFreqInfo
          dl-CarrierFreq: 3350
          q-RxLevMin: -106dBm (-53)
          t-ReselectionEUTRA: 1s
        ▸ t-ReselectionEUTRA-SF
          threshX-High: 20dB (10)
          threshX-Low: 10dB (5)
          allowedMeasBandwidth: mbw100 (5)
          .... ...1 presenceAntennaPort1: True
          cellReselectionPriority: 2
          neighCellConfig: Not all neighbour cel
          q-OffsetFreq: dB-22 (1)
```

Example nearest neighbor list

[Got19],[Sha17]

Never Let Me Down Again – Downgrade Attacks

Downgrade Attacks are very **valuable**.

- **5G-SA to 4G**: Easier IMSI-Catching.
- **4G to 2G**: MitM Attacks, Call/SMS Decryption, etc.etc.etc.

One technique: Lure victim into **reselecting** our cell with different TAC, then send **NAS Reject Message**.

NAS Request Message	NAS Reject Message	Reject cause	Generation
TAU Request	TAU Reject	#7, **#42**	4G, 5G-NSA
Attach Request	Attach Reject	#7, **#42**	4G, 5G-NSA
Service Request	Service Reject	#7, **#42**	4G, 5G-NSA
Registration Request	Registration Reject	#7, **#27**	5G-SA

[Kar21]

Reject causes

4G/5G-NSA causes: [3GPP TS 24.301 Sec5.5.3.2.5]

Cause #7: “EPS services not allowed”:

> The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed or the timer T3245 expires.

Cause **#42**: “Severe Network Failure”:

> The UE […] shall disable the E-UTRA capability as long as the [implementation specific] timer is runnning.

5G-SA causes: [3GPP TS 24.501 Sec5.5.1.3.5]

Cause #7: “5GS services not allowed”:

> The UE shall consider the USIM as invalid for 5GS services until switching off, the UICC containing the USIM is removed or the timer T3245 expires.

Cause **#27**: “N1 mode not allowed”:

> The UE shall disable the N1 mode capability for the specific access type for which the message was received.

→ Exact behavior is **implementation defined**. Some codes may cause a **downgrade**, some **DoS**.

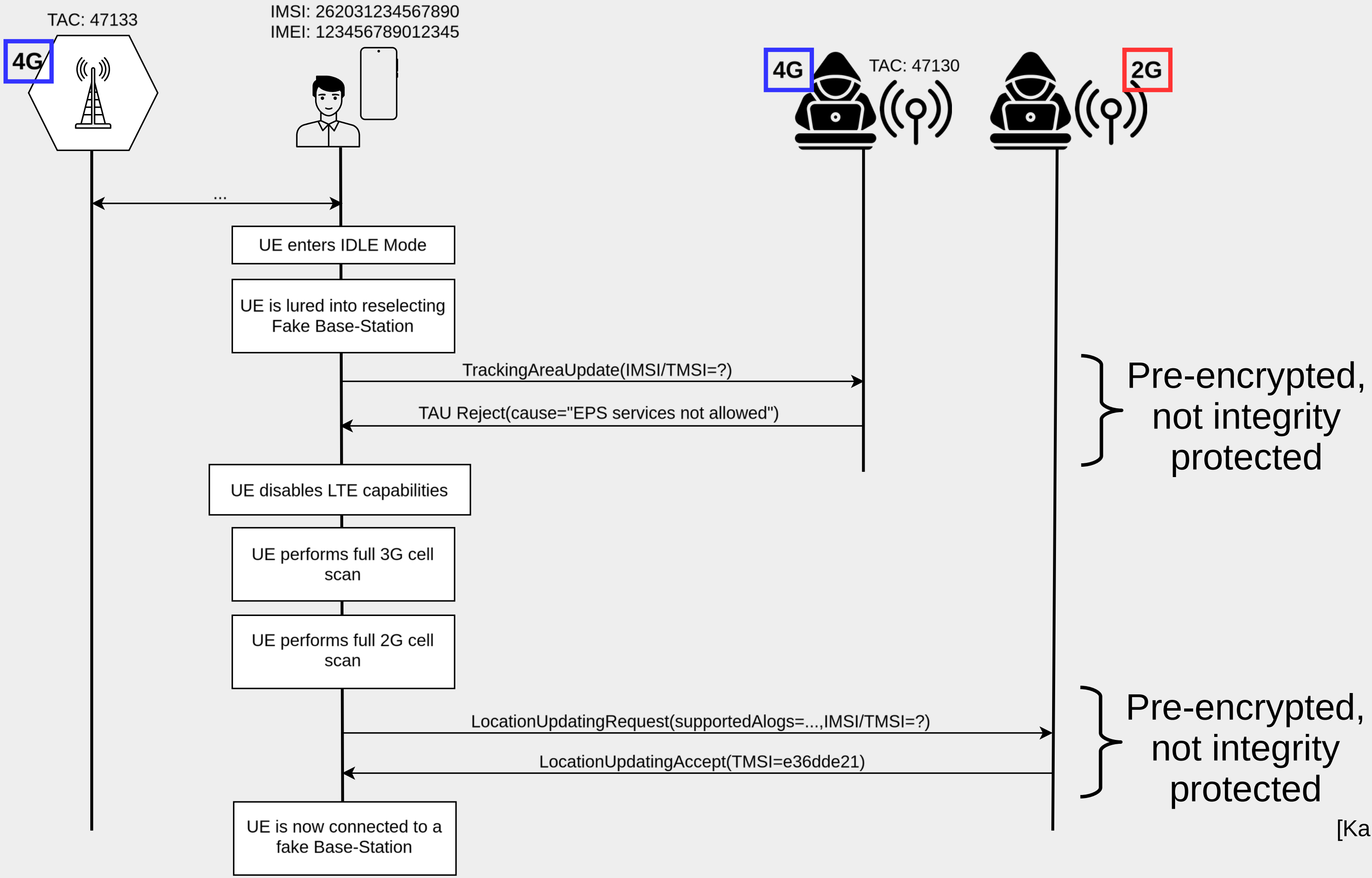
Sidenote: Denial-of-Service

4G/5G-NSA causes: [3GPP TS 24.301 Sec5.5.3.2.5]

Cause #8: “EPS services and non-EPS services not allowed”:

> The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed or the timer T3245 expires. […]. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed or the timer T3245 expires.

Attack 2.5: Downgrade Dance

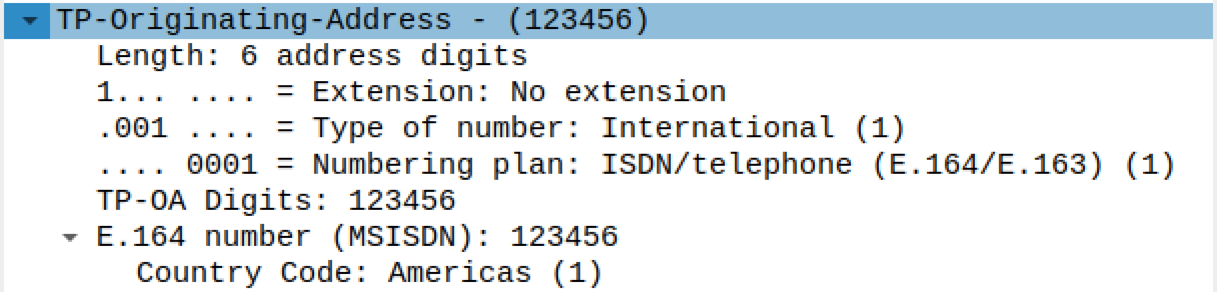


TAC: 47133
4G
IMSI: 262031234567890
IMEI: 123456789012345
4G
TAC: 47130
2G
...
UE enters IDLE Mode
UE is lured into reselecting Fake Base-Station
TrackingAreaUpdate(IMSI/TMSI=?)
TAU Reject(cause="EPS services not allowed")
UE disables LTE capabilities
UE performs full 3G cell scan
UE performs full 2G cell scan
LocationUpdatingRequest(supportedAlogs=...,IMSI/TMSI=?)
LocationUpdatingAccept(TMSI=e36dde21)
UE is now connected to a fake Base-Station
Pre-encrypted, not integrity protected
Pre-encrypted, not integrity protected

[Kar21]

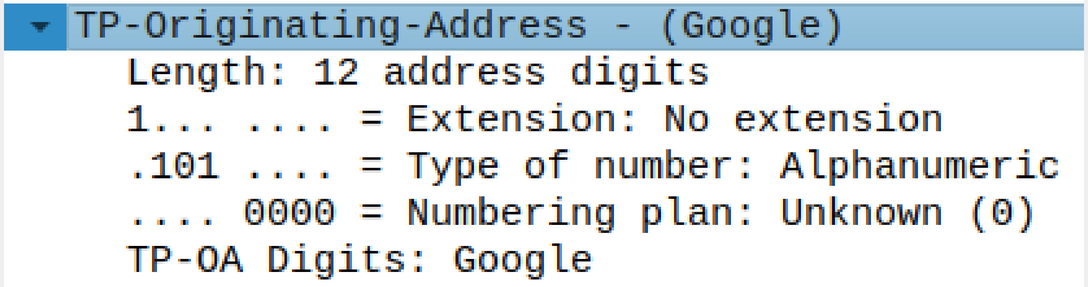
Attack 2.6: SMS Blasting

- SMS Protocol has **no** builtin **sender-id verification**.
- If the Base-Station is trusted from which the SMS is received, the SMS is trusted.



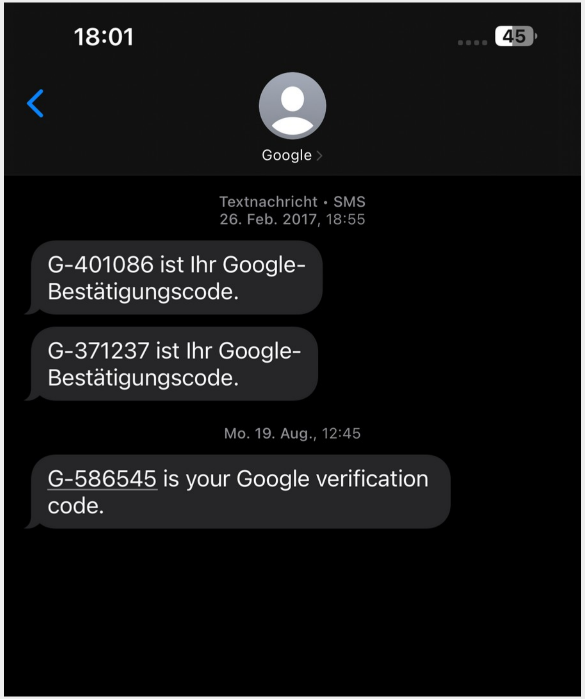
```
▾ TP-Originating-Address - (123456)
    Length: 6 address digits
    1... .... = Extension: No extension
    .001 .... = Type of number: International (1)
    .... 0001 = Numbering plan: ISDN/telephone (E.164/E.163) (1)
    TP-OA Digits: 123456
  ▾ E.164 number (MSISDN): 123456
      Country Code: Americas (1)
```

Fake SMS with international number sender-id



```
▾ TP-Originating-Address - (Google)
    Length: 12 address digits
    1... .... = Extension: No extension
    .101 .... = Type of number: Alphanumeric
    .... 0000 = Numbering plan: Unknown (0)
    TP-OA Digits: Google
```

Fake SMS with alphanumeric sender-id



Textnachricht • SMS
26. Feb. 2017, 18:55

G-401086 ist Ihr Google-Bestätigungscode.

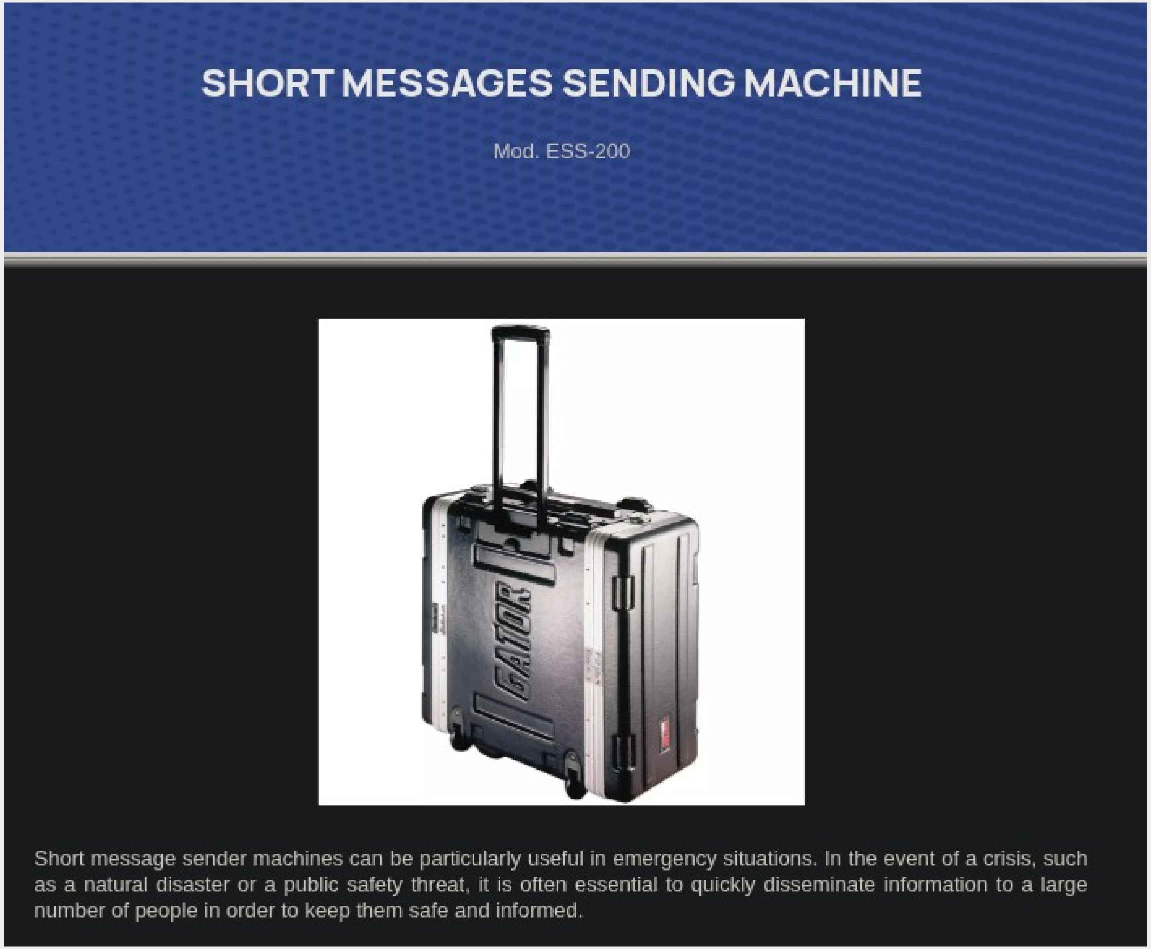
G-371237 ist Ihr Google-Bestätigungscode.

Mo. 19. Aug., 12:45

G-586545 is your Google verification code.

Many popular companies use alphanumeric sender-id

Commercial Options



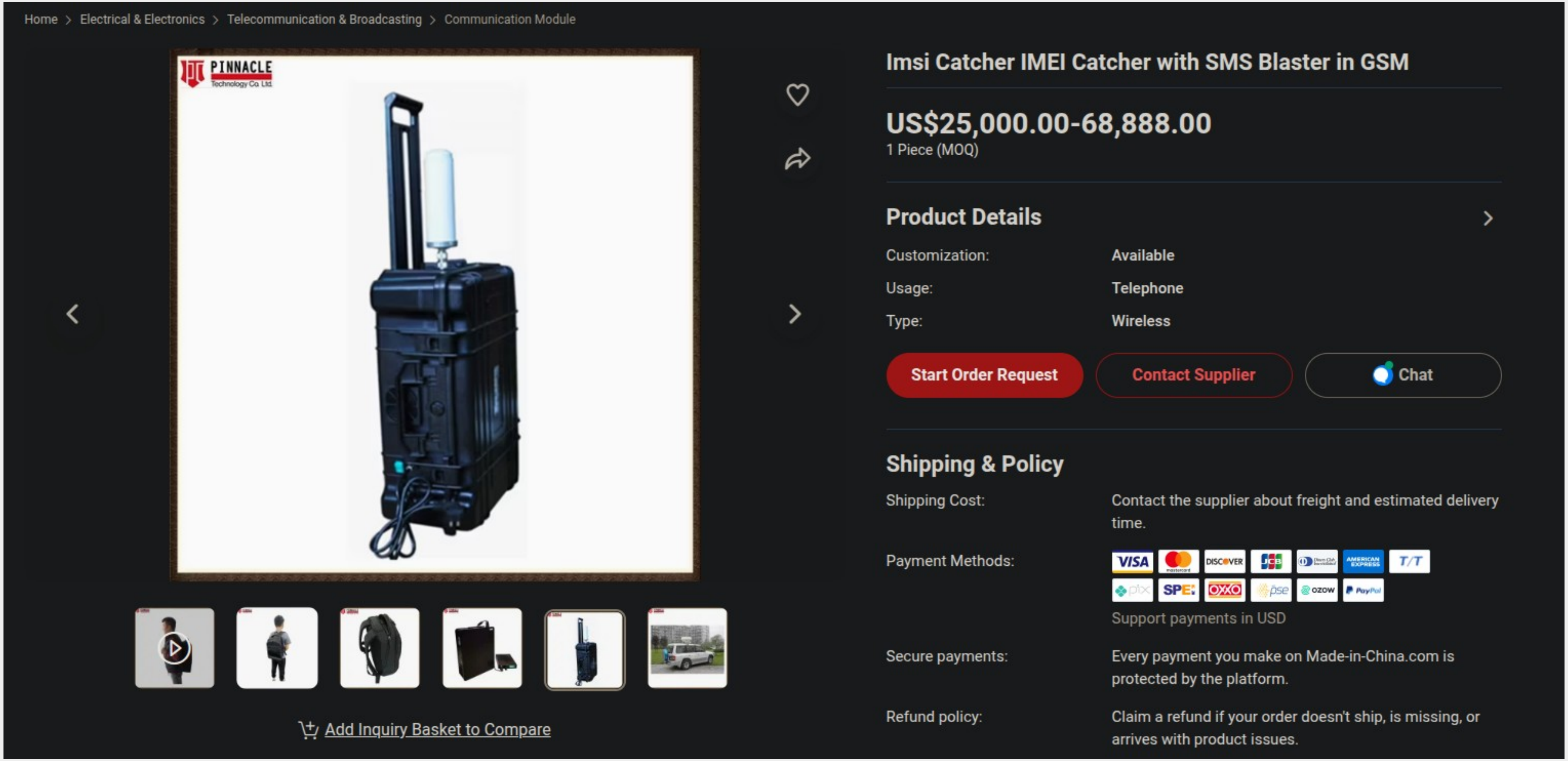
SHORT MESSAGES SENDING MACHINE

Mod. ESS-200

Short message sender machines can be particularly useful in emergency situations. In the event of a crisis, such as a natural disaster or a public safety threat, it is often essential to quickly disseminate information to a large number of people in order to keep them safe and informed.

A commercial SMS-Blaster from Proximus. [PoX]

Commercial Options



Home > Electrical & Electronics > Telecommunication & Broadcasting > Communication Module

Imsi Catcher IMEI Catcher with SMS Blaster in GSM

US$25,000.00-68,888.00

1 Piece (MOQ)

Product Details

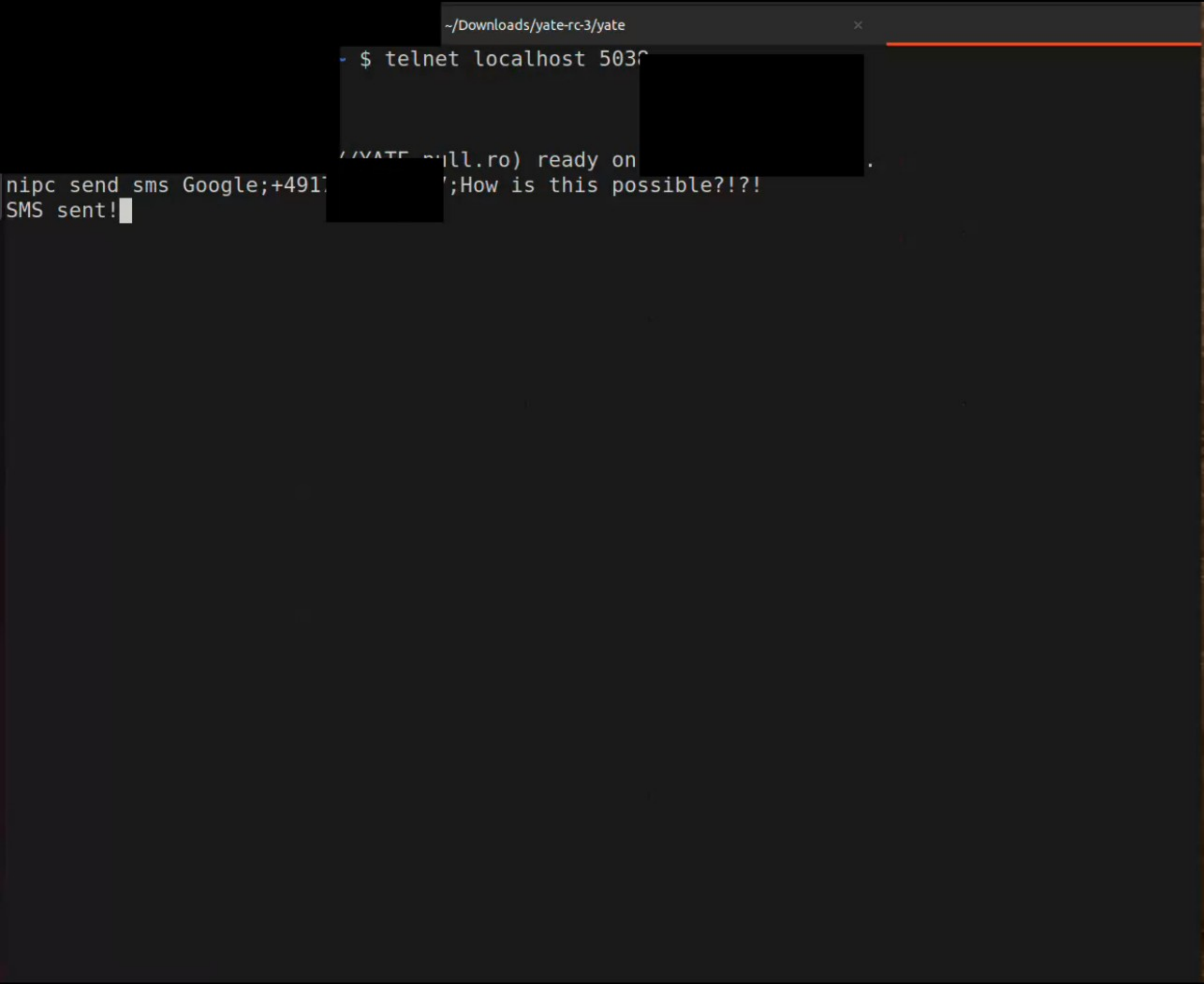
Customization:	Available
Usage:	Telephone
Type:	Wireless

Shipping & Policy

Shipping Cost:	Contact the supplier about freight and estimated delivery time.
Payment Methods:	VISA, DISCOVER, JCB, AMERICAN EXPRESS, T/T, pix, SPEI, OXXO, pse, ozow, PayPal Support payments in USD
Secure payments:	Every payment you make on Made-in-China.com is protected by the platform.
Refund policy:	Claim a refund if your order doesn't ship, is missing, or arrives with product issues.

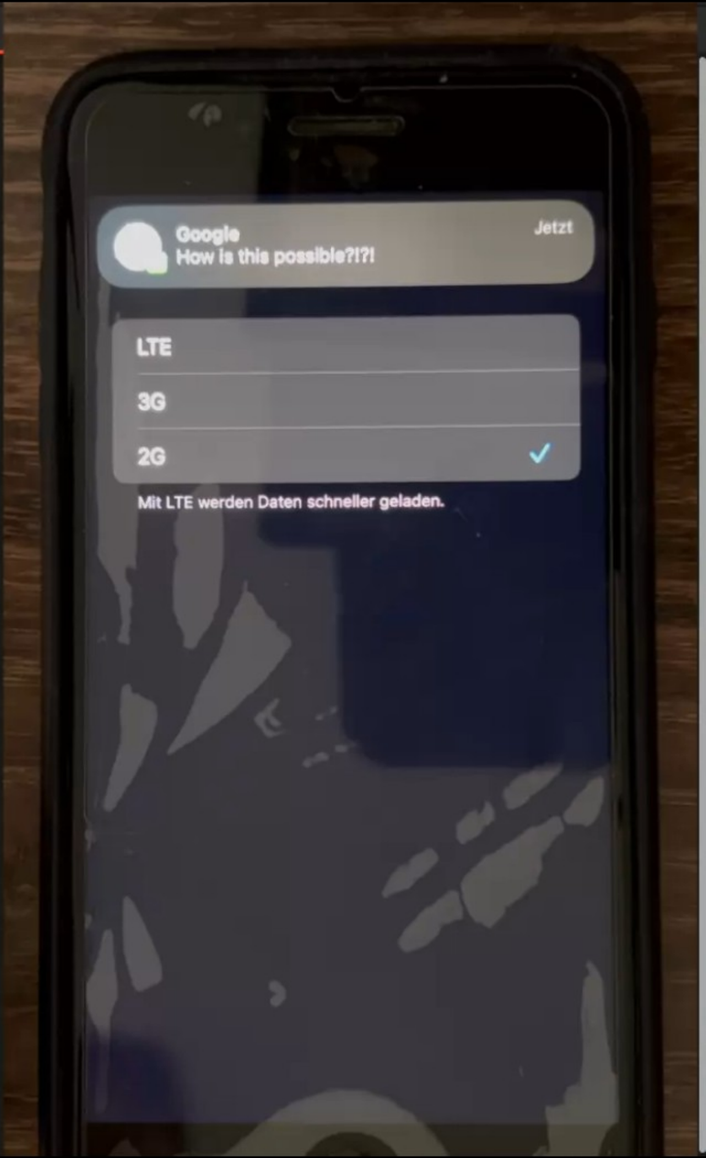
A commercial IMSI Catcher and SMS Blaster from Made-in-China.com [MiC]

Demo: SMS Blasting



~/Downloads/yate-rc-3/yate

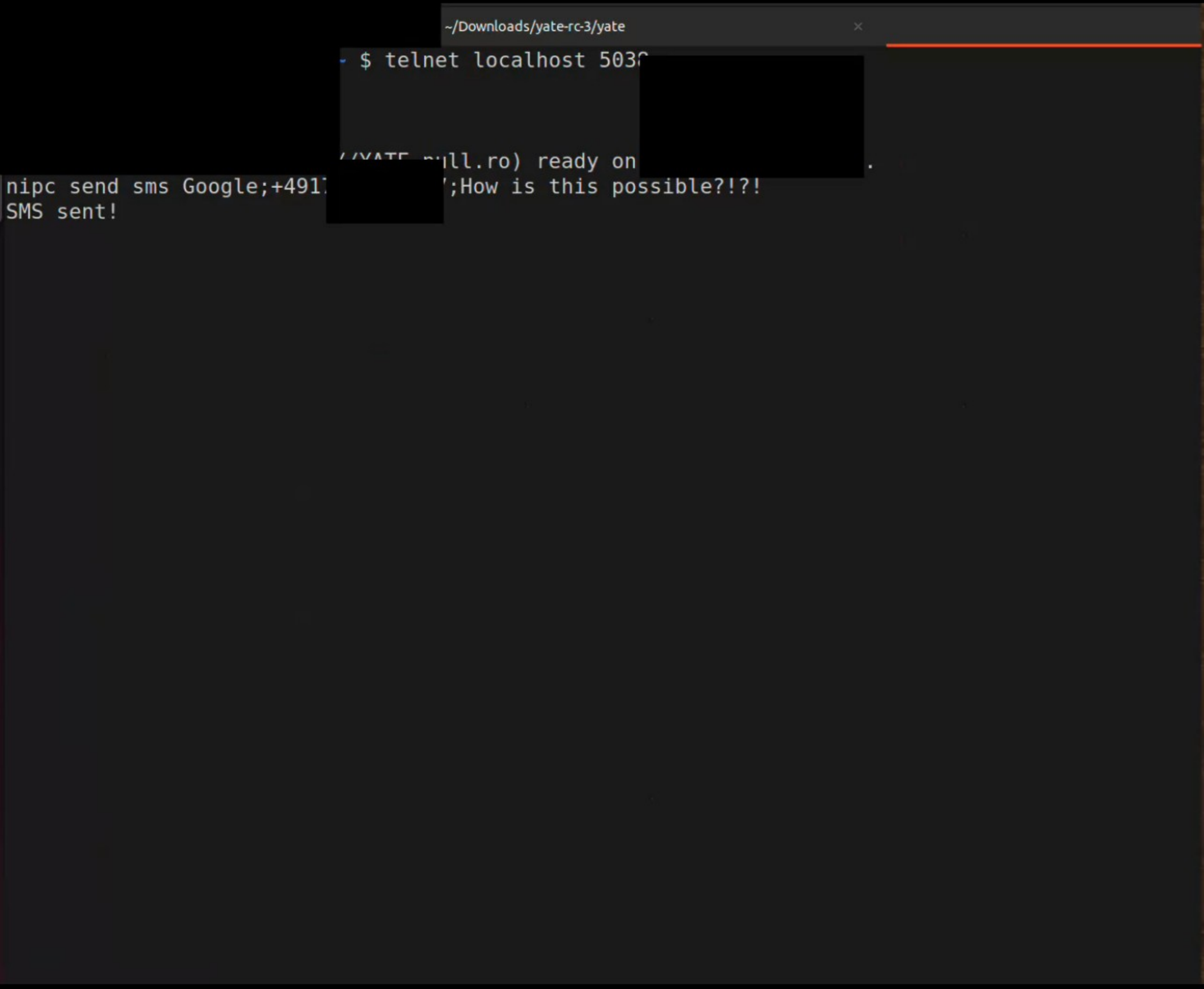
```
~ $ telnet localhost 503[redacted]

(YATE null.ro) ready on [redacted].
nipc send sms Google;+491[redacted];How is this possible?!?!
SMS sent!
```



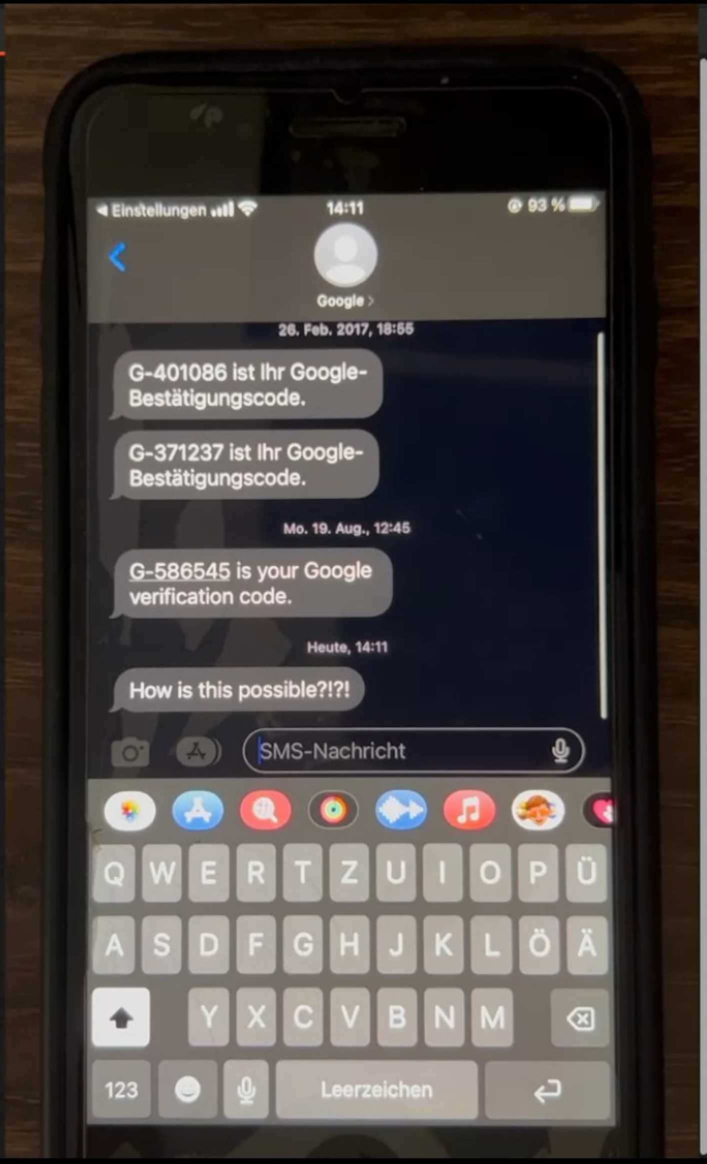
Google
How is this possible?!?!
Jetzt

LTE
3G
2G ✓

Mit LTE werden Daten schneller geladen.



```
~ $ telnet localhost 503[redacted]


//YATE null.ro) ready on .
nipc send sms Google;+491[redacted];How is this possible?!?!
SMS sent!
```



26. Feb. 2017, 18:55

G-401086 ist Ihr Google-Bestätigungscode.

G-371237 ist Ihr Google-Bestätigungscode.

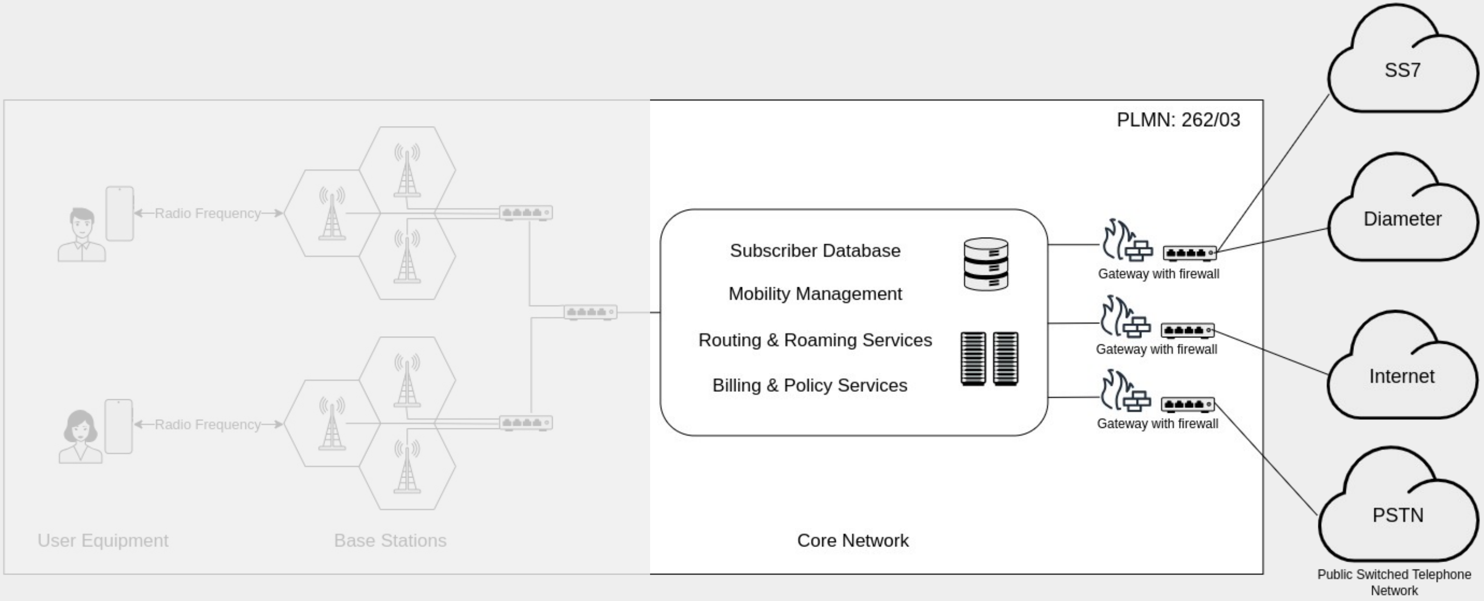
Mo. 19. Aug., 12:45

G-586545 is your Google verification code.

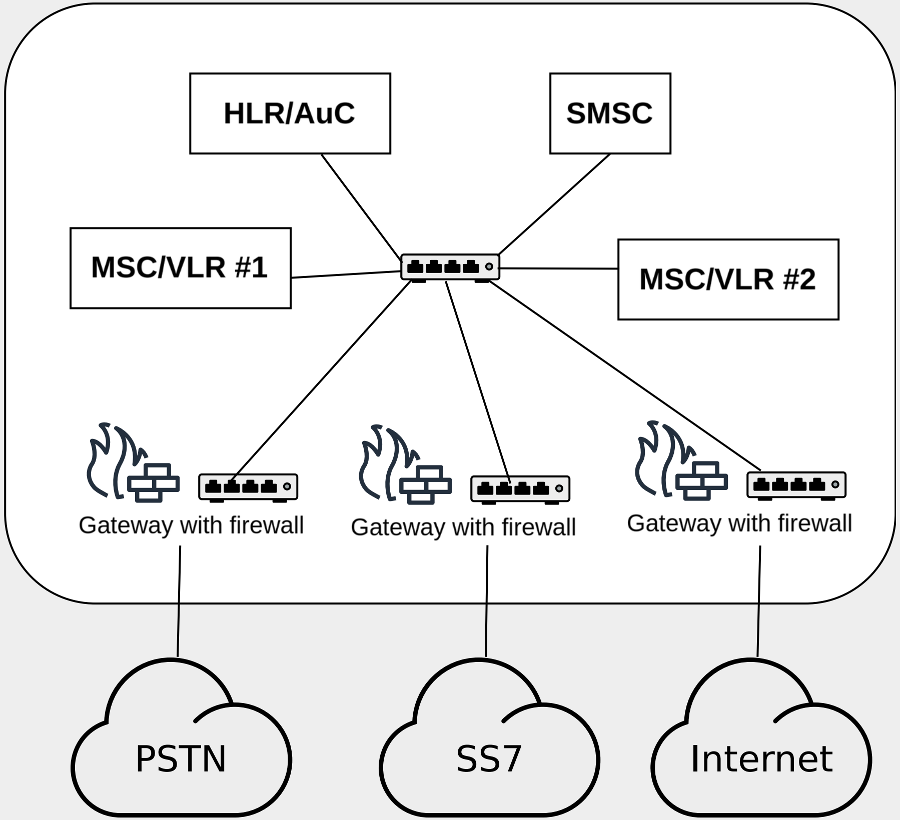
Heute, 14:11

How is this possible?!?!

Attack Surface #3: Core Network



GSM Core (2G)



HLR (Home Location Register):
Central database storing permanent subscriber data, including IMSI, MSISDN, services, and current location (VLR).

AuC (Authentication Center):
Security component linked to the HLR that stores secret keys and generates authentication vectors.

VLR (Visitor Location Register):
Temporary database that stores information about roaming subscribers currently served by a particular MSC.

MSC (Mobile Switching Center):
Core switching node that handles voice calls and mobility for circuit-switched services.

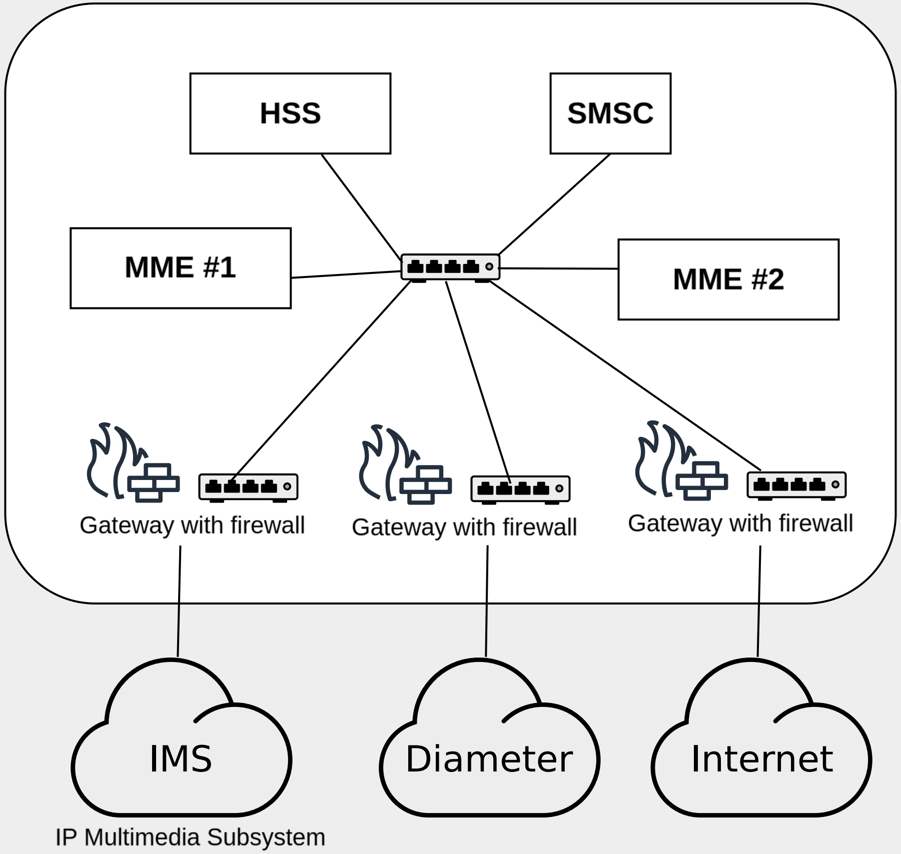
SMSC (SMS Center):
Handles store-and-forward delivery of SMS messages.

...

UMTS Core (3G)

- We skip this, nothing fancy to see here!

Evolved Packet Core (4G)



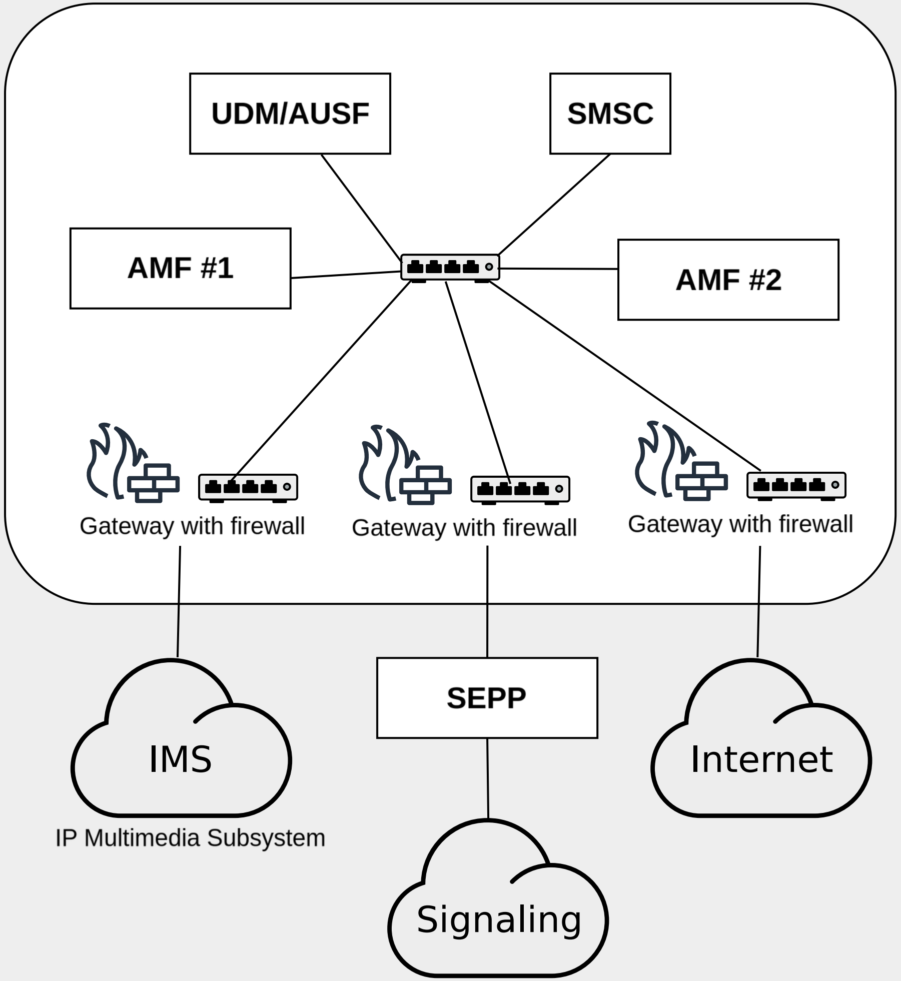
HSS (Home Subscriber Service):
Central database with user profiles, subscription data, and authentication credentials. Equivalent to HLR/AuC from 2G/3G.

MME (Mobility Management Entity):
Control-plane node responsible for user authentication, bearer management, and mobility (handover, tracking).

SMSC (SMS Center):
Handles store-and-forward delivery of SMS messages over IMS.

...

5G Core (5G-SA)



UDM (Unified Data Management): Stores subscriber data and profiles, handles subscription management and authentication data.

AUSF (Authentication Server Function): Responsible for authenticating subscribers, working closely with UDM.

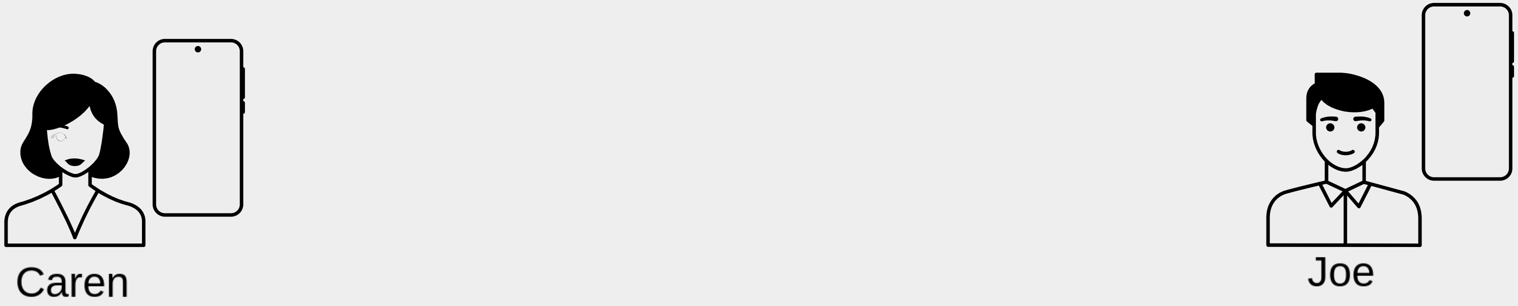
AMF (Access and Mobility Management Function): Manages UE registration, connection, reachability, mobility, and authentication. Acts as the entry point for signaling from the RAN.

SMSC (SMS Center): Handles store-and-forward delivery of SMS messages over IMS.

SEPP (Security Edge Protection Proxy): Secures inter-operator communication, protecting signaling messages between different operator networks.

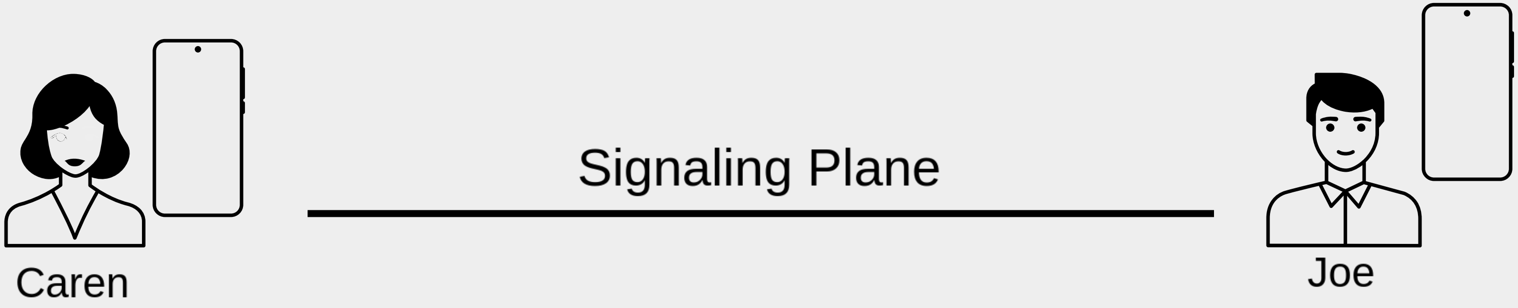
...

Signaling Networks



1. Locate both users
2. Authenticate them
3. Allocate radio and core network resources
4. Set up a call path

Signaling Networks



Signaling Plane

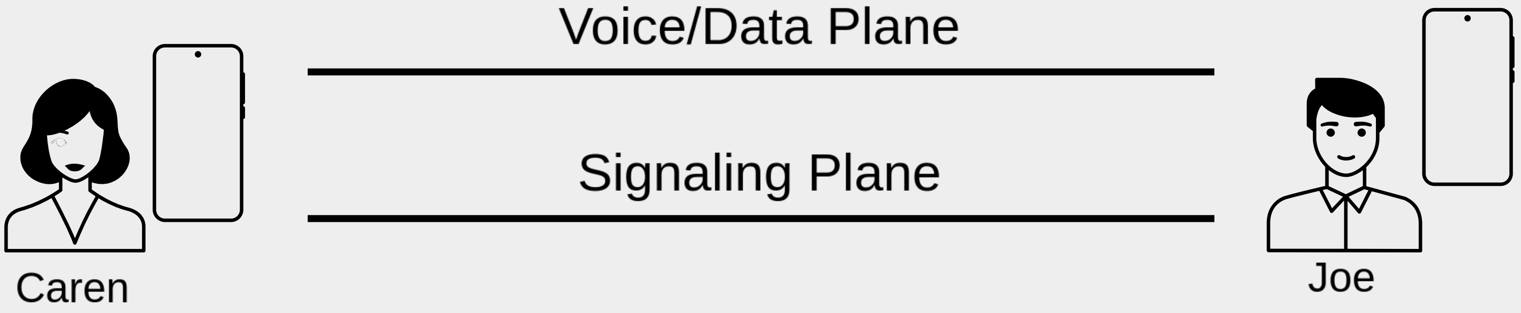
Caren

Joe

1. Locate both users
2. Authenticate them
3. Allocate radio and core network resources
4. Set up a call path
5. They can talk to each other

Signaling Plane

Signaling Networks



Voice/Data Plane

Signaling Plane

Caren

Joe

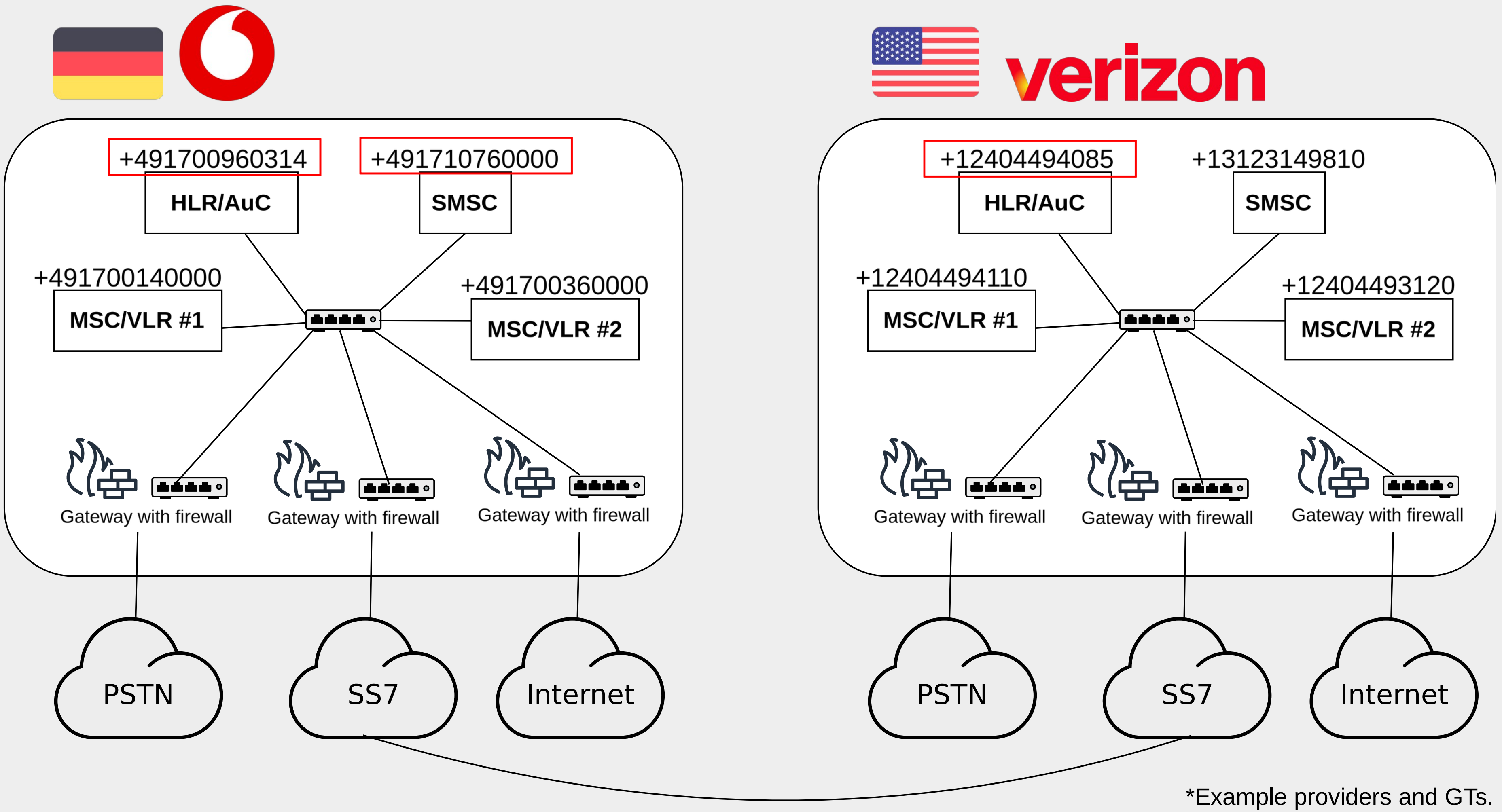
1. Locate both users
2. Authenticate them
3. Allocate radio and core network resources
4. Set up a call path
5. They can talk to each other
6. Tear everything down when the call ends

Signaling Plane

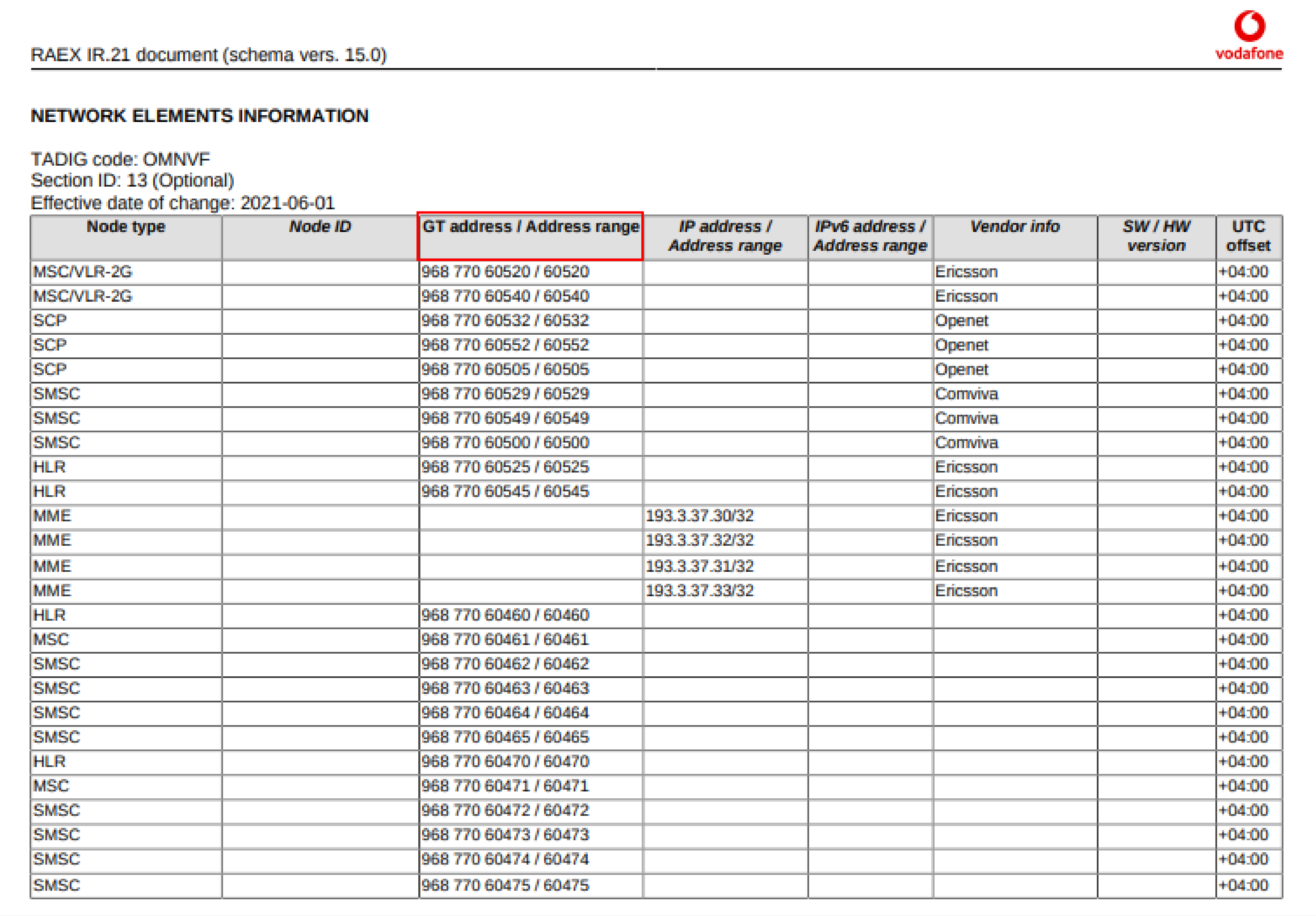
Voice/Data Plane

Signaling Plane

SS7 and Global Titles



*Example providers and GTs. Not real.



RAEX IR.21 document (schema vers. 15.0)

NETWORK ELEMENTS INFORMATION

TADIG code: OMNVF
Section ID: 13 (Optional)
Effective date of change: 2021-06-01

Node type	*Node ID*	GT address / Address range	*IP address / Address range*	*IPv6 address / Address range*	*Vendor info*	*SW / HW version*	UTC offset
MSC/VLR-2G		968 770 60520 / 60520			Ericsson		+04:00
MSC/VLR-2G		968 770 60540 / 60540			Ericsson		+04:00
SCP		968 770 60532 / 60532			Openet		+04:00
SCP		968 770 60552 / 60552			Openet		+04:00
SCP		968 770 60505 / 60505			Openet		+04:00
SMSC		968 770 60529 / 60529			Comviva		+04:00
SMSC		968 770 60549 / 60549			Comviva		+04:00
SMSC		968 770 60500 / 60500			Comviva		+04:00
HLR		968 770 60525 / 60525			Ericsson		+04:00
HLR		968 770 60545 / 60545			Ericsson		+04:00
MME			193.3.37.30/32		Ericsson		+04:00
MME			193.3.37.32/32		Ericsson		+04:00
MME			193.3.37.31/32		Ericsson		+04:00
MME			193.3.37.33/32		Ericsson		+04:00
HLR		968 770 60460 / 60460					+04:00
MSC		968 770 60461 / 60461					+04:00
SMSC		968 770 60462 / 60462					+04:00
SMSC		968 770 60463 / 60463					+04:00
SMSC		968 770 60464 / 60464					+04:00
SMSC		968 770 60465 / 60465					+04:00
HLR		968 770 60470 / 60470					+04:00
MSC		968 770 60471 / 60471					+04:00
SMSC		968 770 60472 / 60472					+04:00
SMSC		968 770 60473 / 60473					+04:00
SMSC		968 770 60474 / 60474					+04:00
SMSC		968 770 60475 / 60475					+04:00

Global Titles owned by Vodafone [IR21]

Global Title Leasing

Operators typically allocate a large GT block range. But not all GT addresses are used by the operator.
Idea: Lease them and make money!
Many businesses need GTs to build their own core-network or access other core-networks:

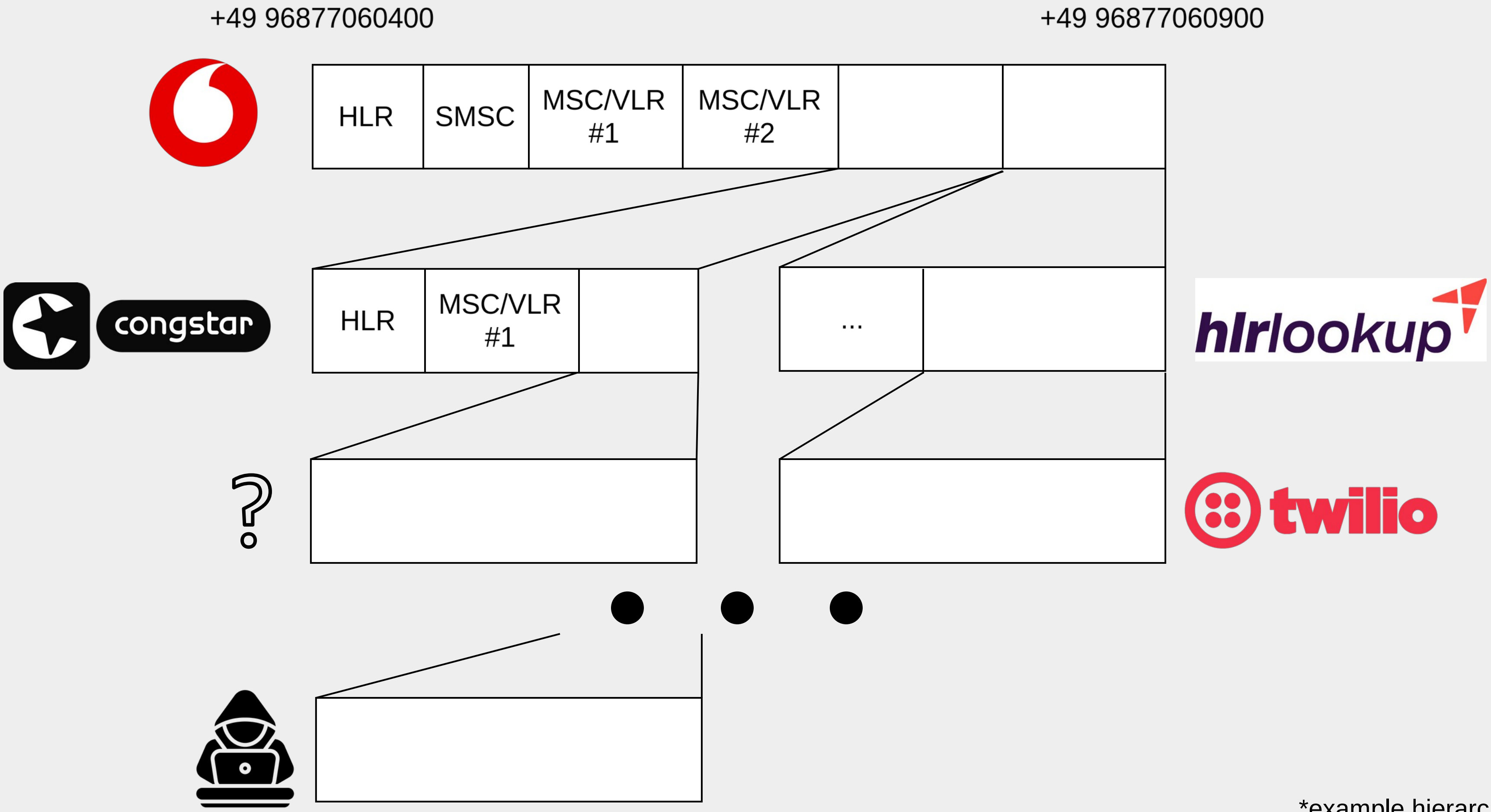
- Virtual Mobile Operators (e.g. Congstar, Aldi Talk, Freenet,etc.)
- Mobile Messaging Services (e.g. Twilio, OneSignal, etc.)
- Phone number verification services (e.g. Twilio, hlrlookup.com, etc.)

→ GT leasing spiral because everyone wants to make profit of unused GTs

→ Can you trust everyone down the line?

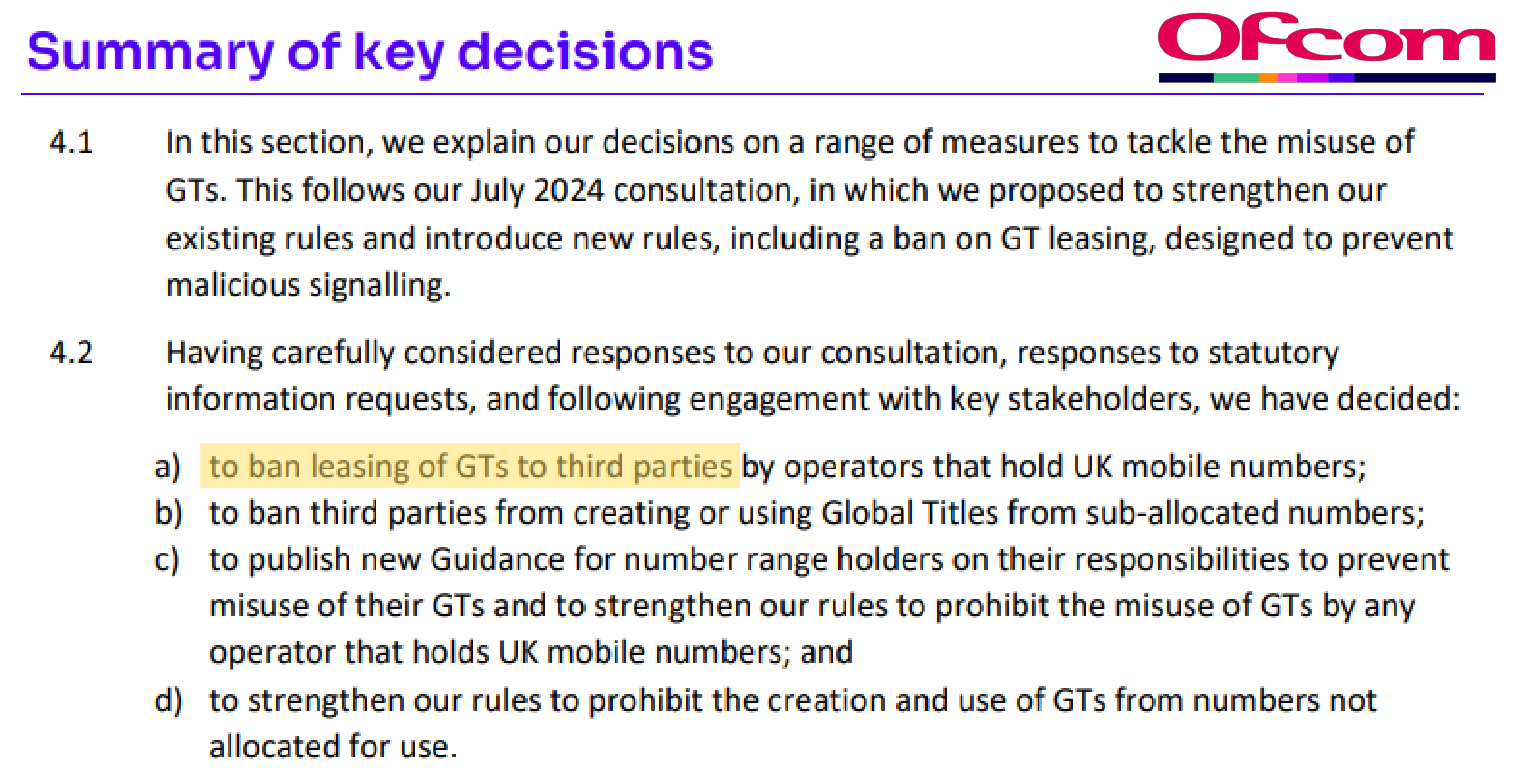
[Fin23],[SS718]

Global Title Leasing



*example hierarchy. Not real.

Sidenote: UK bans Global Title Leasing



Summary of key decisions

4.1 In this section, we explain our decisions on a range of measures to tackle the misuse of GTs. This follows our July 2024 consultation, in which we proposed to strengthen our existing rules and introduce new rules, including a ban on GT leasing, designed to prevent malicious signalling.

4.2 Having carefully considered responses to our consultation, responses to statutory information requests, and following engagement with key stakeholders, we have decided:

a) to ban leasing of GTs to third parties by operators that hold UK mobile numbers;

b) to ban third parties from creating or using Global Titles from sub-allocated numbers;

c) to publish new Guidance for number range holders on their responsibilities to prevent misuse of their GTs and to strengthen our rules to prohibit the misuse of GTs by any operator that holds UK mobile numbers; and

d) to strengthen our rules to prohibit the creation and use of GTs from numbers not allocated for use.

Statement by Ofcom to ban GT Leasing in UK [OfC]

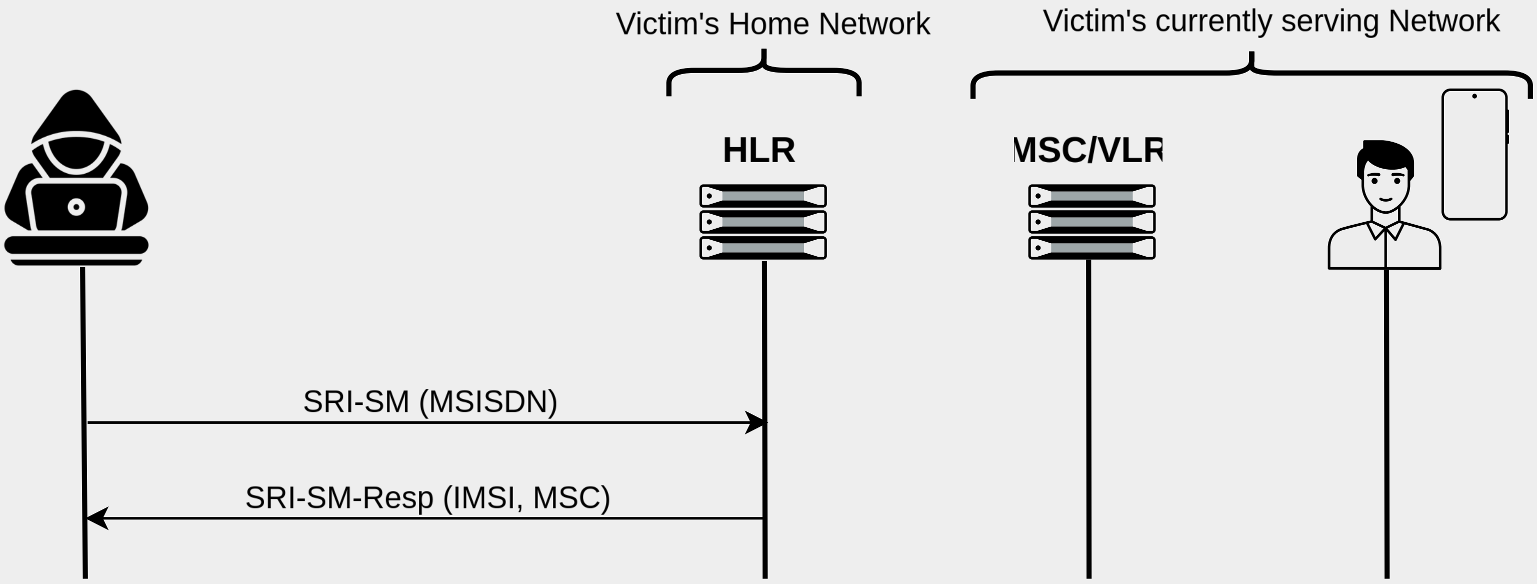
SS7 Security

- Has **no** built-in **authentication**.
- Once inside, there is little to no information about validity of message.
- Every message contains the **originating core network**, but who knows if it's from the **actual operator** or one of the **sub-lesses** with malicious intents.

→ Blocking valid requests may result in outage for roaming customers.

[Fin23],[SS718]

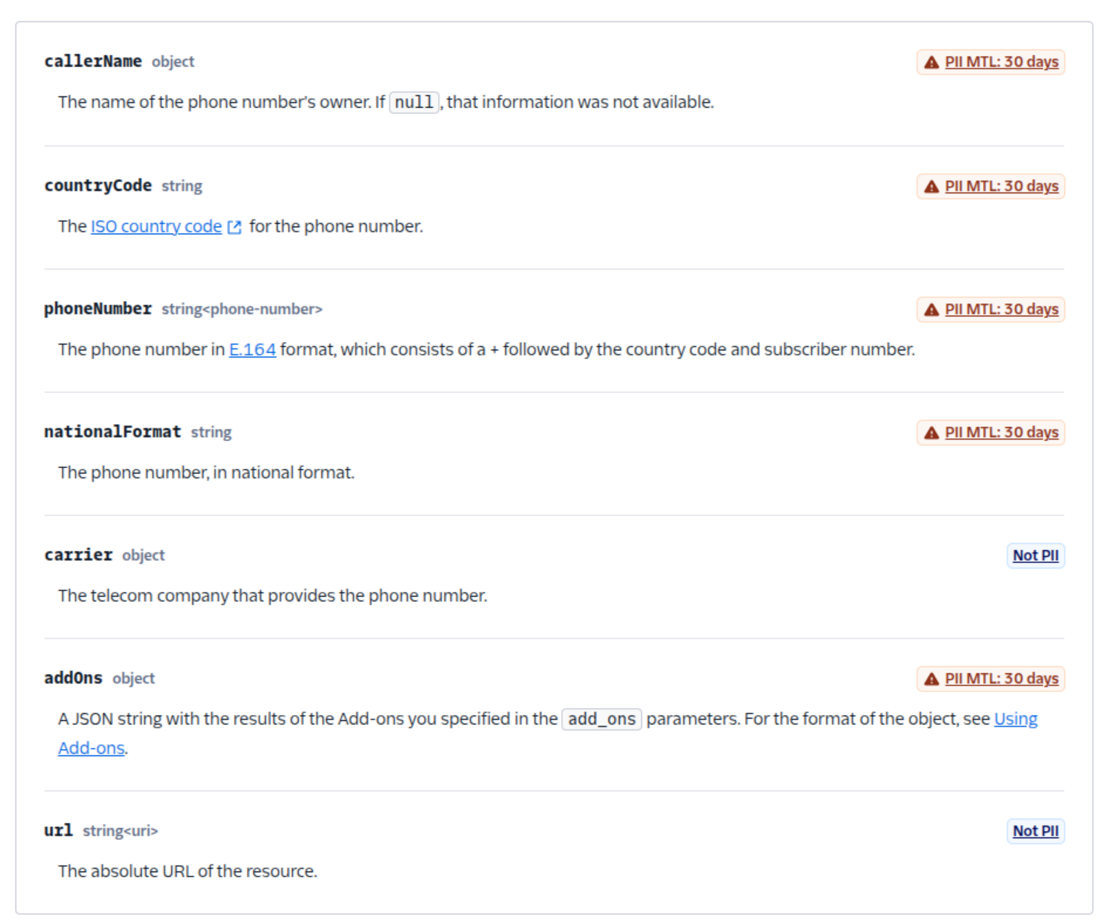
Attack 3.1: IMSI-Disclosure via Core Network



- **SendRoutingInfo-for-SM** (SRI-SM) gives **IMSI** and currently serving **MSC** in exchange for MSISDN.
- Valid Use-Case: foreign SMS-Center needs to know how to route an SMS to the user
  (e.g. two-factor-authentication codes are usually sent from foreign networks)

[Cel],[LTM],[WtW22]

CaseStudy: Online HLR-Lookup Providers



callerName object — ⚠ PII MTL: 30 days

The name of the phone number's owner. If `null`, that information was not available.

countryCode string — ⚠ PII MTL: 30 days

The ISO country code for the phone number.

phoneNumber string<phone-number> ⚠ PII MTL: 30 days

The phone number in E.164 format, which consists of a + followed by the country code and subscriber number.

nationalFormat string — ⚠ PII MTL: 30 days

The phone number, in national format.

carrier object — Not PII

The telecom company that provides the phone number.

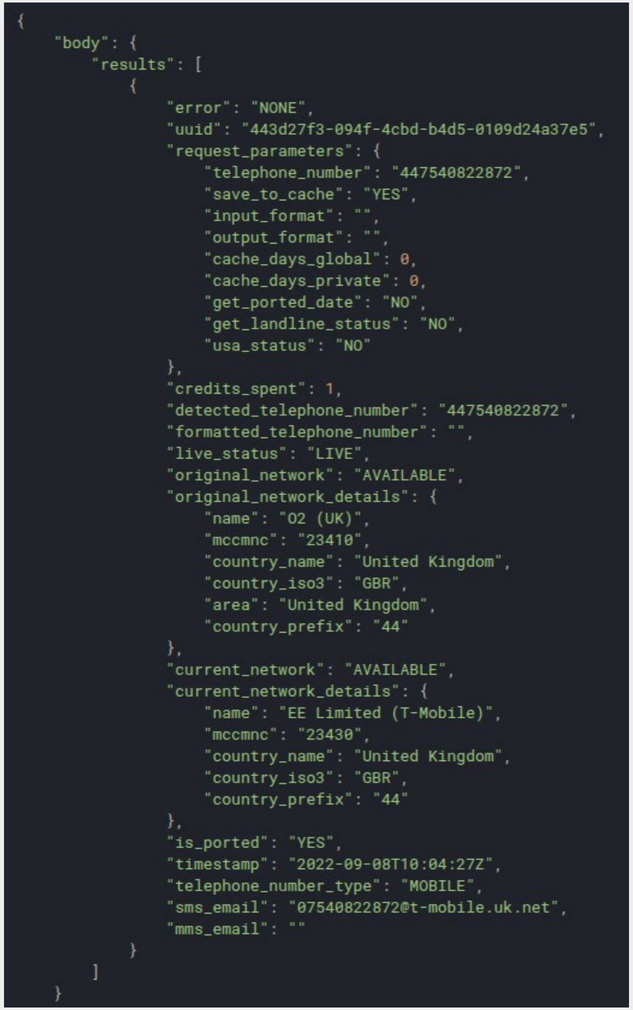
addOns object — ⚠ PII MTL: 30 days

A JSON string with the results of the Add-ons you specified in the `add_ons` parameters. For the format of the object, see Using Add-ons.

url string<uri> Not PII

The absolute URL of the resource.

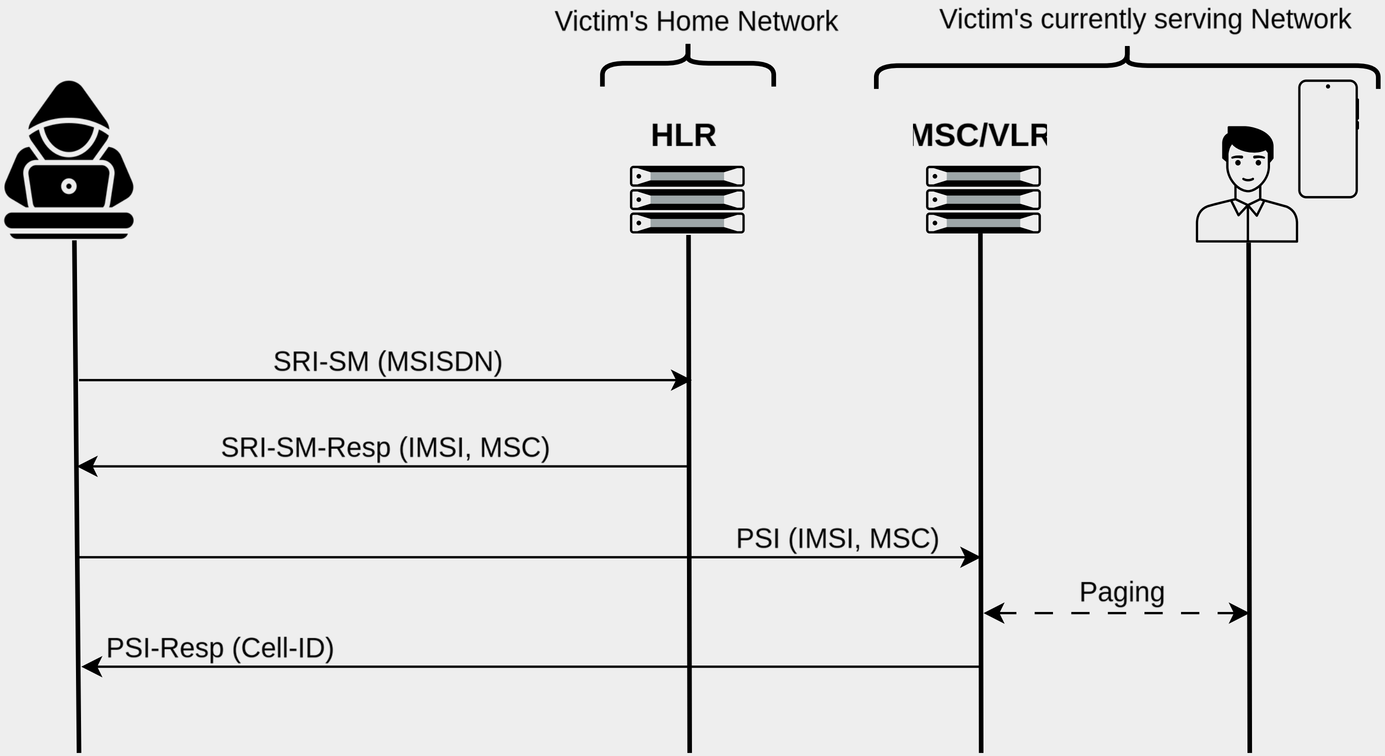
Twilio Lookup API v1 response fields [TwO]



```
{
    "body": {
        "results": [
            {
                "error": "NONE",
                "uuid": "443d27f3-094f-4cbd-b4d5-0109d24a37e5",
                "request_parameters": {
                    "telephone_number": "447540822872",
                    "save_to_cache": "YES",
                    "input_format": "",
                    "output_format": "",
                    "cache_days_global": 0,
                    "cache_days_private": 0,
                    "get_ported_date": "NO",
                    "get_landline_status": "NO",
                    "usa_status": "NO"
                },
                "credits_spent": 1,
                "detected_telephone_number": "447540822872",
                "formatted_telephone_number": "",
                "live_status": "LIVE",
                "original_network": "AVAILABLE",
                "original_network_details": {
                    "name": "O2 (UK)",
                    "mccmnc": "23410",
                    "country_name": "United Kingdom",
                    "country_iso3": "GBR",
                    "area": "United Kingdom",
                    "country_prefix": "44"
                },
                "current_network": "AVAILABLE",
                "current_network_details": {
                    "name": "EE Limited (T-Mobile)",
                    "mccmnc": "23430",
                    "country_name": "United Kingdom",
                    "country_iso3": "GBR",
                    "country_prefix": "44"
                },
                "is_ported": "YES",
                "timestamp": "2022-09-08T10:04:27Z",
                "telephone_number_type": "MOBILE",
                "sms_email": "07540822872@t-mobile.uk.net",
                "mms_email": ""
            }
        ]
    }
```

Hlrlookup.com API response fields [HIR]

Attack 3.2: Location Tracking via Core Network

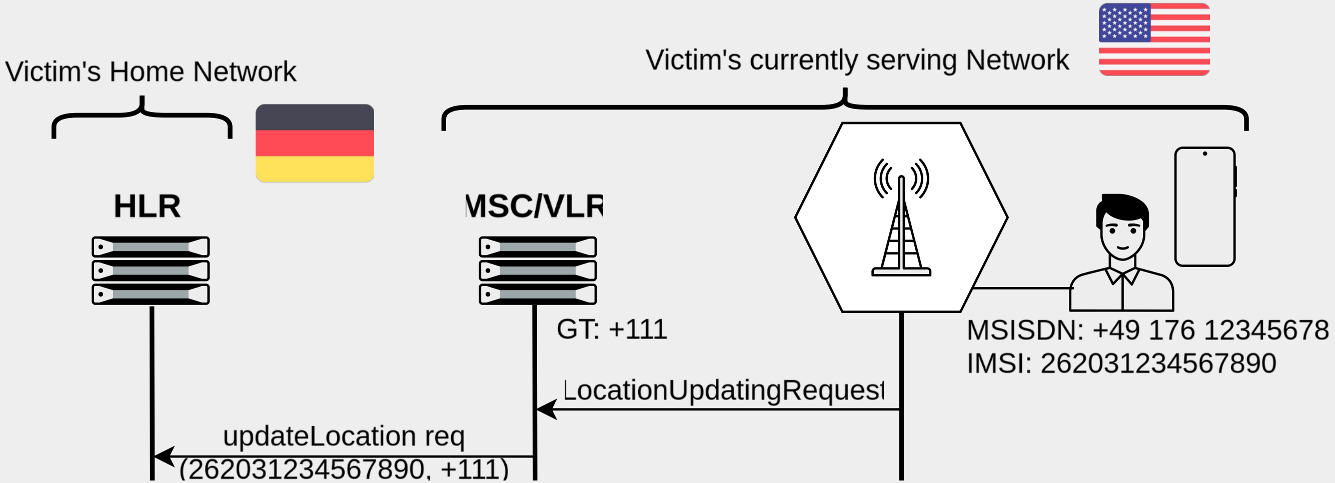


- **ProvideSubscriberInfo** (PSI) gives **Cell-ID** in exchange for IMSI (if sent to the right MSC).
- Valid Use-Case: Lawful location tracking for eCall emergency calls.
- Might result in a PagingRequest to the victims UE if its in IDLE mode.

[Cel],[LTM],[WtW22]

What happens when you're roaming?

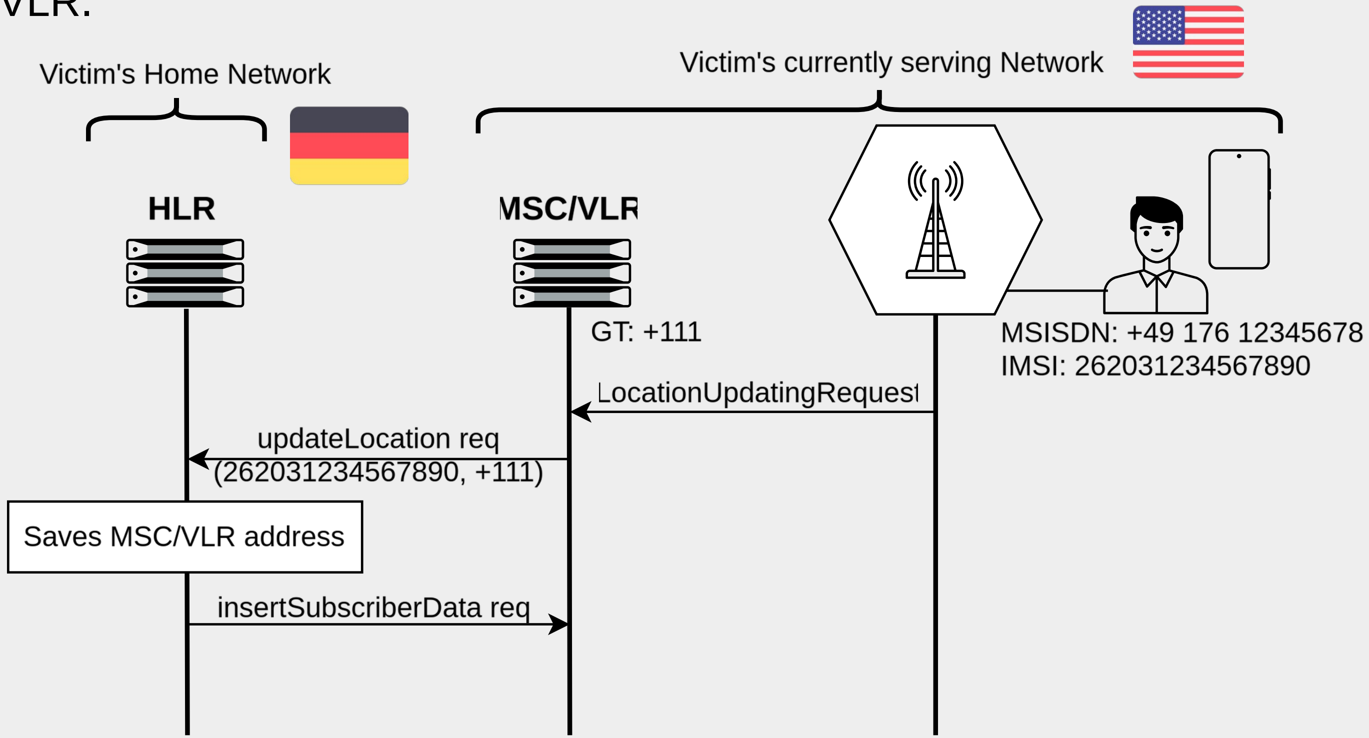
- When a subscriber connects the first time to a foreign network with roaming enabled, the VLR/MSC sends an updateLocation request to the subscribers home network HLR.



[Cel],[LTM]

What happens when you’re roaming?

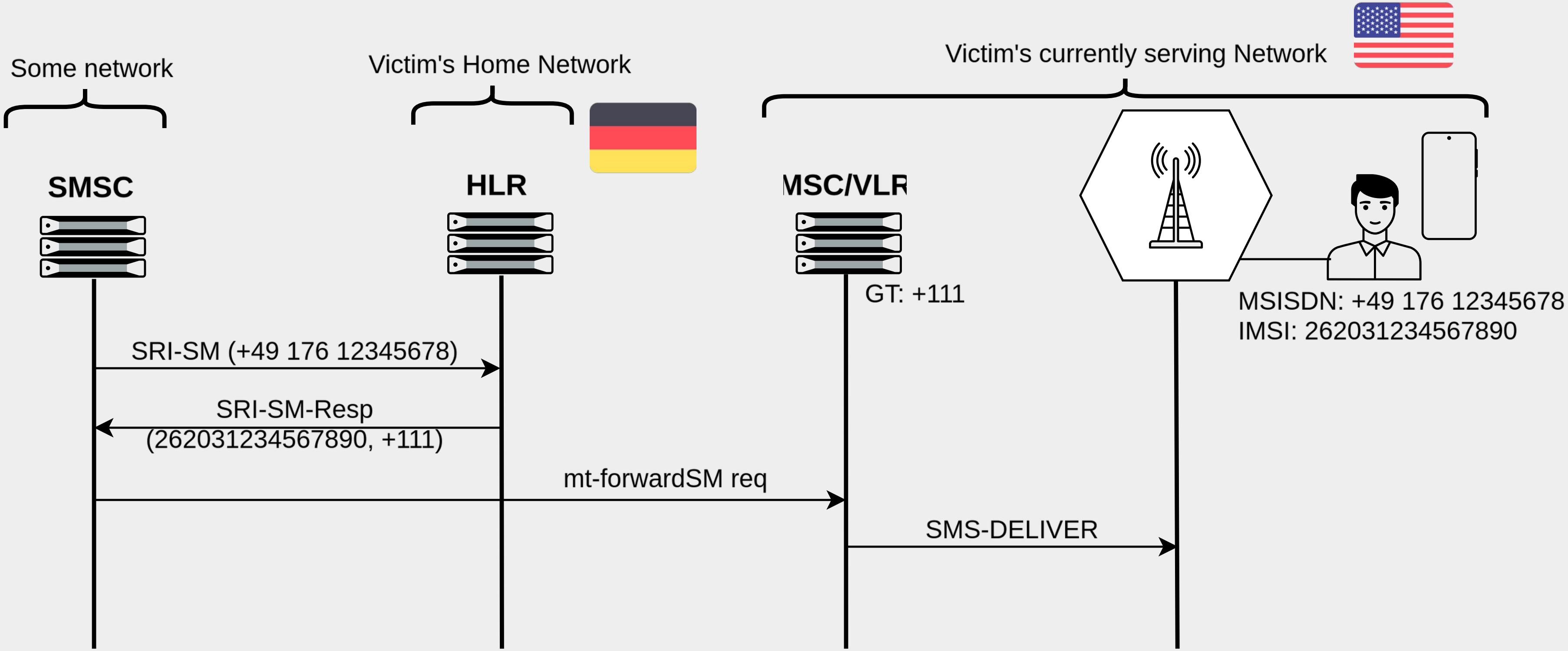
- When a subscriber connects the first time to a foreign network with roaming enabled, the VLR/MSC sends an UpdateLocationRequest to the subscribers home network HLR.
- The HLR sends a copy of the subscribers data to the MSC/VLR and saves the address of the MSC/VLR.



[Cel],[LTM]

What happens when you’re roaming?

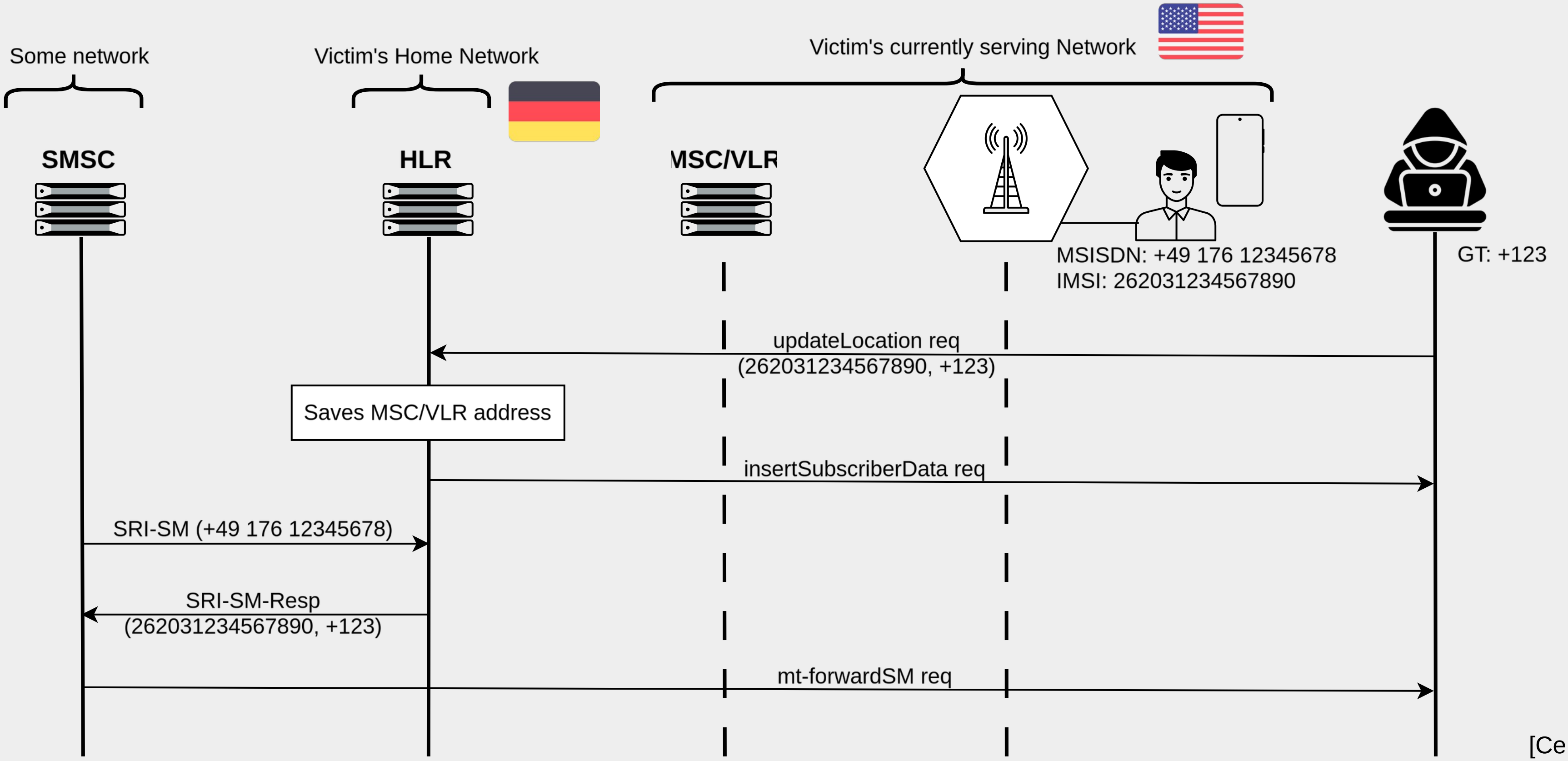
- When somebody wants to call or text the subscriber, the HLR gets asked for routing information (using SRI-SM) and hands out the saved address of the foreign MSC/VLR.



[Cel],[LTM]

Attack 3.3: Call Redirection/SMS Interception via Core Network

- We can send the updateLocation request on our own and specify our GT as the “foreign MSC/VLR”. (updateLocation request is unauthenticated).



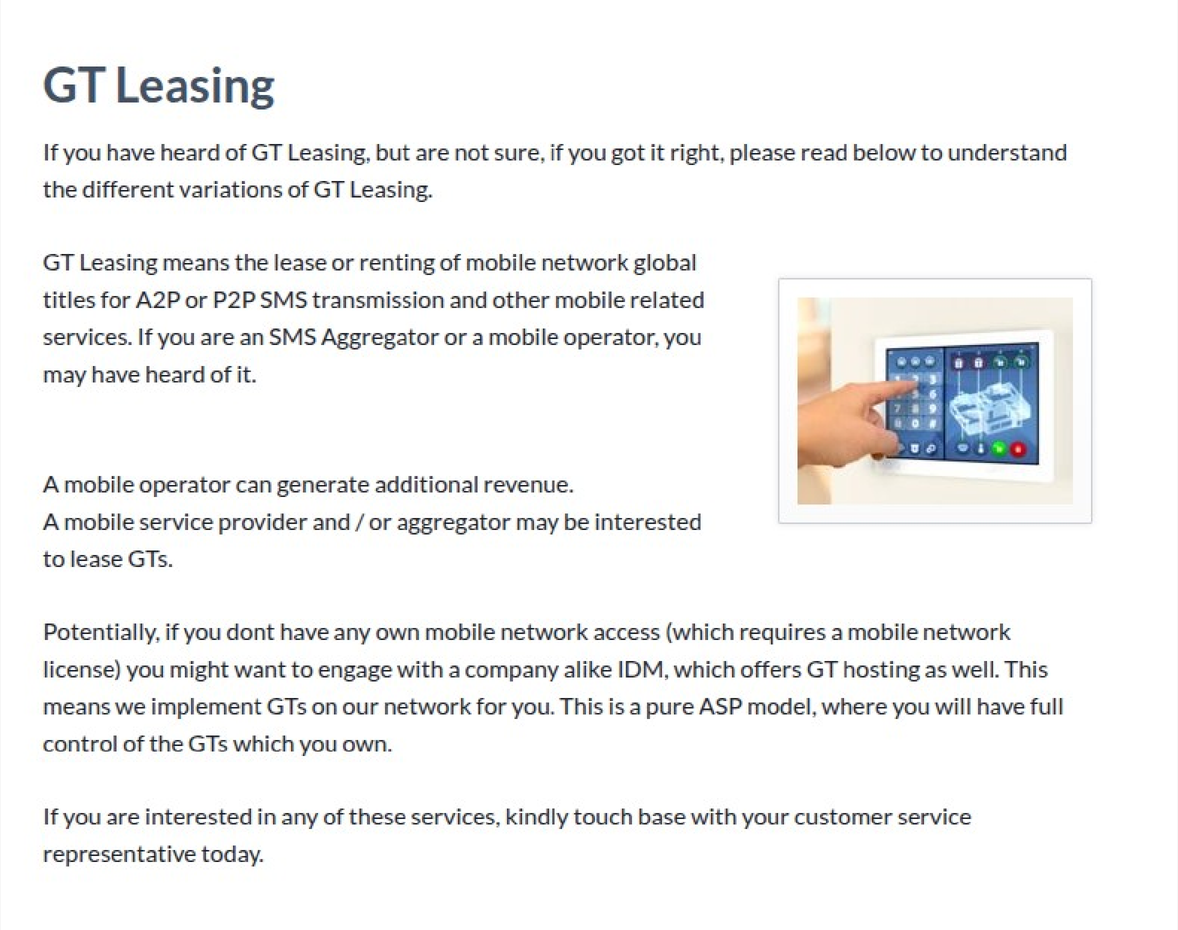
[Cel],[LTM]

How to get access to SS7?

- Lease GTs
- Hack some company with SS7 access
- Exploit Signaling Gateways
- SS7-over-IP (SIGTRAN) exploits
- Darknet
- ...

> “There is probably thousand of ways into SS7 at reasonable effort or cost.”
>
> - Karsten Nohl, SRLabs Berlin [Noh24]

How to get access to SS7?



GT Leasing

If you have heard of GT Leasing, but are not sure, if you got it right, please read below to understand the different variations of GT Leasing.

GT Leasing means the lease or renting of mobile network global titles for A2P or P2P SMS transmission and other mobile related services. If you are an SMS Aggregator or a mobile operator, you may have heard of it.

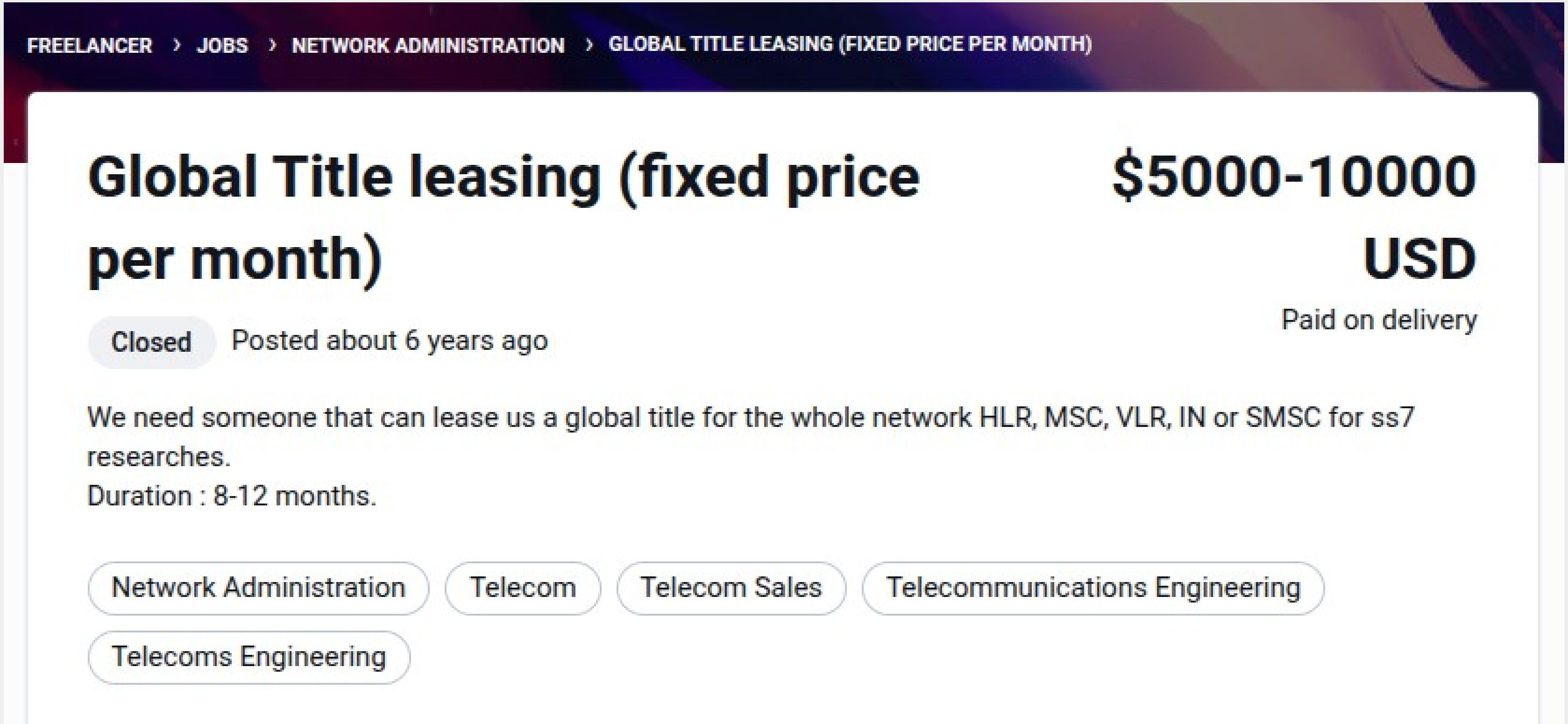
A mobile operator can generate additional revenue.
A mobile service provider and / or aggregator may be interested to lease GTs.

Potentially, if you dont have any own mobile network access (which requires a mobile network license) you might want to engage with a company alike IDM, which offers GT hosting as well. This means we implement GTs on our network for you. This is a pure ASP model, where you will have full control of the GTs which you own.

If you are interested in any of these services, kindly touch base with your customer service representative today.

GT Leasing offer by IDM GmbH [IDM]

How to get access to SS7?



FREELANCER › JOBS › NETWORK ADMINISTRATION › GLOBAL TITLE LEASING (FIXED PRICE PER MONTH)

Global Title leasing (fixed price per month)

$5000-10000 USD

Paid on delivery

Closed Posted about 6 years ago

We need someone that can lease us a global title for the whole network HLR, MSC, VLR, IN or SMSC for ss7 researches.
Duration : 8-12 months.

Network Administration | Telecom | Telecom Sales | Telecommunications Engineering | Telecoms Engineering

Freelancer inquiry looking for a GT leasing offer [FrL]

What about Diameter and 5GC?

Diameter:

- Inherits most of the vulnerabilities of SS7.
- Has TLS/IPSec, but once inside the network you’re trusted.

→ See handout for similar attack messages in Diameter.

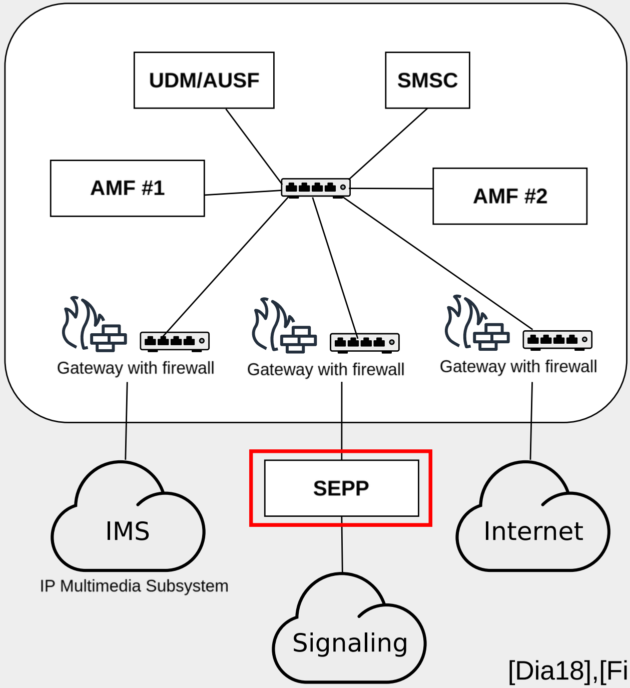
5GC:

- **SEPP** drastically improves security of Signaling abuse by adding encryption, integrity and authentication.

→ Only works if the majority has deployed SEPP.

→ “first-mover-disadvantage”

→ Out of 354 operators that have launched 5G, only 73 have launched a full compliant 5G-SA network (as of April 2025). [GSA]



[Dia18],[Fin23]

SS7 Countermeasures

Firewalls !!!

- Only accept roaming messages from roaming partner networks
- Detect quick change of roaming vs. non-roaming states

→ Secure firewall configuration is key

→ Many operators don't have interest in upgrading firewalls (costs money, impact on customer satisfaction)

How do we know what is malicious?

- Vast majority of "suspicious" traffic is "noise": misconfigured nodes, local-specific configs.
- Only 0.04% of SS7 traffic is irregular/suspicious (2022).
- Only 1.37% of this suspicious traffic is actually malicious (2022).

[WtW22]

Pretend its a legit roaming request
Block suspicious signaling traffic
YOUR SS7 FIREWALL
(if it even exists)

What else is there?

Attack Surface User Equipment:

- SIM-swapping.
- SIM-jacking.

Attack Surface RF + Base Stations:

- Signal overshadowing (SigOver, AdaptOver).
- IMSI brute-forcing (PIERCER Attack).
- Passive Location Tracking via signal arriving delay (LTrack).
- Fine-grained Location Tracking via MeasurementReports (Trilateration with signal strength).
- much more...

Attack Surface Core Network:

- VoIP (really interesting attack surface).
- Caller-ID spoofing using VoIP with PSTN gateways.
- Hidden phone numbers.
- Obtain IMSI from TMSI via special command in SS7.
- Country-based location via ringback-tone fingerprinting.
- much more...

What can you do to protect yourself?

Against User Equipment Attacks:

- Request newer SIM from your provider if yours is really old.
- Throw away your phone!

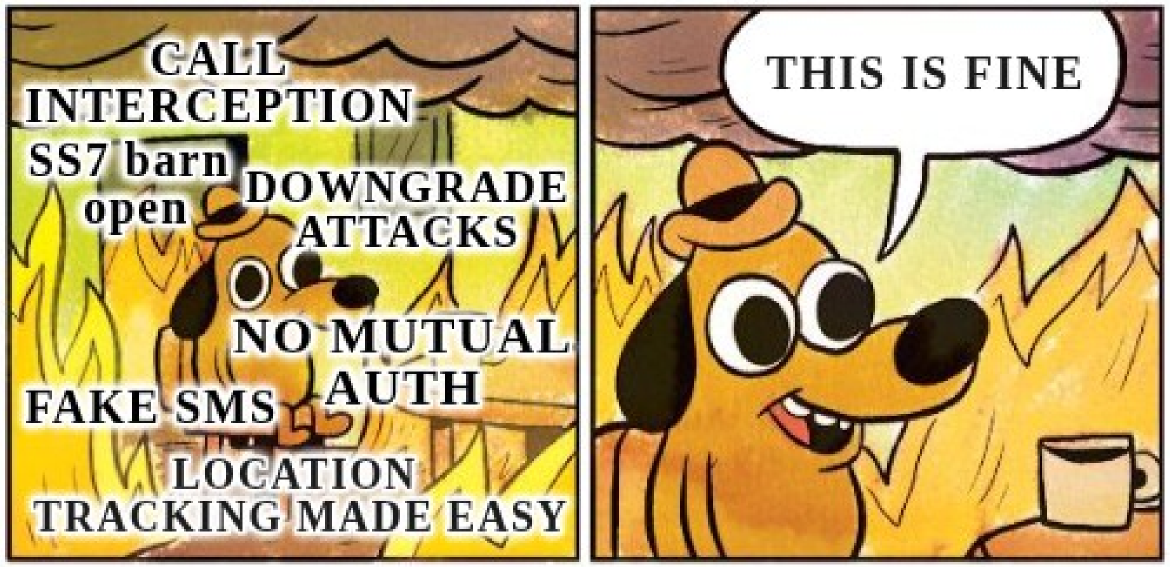
Against RF + Base Stations Attacks:

- If your phone supports it, disable 2G in settings (but again, what is actually happening is decided by baseband processor).
- Be extra cautious and attentive in bad-coverage ares (tunnels,ships,planes,rural areas) and tracking-area borders.
- Throw away your phone!

Against Core Network Attacks:

- Throw away your phone!

→ Pressure operators/regulators to take **more** action. First steps would be to **ban/restrict GT Leasing** and **discontinue 2G** !!!


CALL INTERCEPTION
SS7 barn open
DOWNGRADE ATTACKS
NO MUTUAL AUTH
FAKE SMS
LOCATION TRACKING MADE EASY
THIS IS FINE

Thank You!

Sources

[Sha17]: Practical Attacks Against Privacy and Availability in
4G/LTE Mobile Communication Systems: https://arxiv.org/abs/1510.07563

[Got19]: Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks:
https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf

[Noh10]: Attacking phone privacy:
https://media.blackhat.com/bh-ad-10/Nohl/BlackHat-AD-2010-Nohl-Attacking-Phone-Privacy-wp.pdf

[Dia18]: Diameter Vulnerabilities Exposure Report 2018:
https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf

[SS718]: SS7 Vulnerabilities and Attack Exposure Report 2018:
https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf

[Vee18]: Automated 2G traffic interception and penetration testing:
https://research.tue.nl/files/130177228/Thomas_Veens.pdf

[Jov16] LTE security, protocol exploits and location tracking
experimentation with low-cost software radio: https://arxiv.org/abs/1607.05171

[Fei19]: LTE is Vulnerable: Implementing Identity Spoofing
and Denial-of-Service Attacks in LTE Networks:
https://research.ece.ncsu.edu/netwis2/papers/19FW-GB.pdf

Sources

[Kar21]: Never Let Me Down Again: Bidding-Down Attacks and
Mitigations in 5G and 4G: https://montsecure.com/files/2021_downgrade.pdf
[Fin23] Findin You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure:
https://citizenlab.ca/wp-content/uploads/2023/11/Report171-FindingYou_Nov8.pdf
[LTM] SS7: Locate. Track. Manipulate:
https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
[Cel] Cellusys SS7 Vulnerabilities Report: https://www.cellusys.com/download/ss7-vulnerabilities.pdf

Sources

[Sta1] https://www.deadzones.com/2011/05/how-many-cell-phone-calls-are-made-day.html

[Sta2] https://www.go-beyond.biz/data-statistics/how-many-texts-are-sent-per-day

[Sta3] https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/

[PaS] https://www.hgexperts.com/expert-witness-articles/proactive-sms-and-a-claim-of-distracted-driving-59979

[3GP] https://portal.3gpp.org/Specifications.aspx

[WiK] https://en.wikipedia.org/wiki/Telephone_numbers_in_Germany

[TeA] https://unitedlex.com/insights/apple-iphone-13-pro-max-teardown-report/

[SiS] https://digit.site36.net/2020/02/10/germany-many-silent-sms-at-federal-and-state-level/

[SmQ] https://dserver.bundestag.de/btd/20/108/2010835.pdf

[Dek] https://brmlab.cz/project/gsm/deka/start

[KrK] https://github.com/joswr1ght/kraken

[PaT] https://patentimages.storage.googleapis.com/0f/c4/de/e3cf41422bec4a/US20220338016A1.pdf

[MiC] https://ptcjammer.en.made-in-china.com/product/IQBRCXSKMvcD/China-Imsi-Catcher-IMEI-Catcher-with-SMS-Blaster-in-GSM.html

[PoX] https://www.proximus.com.ua/solutions/ESS-200-SMS-sender.html

[IR21] https://18416860185297090996.googlegroups.com/attach/12732e6205cc22/IR.21_OMNVF_20210709_v14.0%20V.2.0.pdf

Sources

[OfC] https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/185679-consultation-global-titles-and-mobile-network-security/associated-documents/statement-global-titles-and-mobile-network-security.pdf

[TwO] https://www.twilio.com/docs/lookup/v1-api#phone-number-lookup

[HlP] https://www.hlrlookup.com/knowledge/fast-start-sample-curl

[Noh24] https://www.youtube.com/watch?v=wVyu7NB7W6Y

[IDM] https://i-digital-m.com/en/gt_leasing.html

[FrL] https://www.freelancer.com/projects/network-administration/global-title-leasing-fixed-price

[GSA] https://gsacom.com/paper/5g-market-snapshot-april-2025/

[WtW22] https://www.youtube.com/watch?v=q_Xs9v6wV08

Discussion Points:

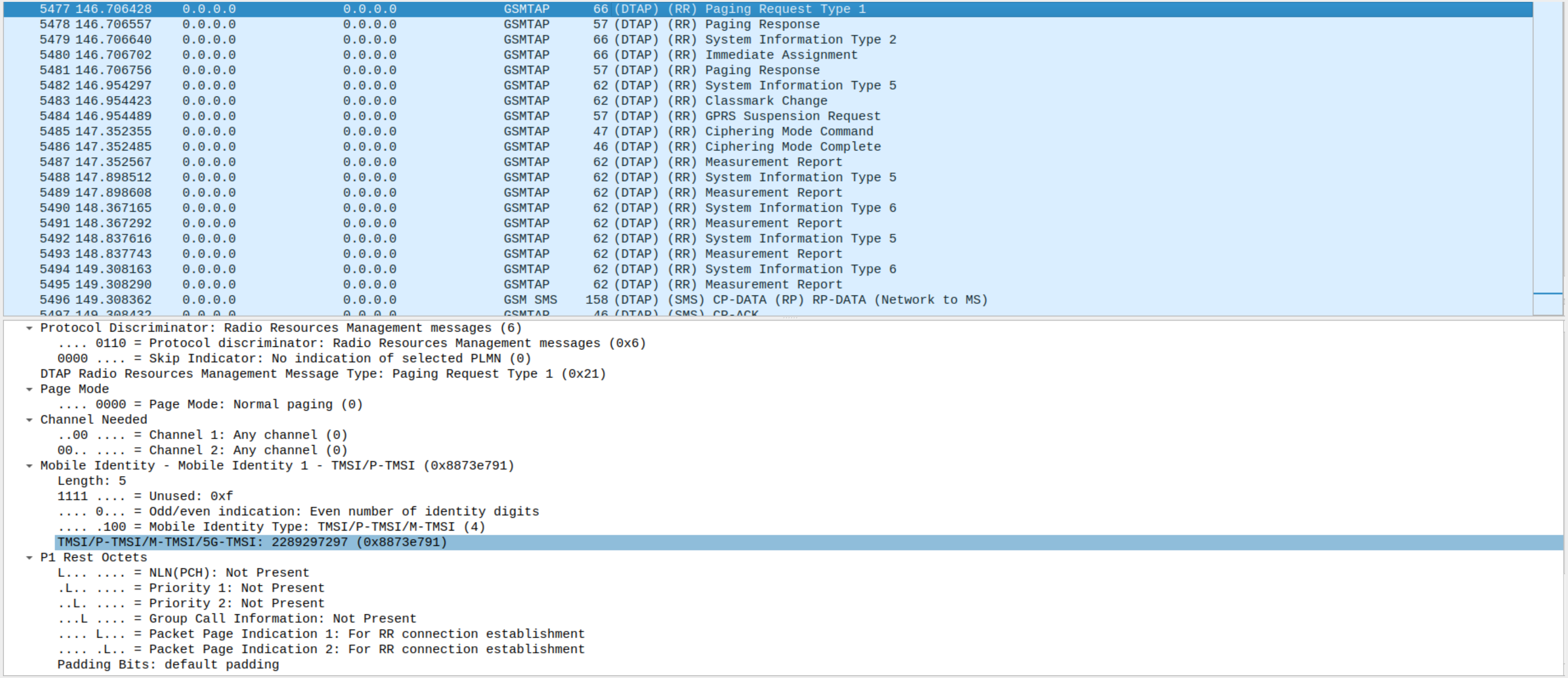
1) Should legacy technologies like 2G finally be shut down — or are they still needed for emergencies and compatibility (e.g. car SOS buttons, cheap IoT, etc.) ?

2) Should mobile operators be allowed to lease signaling access to third parties at all? If so, who is accountable when Global Title leasing is abused — the mobile operators or the lessee?

3) Should law enforcement be allowed to use IMSI catchers — or do the privacy risks outweigh their benefits?

Extra Slides

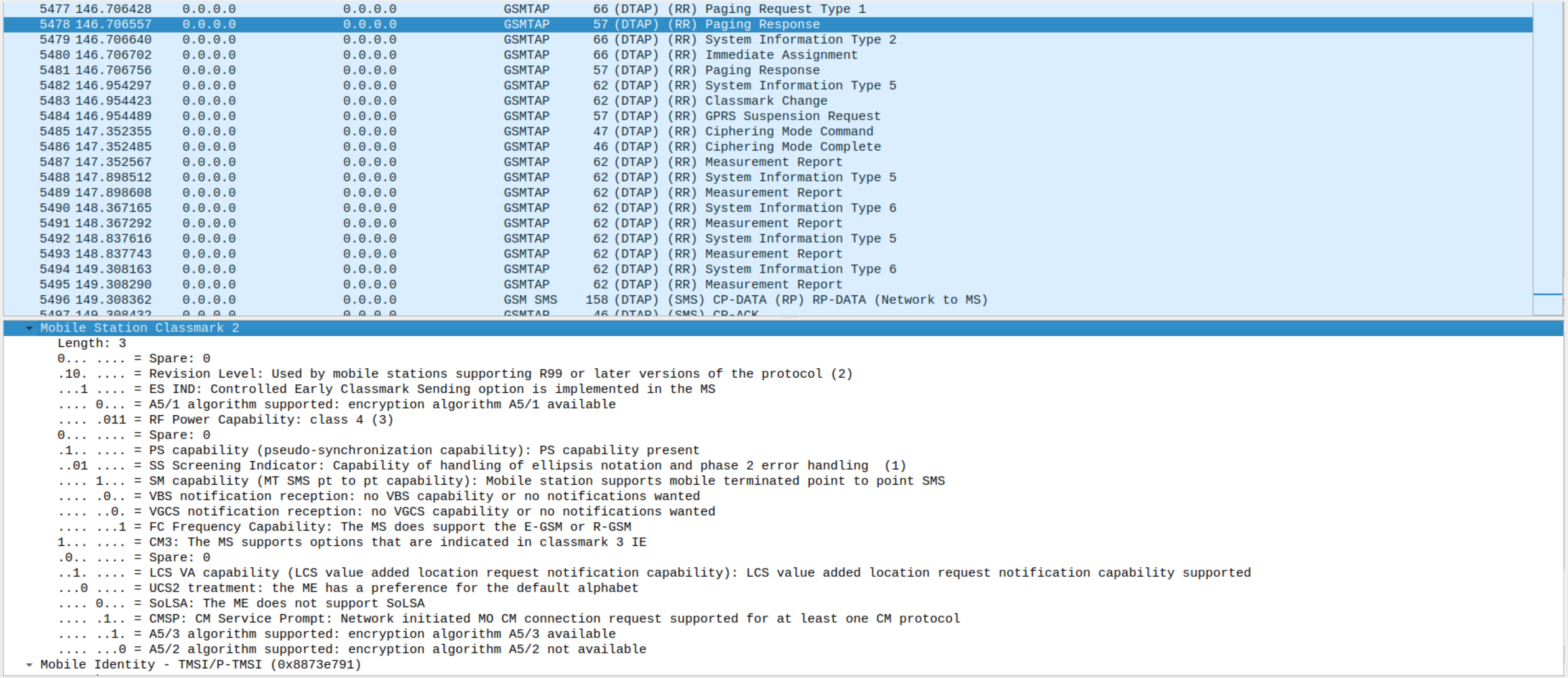
Attack 2.1: Decrypt SMS / Phone Calls



```
5477 146.706428  0.0.0.0  0.0.0.0  GSMTAP   66 (DTAP) (RR) Paging Request Type 1
5478 146.706557  0.0.0.0  0.0.0.0  GSMTAP   57 (DTAP) (RR) Paging Response
5479 146.706640  0.0.0.0  0.0.0.0  GSMTAP   66 (DTAP) (RR) System Information Type 2
5480 146.706702  0.0.0.0  0.0.0.0  GSMTAP   66 (DTAP) (RR) Immediate Assignment
5481 146.706756  0.0.0.0  0.0.0.0  GSMTAP   57 (DTAP) (RR) Paging Response
5482 146.954297  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) System Information Type 5
5483 146.954423  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Classmark Change
5484 146.954489  0.0.0.0  0.0.0.0  GSMTAP   57 (DTAP) (RR) GPRS Suspension Request
5485 147.352355  0.0.0.0  0.0.0.0  GSMTAP   47 (DTAP) (RR) Ciphering Mode Command
5486 147.352485  0.0.0.0  0.0.0.0  GSMTAP   46 (DTAP) (RR) Ciphering Mode Complete
5487 147.352567  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Measurement Report
5488 147.898512  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) System Information Type 5
5489 147.898608  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Measurement Report
5490 148.367165  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) System Information Type 6
5491 148.367292  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Measurement Report
5492 148.837616  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) System Information Type 5
5493 148.837743  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Measurement Report
5494 149.308163  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) System Information Type 6
5495 149.308290  0.0.0.0  0.0.0.0  GSMTAP   62 (DTAP) (RR) Measurement Report
5496 149.308362  0.0.0.0  0.0.0.0  GSM SMS 158 (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
5497 149.308432  0.0.0.0  0.0.0.0  GSMTAP   46 (DTAP) (SMS) CP-ACK
```

```
▾ Protocol Discriminator: Radio Resources Management messages (6)
    .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
    0000 .... = Skip Indicator: No indication of selected PLMN (0)
  DTAP Radio Resources Management Message Type: Paging Request Type 1 (0x21)
▾ Page Mode
    .... 0000 = Page Mode: Normal paging (0)
▾ Channel Needed
    ..00 .... = Channel 1: Any channel (0)
    00.. .... = Channel 2: Any channel (0)
▾ Mobile Identity - Mobile Identity 1 - TMSI/P-TMSI (0x8873e791)
    Length: 5
    1111 .... = Unused: 0xf
    .... 0... = Odd/even indication: Even number of identity digits
    .... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
    TMSI/P-TMSI/M-TMSI/5G-TMSI: 2289297297 (0x8873e791)
▾ P1 Rest Octets
    L... .... = NLN(PCH): Not Present
    .L.. .... = Priority 1: Not Present
    ..L. .... = Priority 2: Not Present
    ...L .... = Group Call Information: Not Present
    .... L... = Packet Page Indication 1: For RR connection establishment
    .... .L.. = Packet Page Indication 2: For RR connection establishment
    Padding Bits: default padding
```

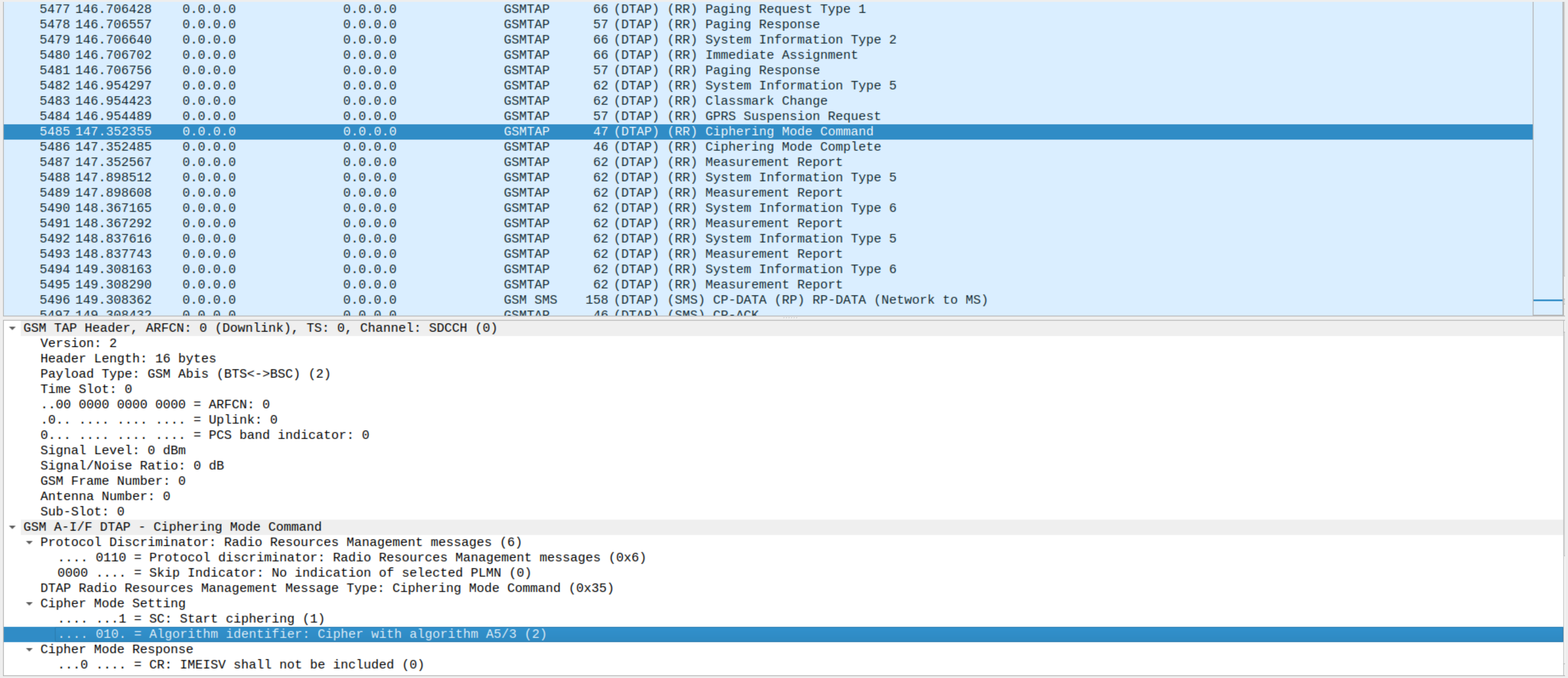
Attack 2.1: Decrypt SMS / Phone Calls



```
5477 146.706428   0.0.0.0        0.0.0.0        GSMTAP      66 (DTAP) (RR) Paging Request Type 1
5478 146.706557   0.0.0.0        0.0.0.0        GSMTAP      57 (DTAP) (RR) Paging Response
5479 146.706640   0.0.0.0        0.0.0.0        GSMTAP      66 (DTAP) (RR) System Information Type 2
5480 146.706702   0.0.0.0        0.0.0.0        GSMTAP      66 (DTAP) (RR) Immediate Assignment
5481 146.706756   0.0.0.0        0.0.0.0        GSMTAP      57 (DTAP) (RR) Paging Response
5482 146.954297   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) System Information Type 5
5483 146.954423   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Classmark Change
5484 146.954489   0.0.0.0        0.0.0.0        GSMTAP      57 (DTAP) (RR) GPRS Suspension Request
5485 147.352355   0.0.0.0        0.0.0.0        GSMTAP      47 (DTAP) (RR) Ciphering Mode Command
5486 147.352485   0.0.0.0        0.0.0.0        GSMTAP      46 (DTAP) (RR) Ciphering Mode Complete
5487 147.352567   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Measurement Report
5488 147.898512   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) System Information Type 5
5489 147.898608   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Measurement Report
5490 148.367165   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) System Information Type 6
5491 148.367292   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Measurement Report
5492 148.837616   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) System Information Type 5
5493 148.837743   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Measurement Report
5494 149.308163   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) System Information Type 6
5495 149.308290   0.0.0.0        0.0.0.0        GSMTAP      62 (DTAP) (RR) Measurement Report
5496 149.308362   0.0.0.0        0.0.0.0        GSM SMS    158 (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
5497 149.308432   0.0.0.0        0.0.0.0        GSMTAP      46 (DTAP) (SMS) CP-ACK
```

```
▾ Mobile Station Classmark 2
    Length: 3
    0... .... = Spare: 0
    .10. .... = Revision Level: Used by mobile stations supporting R99 or later versions of the protocol (2)
    ...1 .... = ES IND: Controlled Early Classmark Sending option is implemented in the MS
    .... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
    .... .011 = RF Power Capability: class 4 (3)
    0... .... = Spare: 0
    .1.. .... = PS capability (pseudo-synchronization capability): PS capability present
    ..01 .... = SS Screening Indicator: Capability of handling of ellipsis notation and phase 2 error handling  (1)
    .... 1... = SM capability (MT SMS pt to pt capability): Mobile station supports mobile terminated point to point SMS
    .... .0.. = VBS notification reception: no VBS capability or no notifications wanted
    .... ..0. = VGCS notification reception: no VGCS capability or no notifications wanted
    .... ...1 = FC Frequency Capability: The MS does support the E-GSM or R-GSM
    1... .... = CM3: The MS supports options that are indicated in classmark 3 IE
    .0.. .... = Spare: 0
    ..1. .... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability supported
    ...0 .... = UCS2 treatment: the ME has a preference for the default alphabet
    .... 0... = SoLSA: The ME does not support SoLSA
    .... .1.. = CMSP: CM Service Prompt: Network initiated MO CM connection request supported for at least one CM protocol
    .... ..1. = A5/3 algorithm supported: encryption algorithm A5/3 available
    .... ...0 = A5/2 algorithm supported: encryption algorithm A5/2 not available
▾ Mobile Identity - TMSI/P-TMSI (0x8873e791)
```

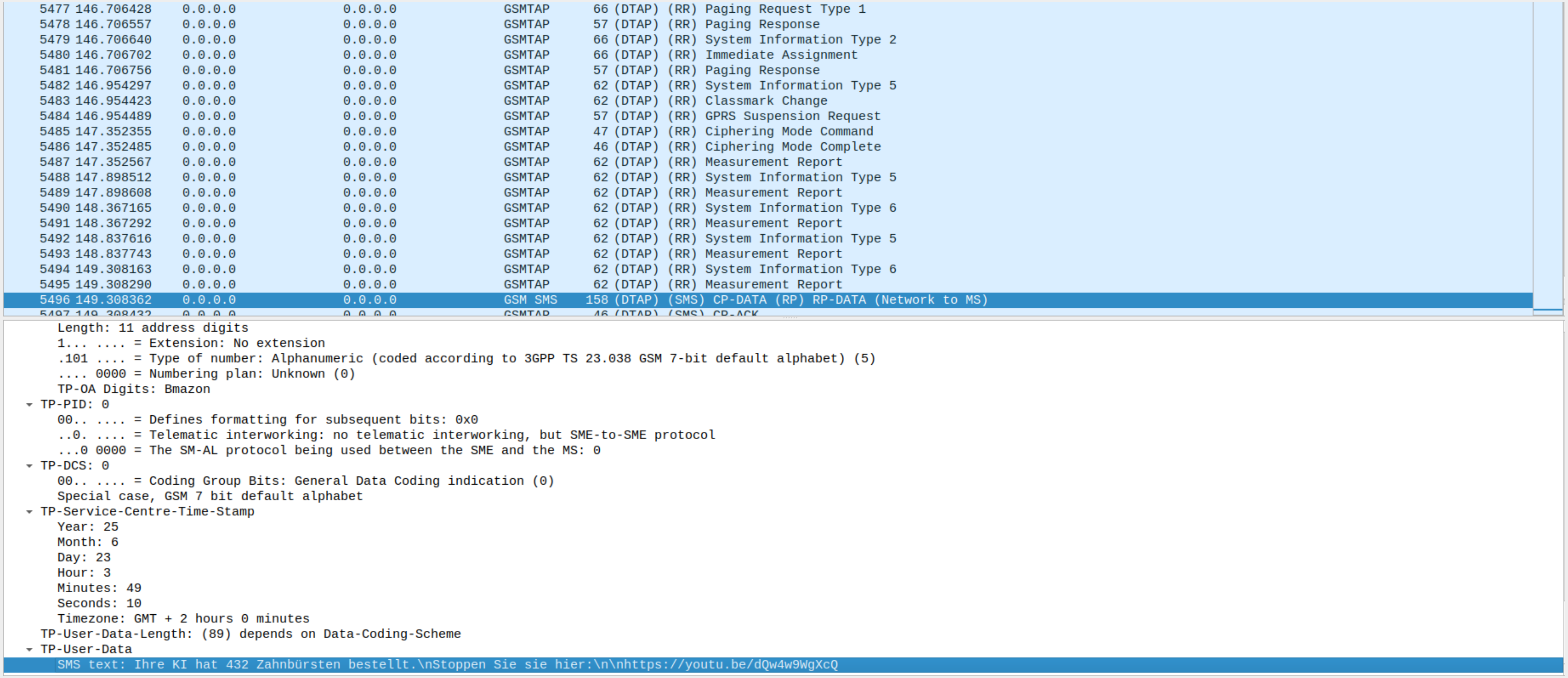
Attack 2.1: Decrypt SMS / Phone Calls



```
5477 146.706428    0.0.0.0             0.0.0.0             GSMTAP      66 (DTAP) (RR) Paging Request Type 1
5478 146.706557    0.0.0.0             0.0.0.0             GSMTAP      57 (DTAP) (RR) Paging Response
5479 146.706640    0.0.0.0             0.0.0.0             GSMTAP      66 (DTAP) (RR) System Information Type 2
5480 146.706702    0.0.0.0             0.0.0.0             GSMTAP      66 (DTAP) (RR) Immediate Assignment
5481 146.706756    0.0.0.0             0.0.0.0             GSMTAP      57 (DTAP) (RR) Paging Response
5482 146.954297    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) System Information Type 5
5483 146.954423    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Classmark Change
5484 146.954489    0.0.0.0             0.0.0.0             GSMTAP      57 (DTAP) (RR) GPRS Suspension Request
5485 147.352355    0.0.0.0             0.0.0.0             GSMTAP      47 (DTAP) (RR) Ciphering Mode Command
5486 147.352485    0.0.0.0             0.0.0.0             GSMTAP      46 (DTAP) (RR) Ciphering Mode Complete
5487 147.352567    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Measurement Report
5488 147.898512    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) System Information Type 5
5489 147.898608    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Measurement Report
5490 148.367165    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) System Information Type 6
5491 148.367292    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Measurement Report
5492 148.837616    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) System Information Type 5
5493 148.837743    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Measurement Report
5494 149.308163    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) System Information Type 6
5495 149.308290    0.0.0.0             0.0.0.0             GSMTAP      62 (DTAP) (RR) Measurement Report
5496 149.308362    0.0.0.0             0.0.0.0             GSM SMS    158 (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
5497 149.308432    0.0.0.0             0.0.0.0             GSMTAP      46 (DTAP) (SMS) CP-ACK
```

```
▾ GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: SDCCH (0)
    Version: 2
    Header Length: 16 bytes
    Payload Type: GSM Abis (BTS<->BSC) (2)
    Time Slot: 0
    ..00 0000 0000 0000 = ARFCN: 0
    .0.. .... .... .... = Uplink: 0
    0... .... .... .... = PCS band indicator: 0
    Signal Level: 0 dBm
    Signal/Noise Ratio: 0 dB
    GSM Frame Number: 0
    Antenna Number: 0
    Sub-Slot: 0
▾ GSM A-I/F DTAP - Ciphering Mode Command
  ▾ Protocol Discriminator: Radio Resources Management messages (6)
      .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  ▾ Cipher Mode Setting
      .... ...1 = SC: Start ciphering (1)
      .... 010. = Algorithm identifier: Cipher with algorithm A5/3 (2)
  ▾ Cipher Mode Response
      ...0 .... = CR: IMEISV shall not be included (0)
```

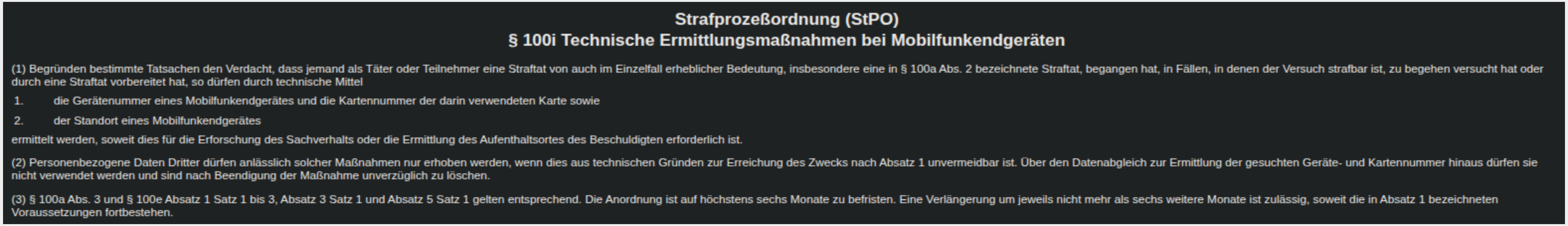
Attack 2.1: Decrypt SMS / Phone Calls



```
5477 146.706428   0.0.0.0          0.0.0.0          GSMTAP     66 (DTAP) (RR) Paging Request Type 1
5478 146.706557   0.0.0.0          0.0.0.0          GSMTAP     57 (DTAP) (RR) Paging Response
5479 146.706640   0.0.0.0          0.0.0.0          GSMTAP     66 (DTAP) (RR) System Information Type 2
5480 146.706702   0.0.0.0          0.0.0.0          GSMTAP     66 (DTAP) (RR) Immediate Assignment
5481 146.706756   0.0.0.0          0.0.0.0          GSMTAP     57 (DTAP) (RR) Paging Response
5482 146.954297   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) System Information Type 5
5483 146.954423   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Classmark Change
5484 146.954489   0.0.0.0          0.0.0.0          GSMTAP     57 (DTAP) (RR) GPRS Suspension Request
5485 147.352355   0.0.0.0          0.0.0.0          GSMTAP     47 (DTAP) (RR) Ciphering Mode Command
5486 147.352485   0.0.0.0          0.0.0.0          GSMTAP     46 (DTAP) (RR) Ciphering Mode Complete
5487 147.352567   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Measurement Report
5488 147.898512   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) System Information Type 5
5489 147.898608   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Measurement Report
5490 148.367165   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) System Information Type 6
5491 148.367292   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Measurement Report
5492 148.837616   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) System Information Type 5
5493 148.837743   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Measurement Report
5494 149.308163   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) System Information Type 6
5495 149.308290   0.0.0.0          0.0.0.0          GSMTAP     62 (DTAP) (RR) Measurement Report
5496 149.308362   0.0.0.0          0.0.0.0          GSM SMS   158 (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
5497 149.308432   0.0.0.0          0.0.0.0          GSMTAP     46 (DTAP) (SMS) CP-ACK
```

```
    Length: 11 address digits
    1... .... = Extension: No extension
    .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
    .... 0000 = Numbering plan: Unknown (0)
    TP-OA Digits: Bmazon
  ▾ TP-PID: 0
    00.. .... = Defines formatting for subsequent bits: 0x0
    ..0. .... = Telematic interworking: no telematic interworking, but SME-to-SME protocol
    ...0 0000 = The SM-AL protocol being used between the SME and the MS: 0
  ▾ TP-DCS: 0
    00.. .... = Coding Group Bits: General Data Coding indication (0)
    Special case, GSM 7 bit default alphabet
  ▾ TP-Service-Centre-Time-Stamp
    Year: 25
    Month: 6
    Day: 23
    Hour: 3
    Minutes: 49
    Seconds: 10
    Timezone: GMT + 2 hours 0 minutes
  TP-User-Data-Length: (89) depends on Data-Coding-Scheme
  ▾ TP-User-Data
    SMS text: Ihre KI hat 432 Zahnbürsten bestellt.\nStoppen Sie sie hier:\n\nhttps://youtu.be/dQw4w9WgXcQ
```

A word on laws



Strafprozeßordnung (StPO)
§ 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, so dürfen durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karte sowie
2. der Standort eines Mobilfunkendgerätes

ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 100a Abs. 3 und § 100e Absatz 1 Satz 1 bis 3, Absatz 3 Satz 1 und Absatz 5 Satz 1 gelten entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.