How to hijack VoLTE network

Pavel Novikov
Pavel.Novikov@security-gen.com

SecurityGen
Telecom Security. Transcending Generations.

Bio

-10 years in telecom security,
-co-author of GSMA FS.20 GPRS Tunneling Protocol (GTP) Security document
-Head of telecom security research in SecurityGen
-Focused on telecom vulnerabilities: RAN, VoLTE, VoWiFi, GTP, Diameter, 5G SA and NSA.
-Conducting telecom security assessments for mobile operators for many years.

Pavel Novikov
Pavel.Novikov@security-gen.com

SecurityGen
Telecom Security. Transcending Generations.

Research Team

-Pavel Novikov (SecurityGen)
-Alex Onegov (ex-SecurityGen)
-Sergey Mashukov (SecurityGen)

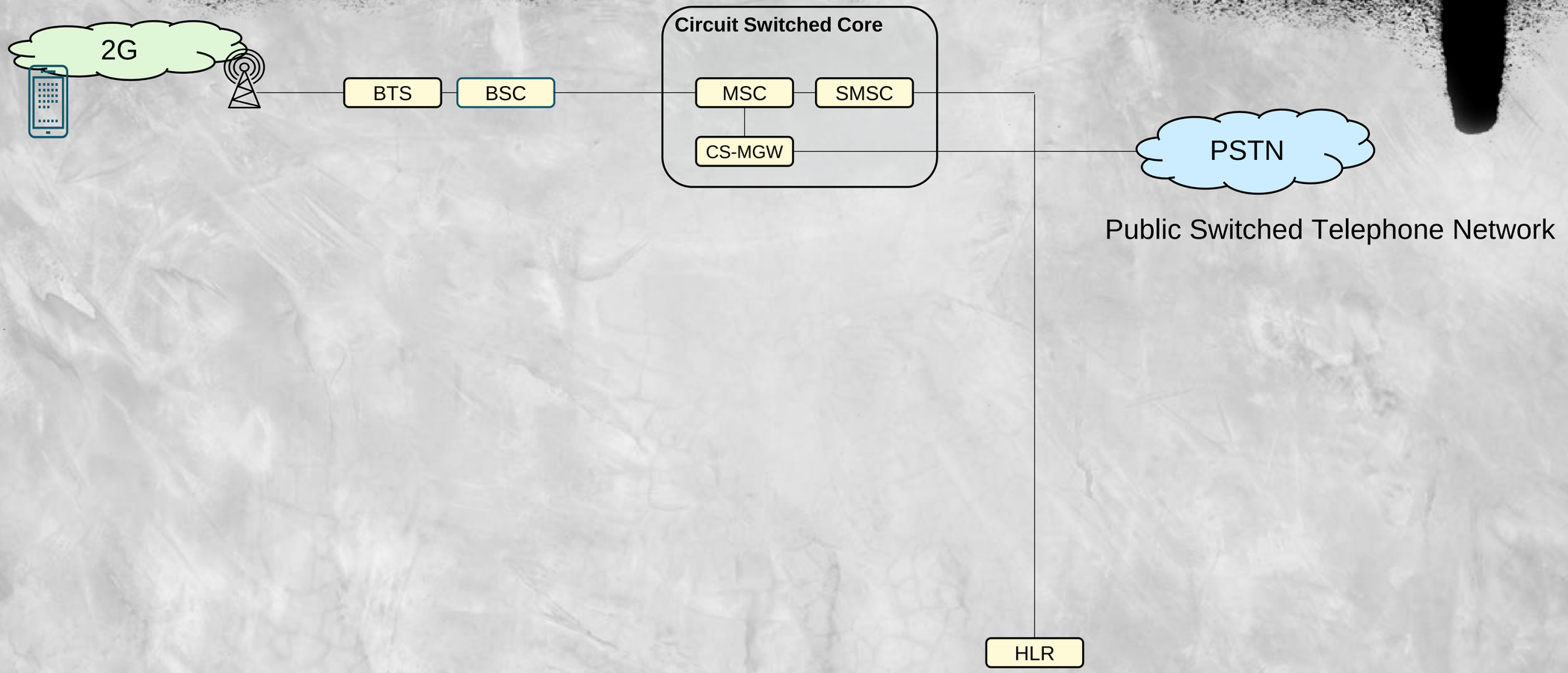
Relevance of the topic

Why now?

SecurityGen
Telecom Security. Transcending Generations.

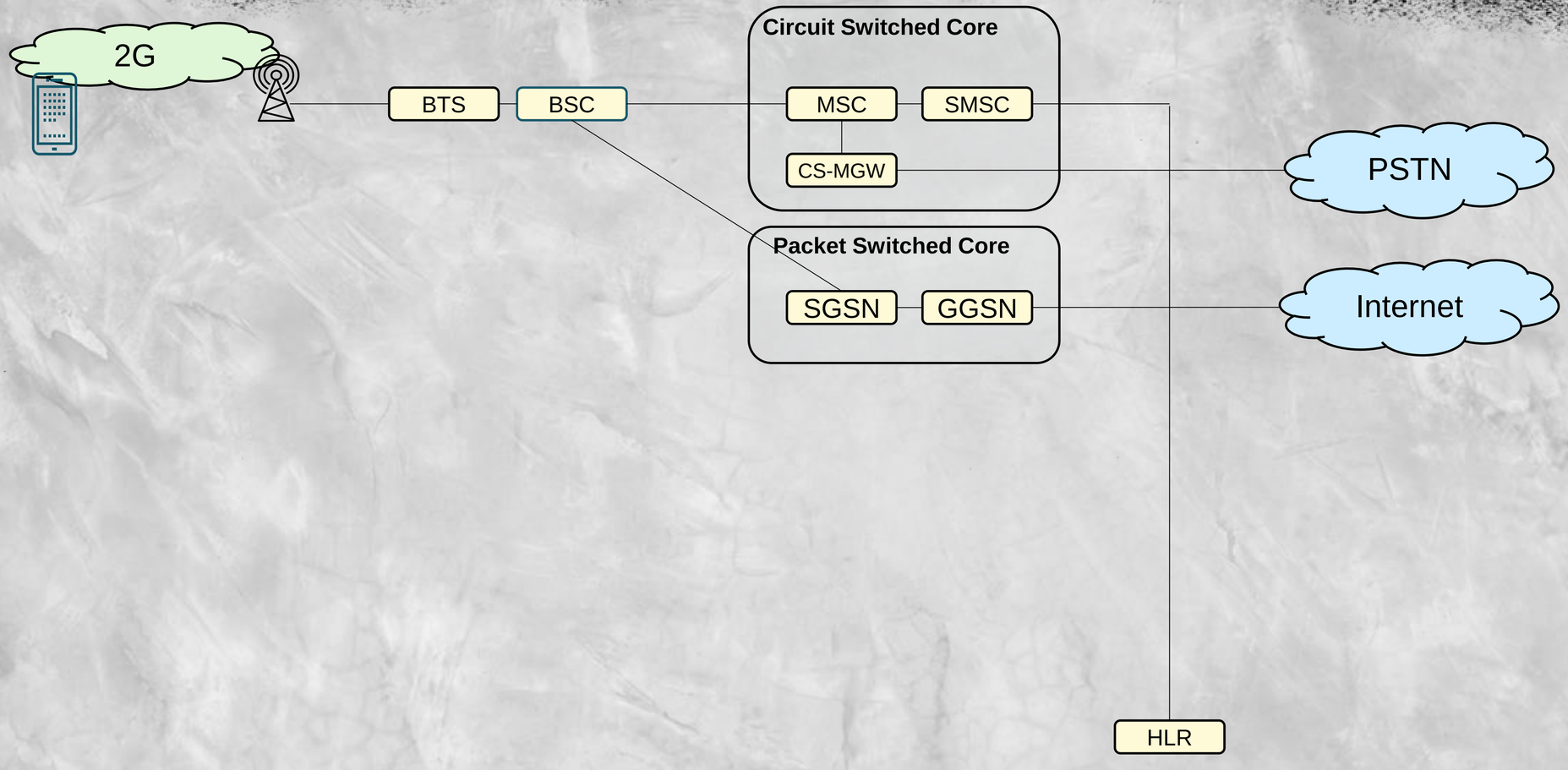
Short course of mobile network evolution

2G voice-only

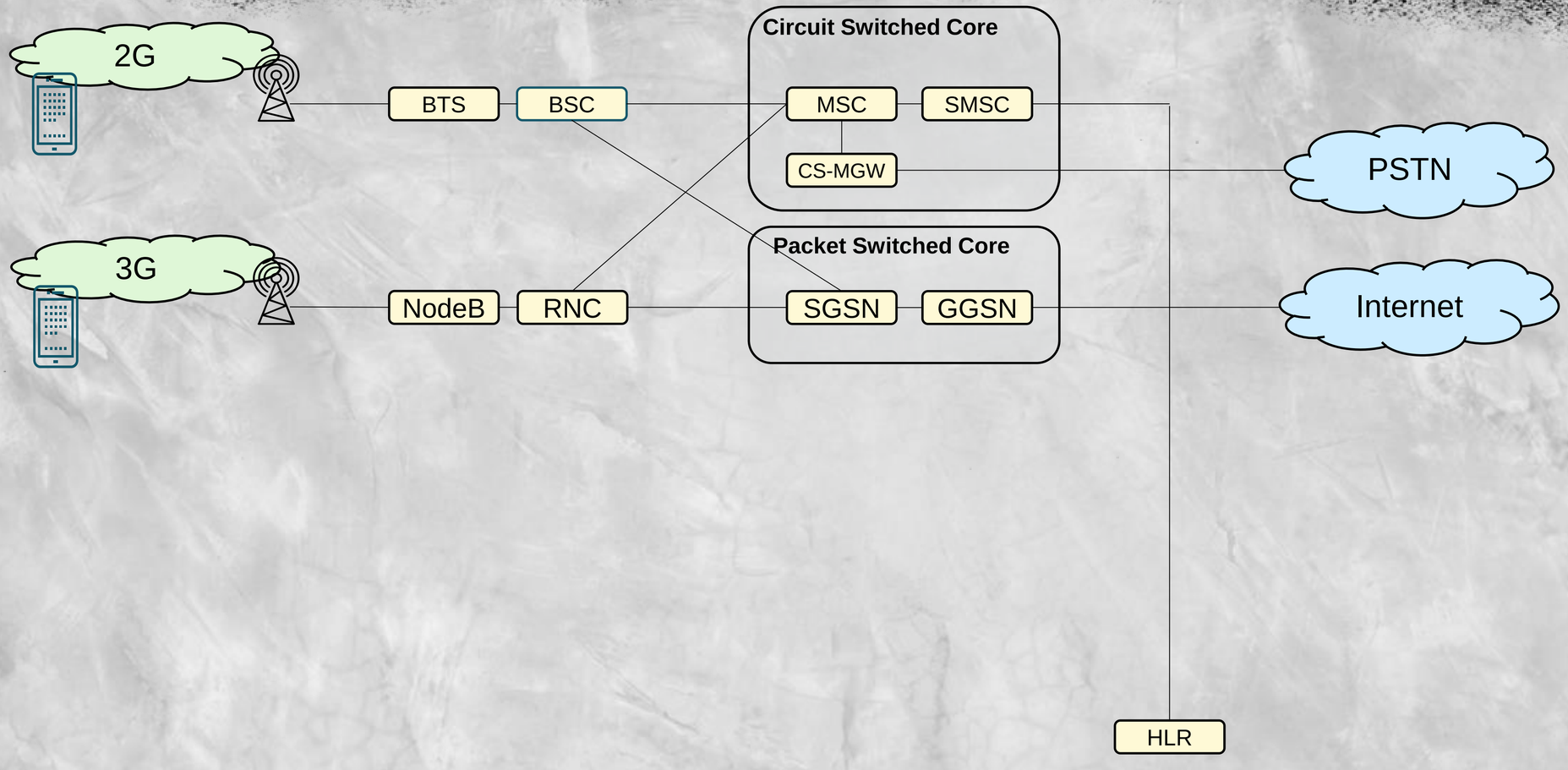


SecurityGen
Telecom Security. Transcending Generations.

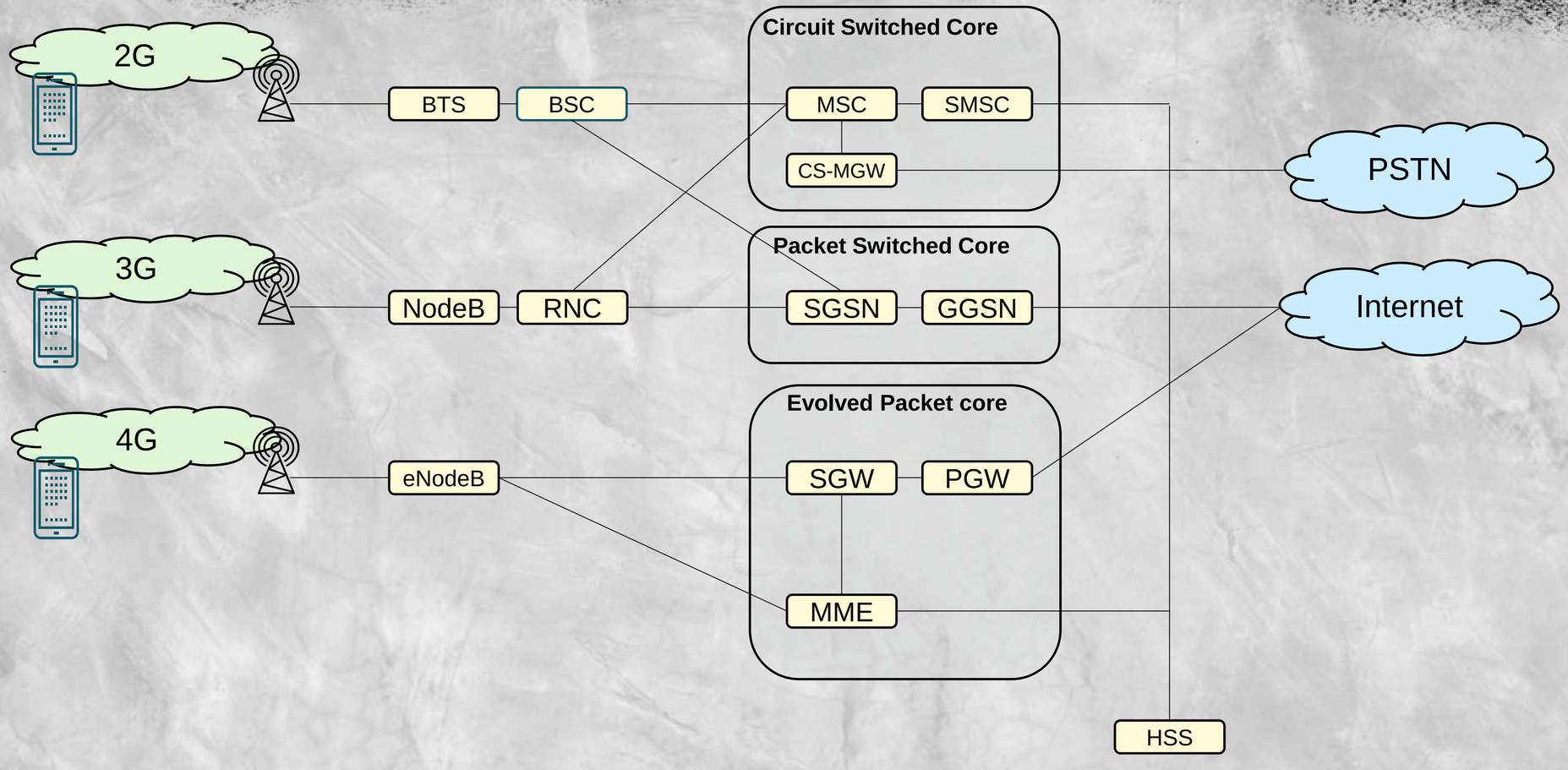
2G +Data


2G
BTS
BSC
Circuit Switched Core
MSC
SMSC
CS-MGW
Packet Switched Core
SGSN
GGSN
PSTN
Internet
HLR

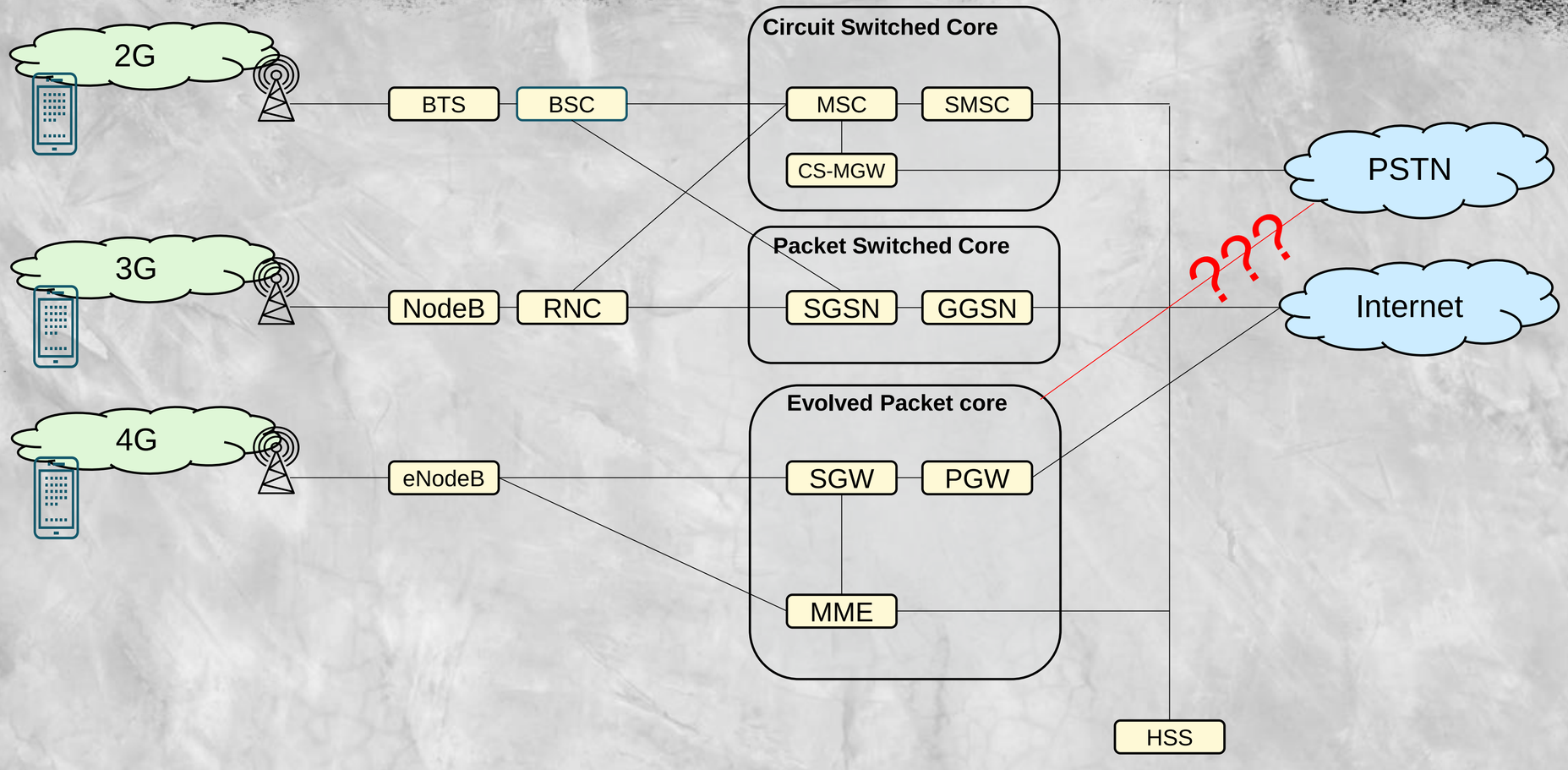
+3G network


2G
3G
BTS
BSC
NodeB
RNC
Circuit Switched Core
MSC
SMSC
CS-MGW
Packet Switched Core
SGSN
GGSN
PSTN
Internet
HLR

+4G data

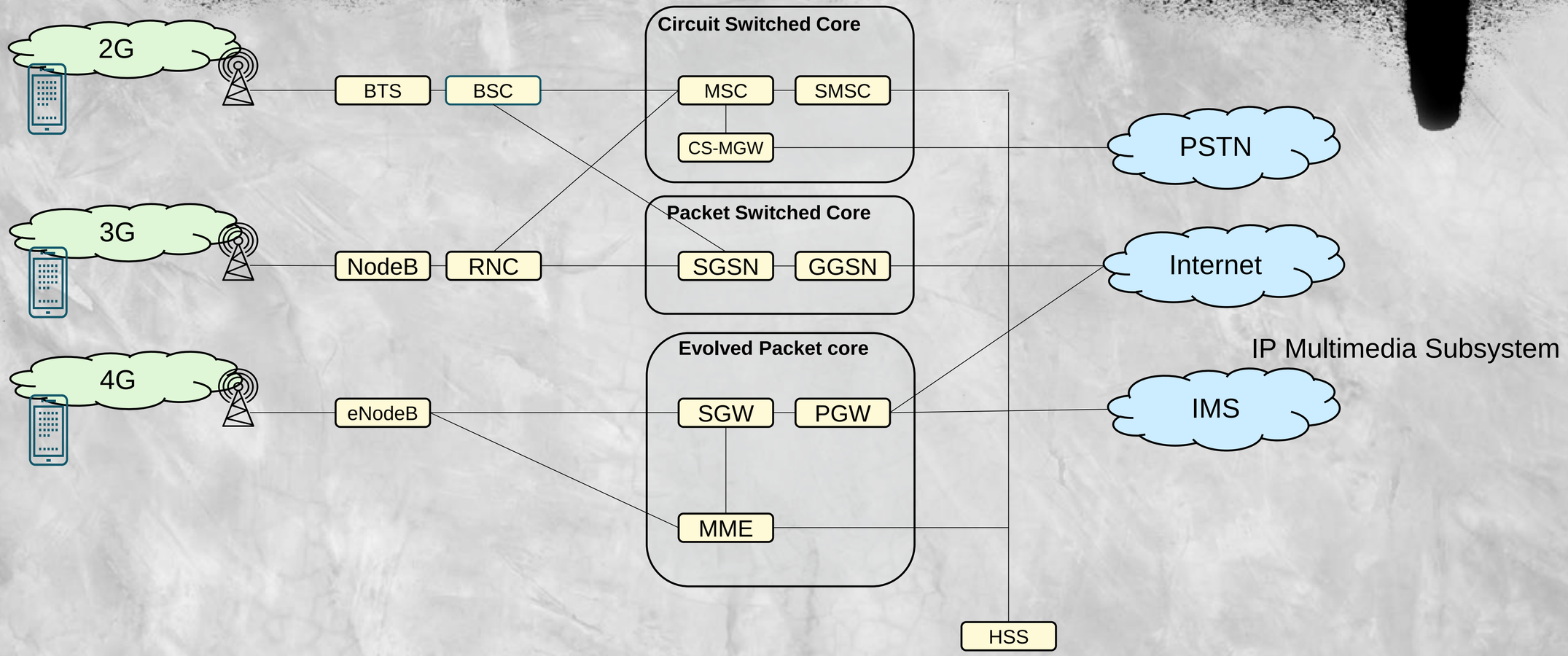

2G
3G
4G
BTS
BSC
NodeB
RNC
eNodeB
Circuit Switched Core
MSC
SMSC
CS-MGW
Packet Switched Core
SGSN
GGSN
Evolved Packet core
SGW
PGW
MME
HSS
PSTN
Internet

4G voice?



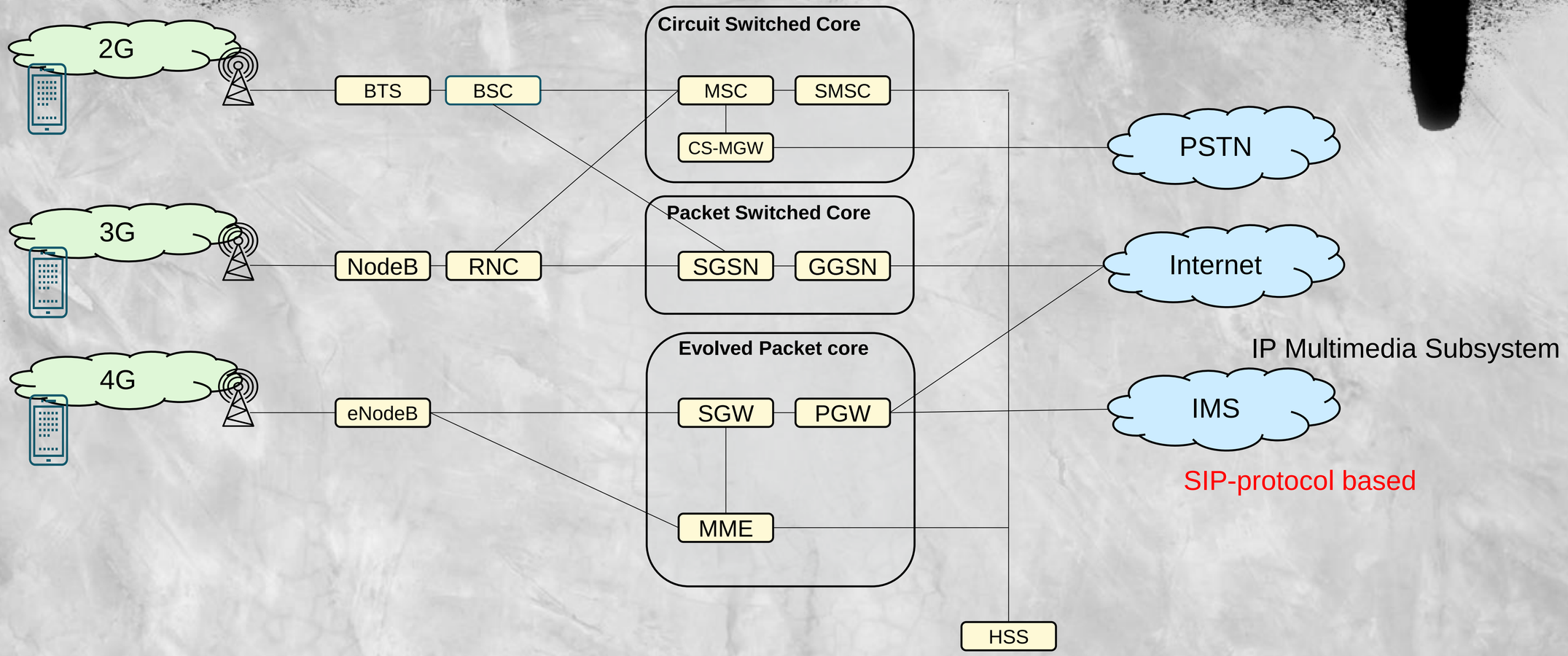
SecurityGen
Telecom Security. Transcending Generations.

4G native voice



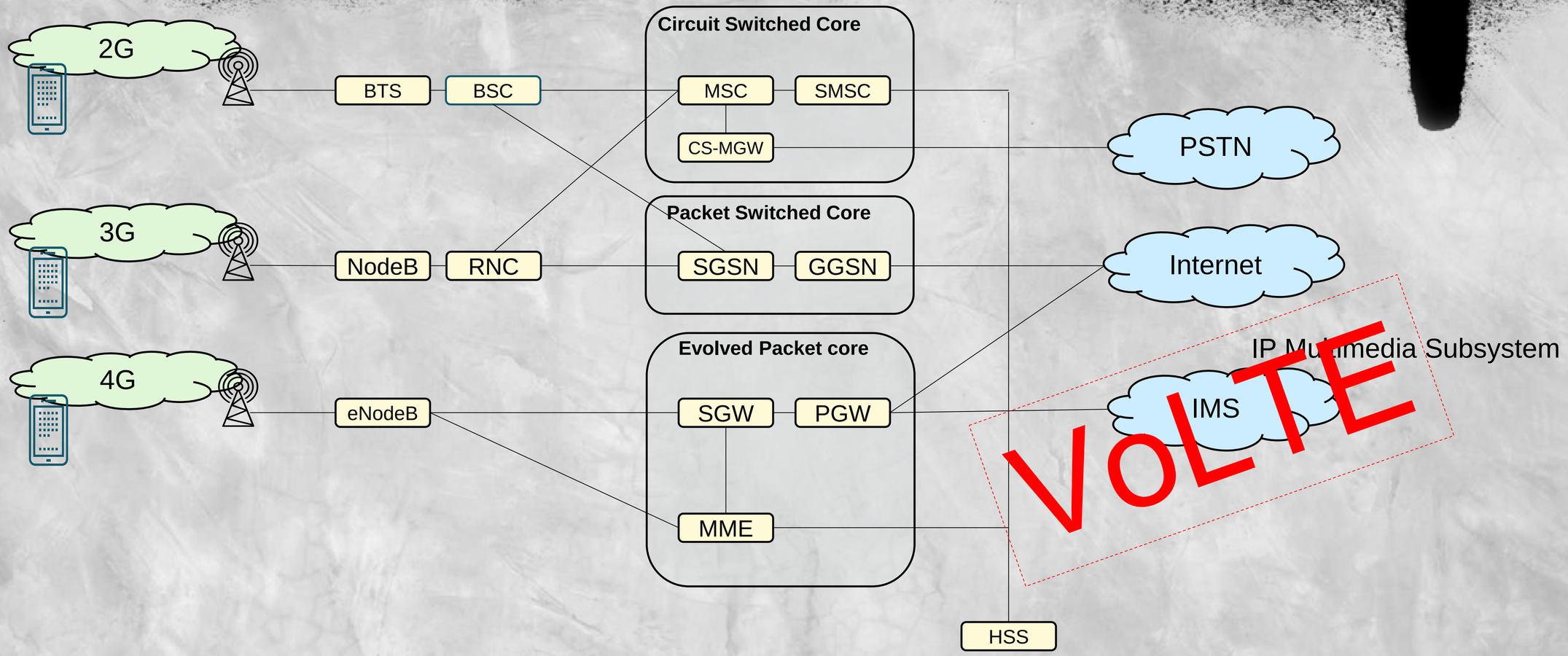
SecurityGen
Telecom Security. Transcending Generations.

4G native voice

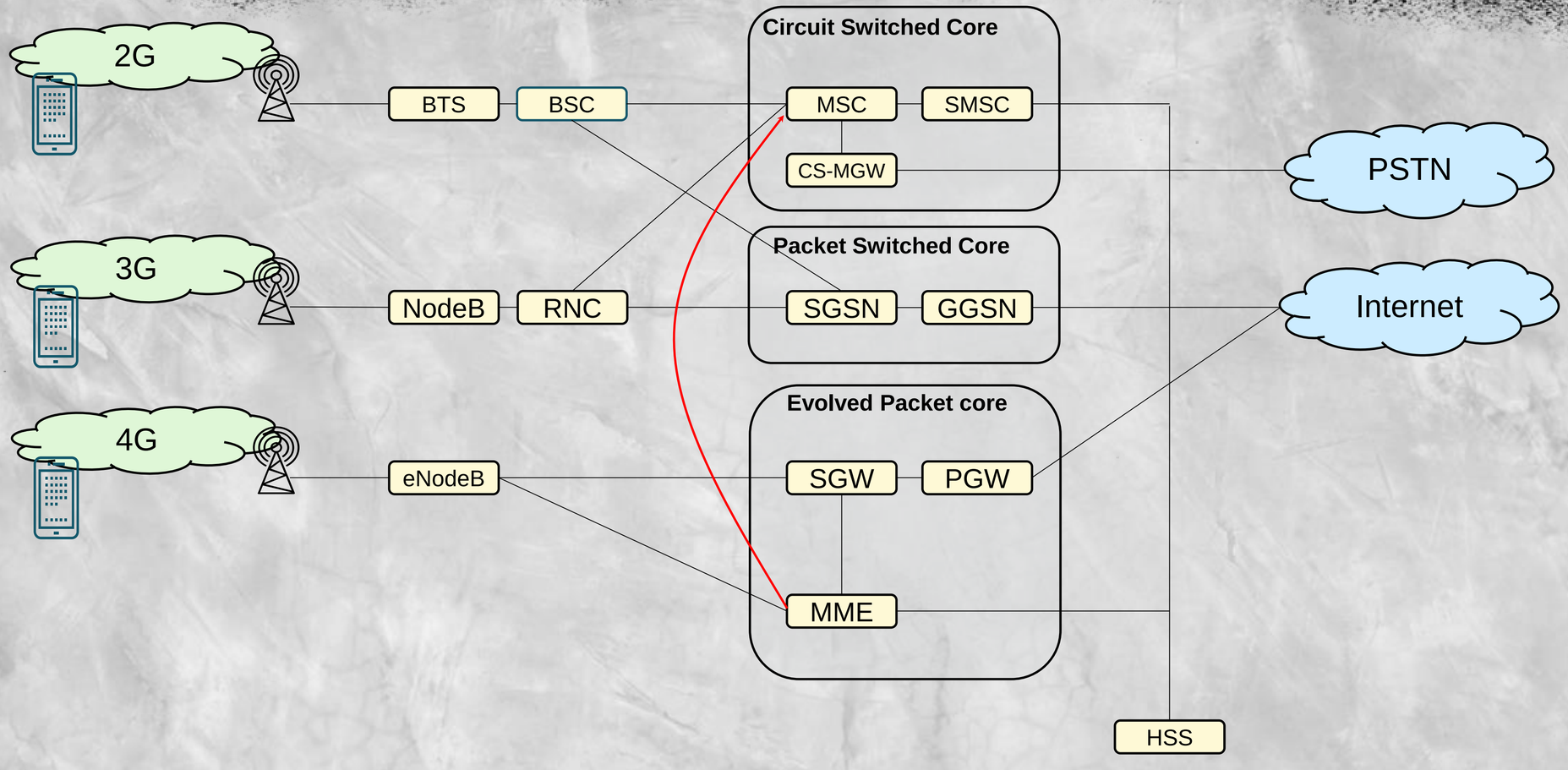


SecurityGen
Telecom Security. Transcending Generations.

Voice-over-LTE = VoLTE

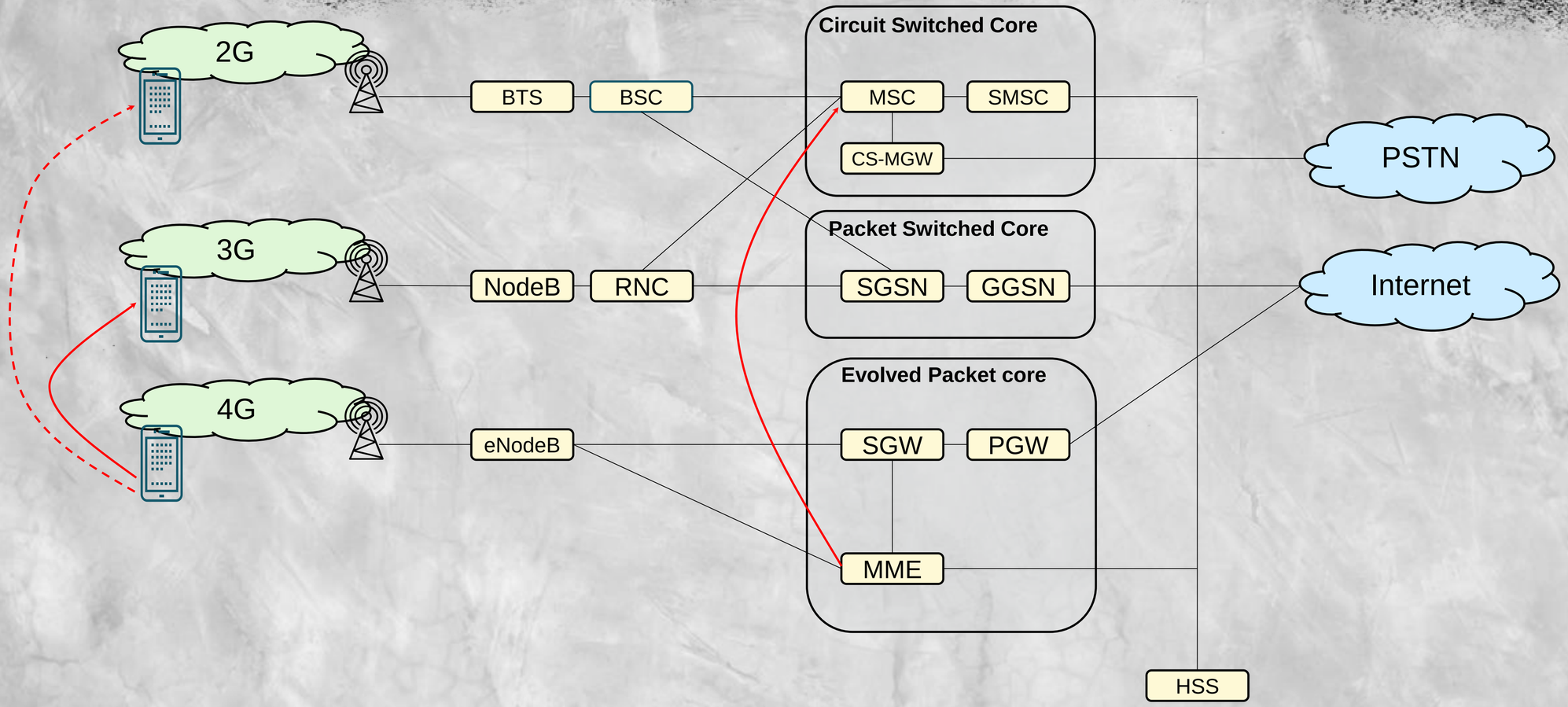


CS-Fallback voice



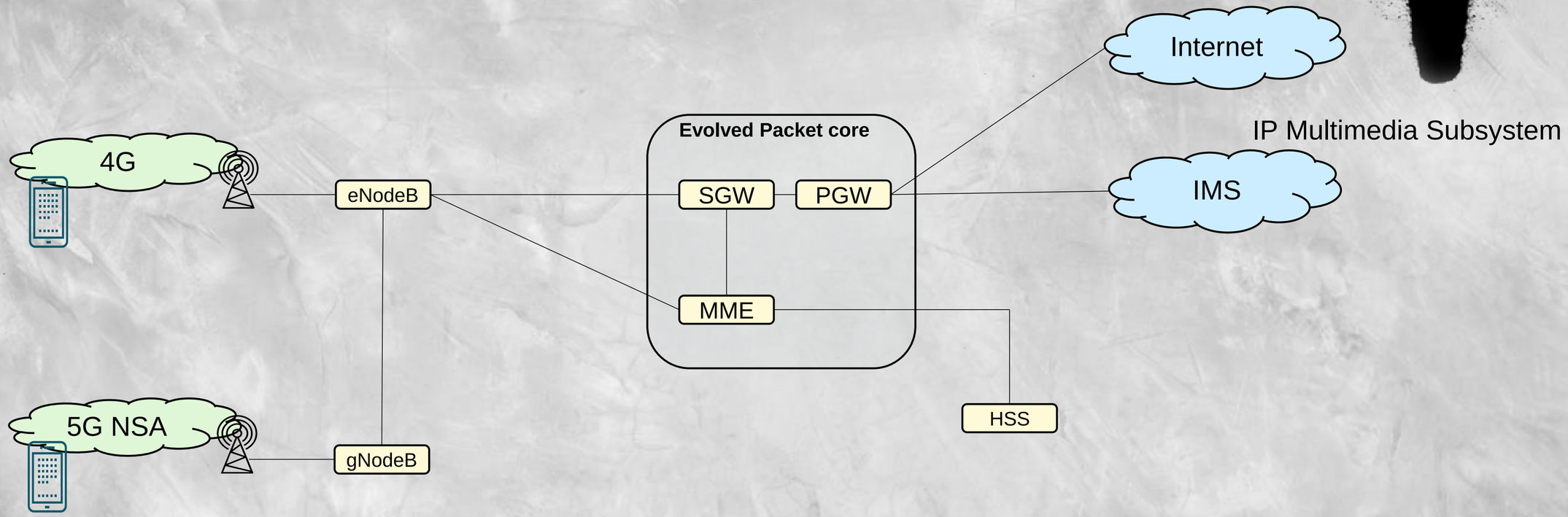
SecurityGen
Telecom Security. Transcending Generations.

CS-Fallback voice

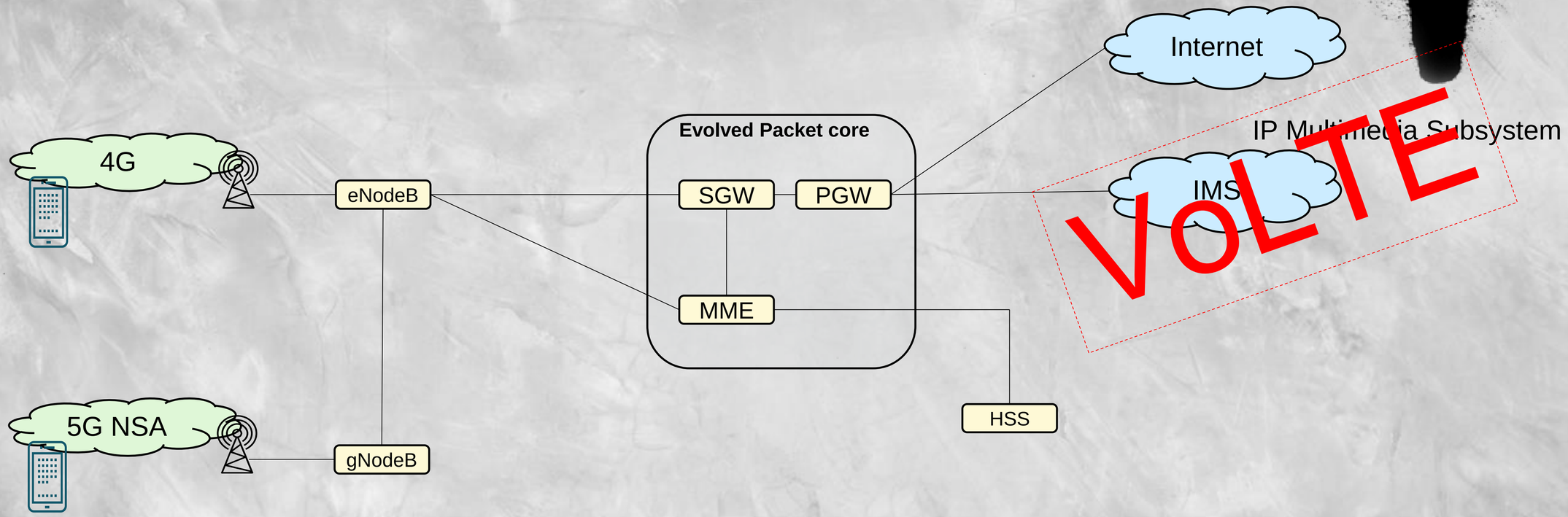


SecurityGen
Telecom Security. Transcending Generations.

5G NSA native voice

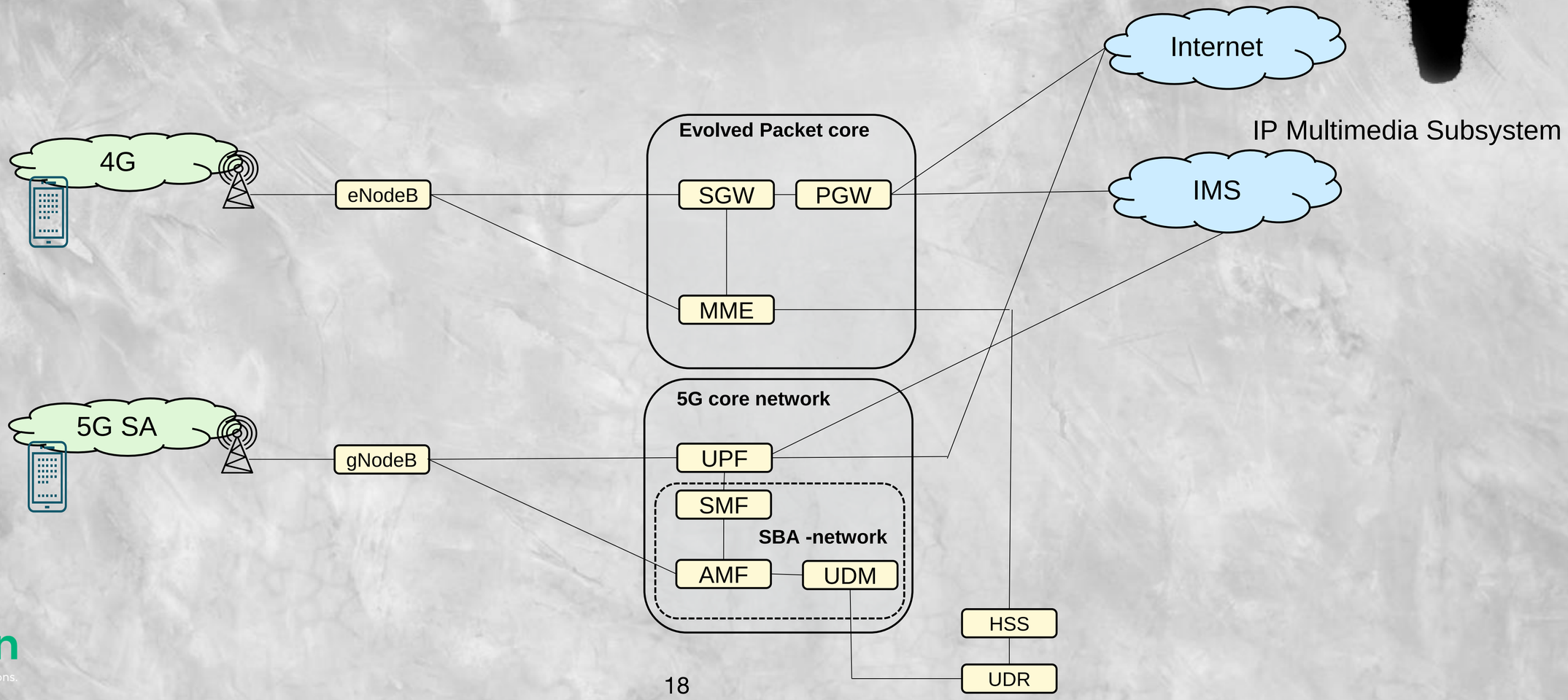


5G NSA native voice



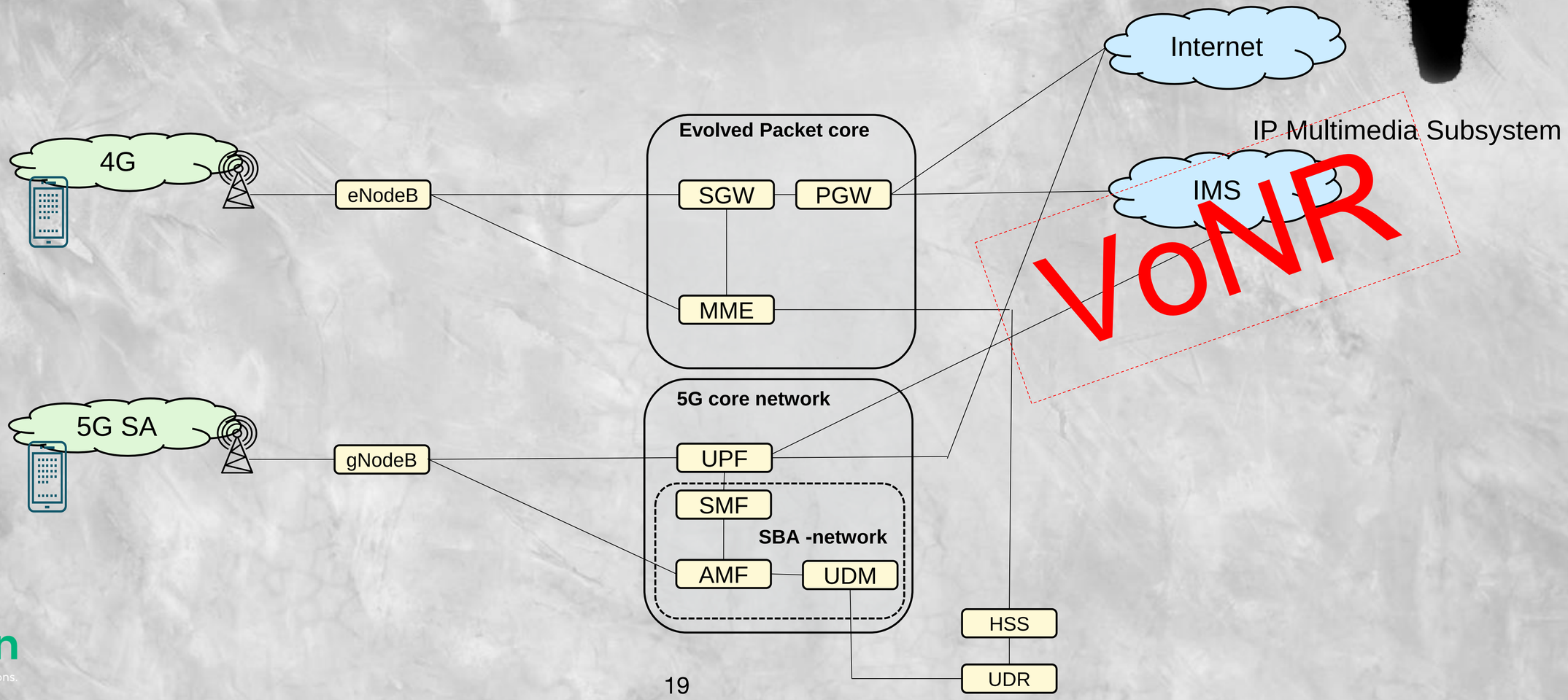
SecurityGen
Telecom Security. Transcending Generations.

5G native voice



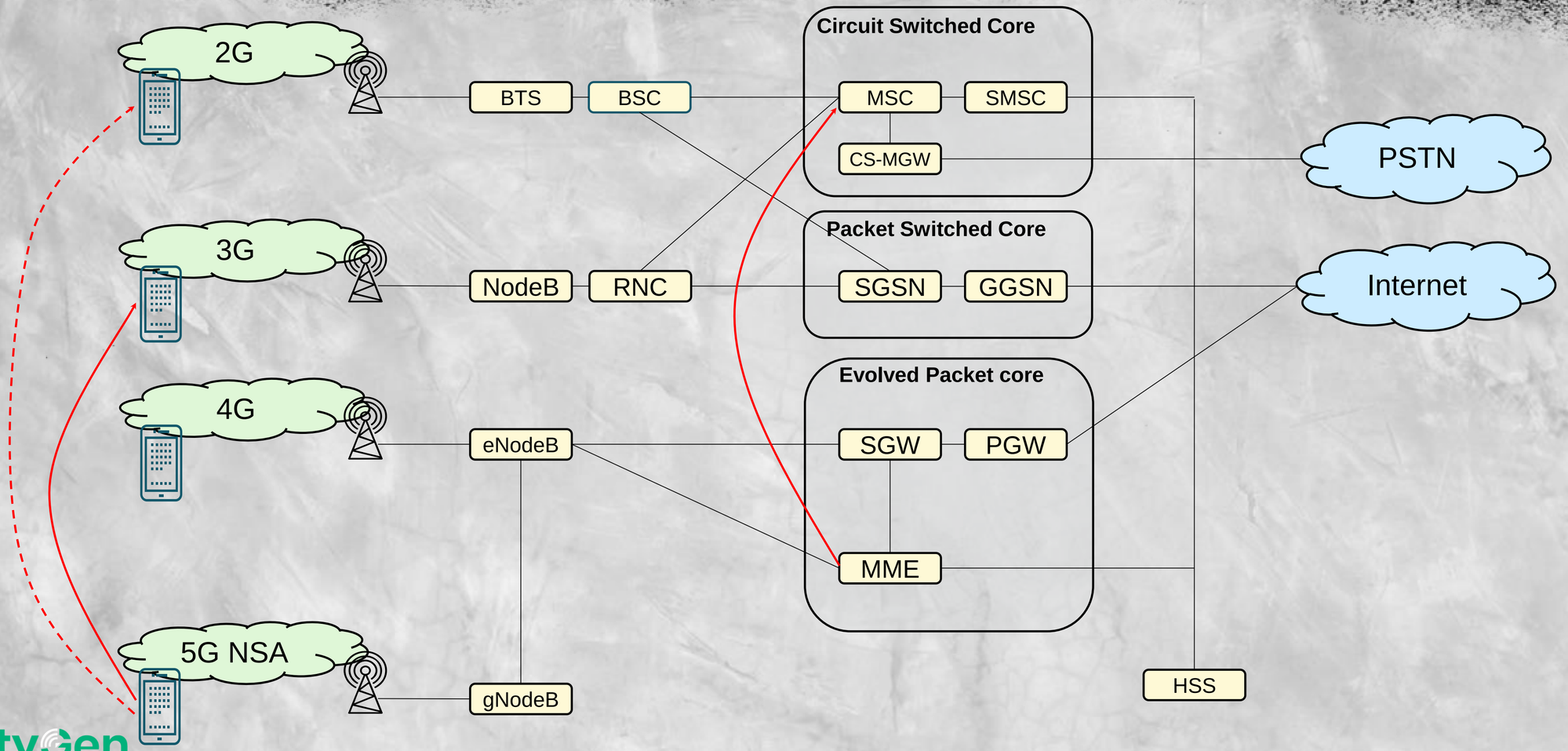
SecurityGen
Telecom Security. Transcending Generations.

Voice-over-New-Radio = VoNR



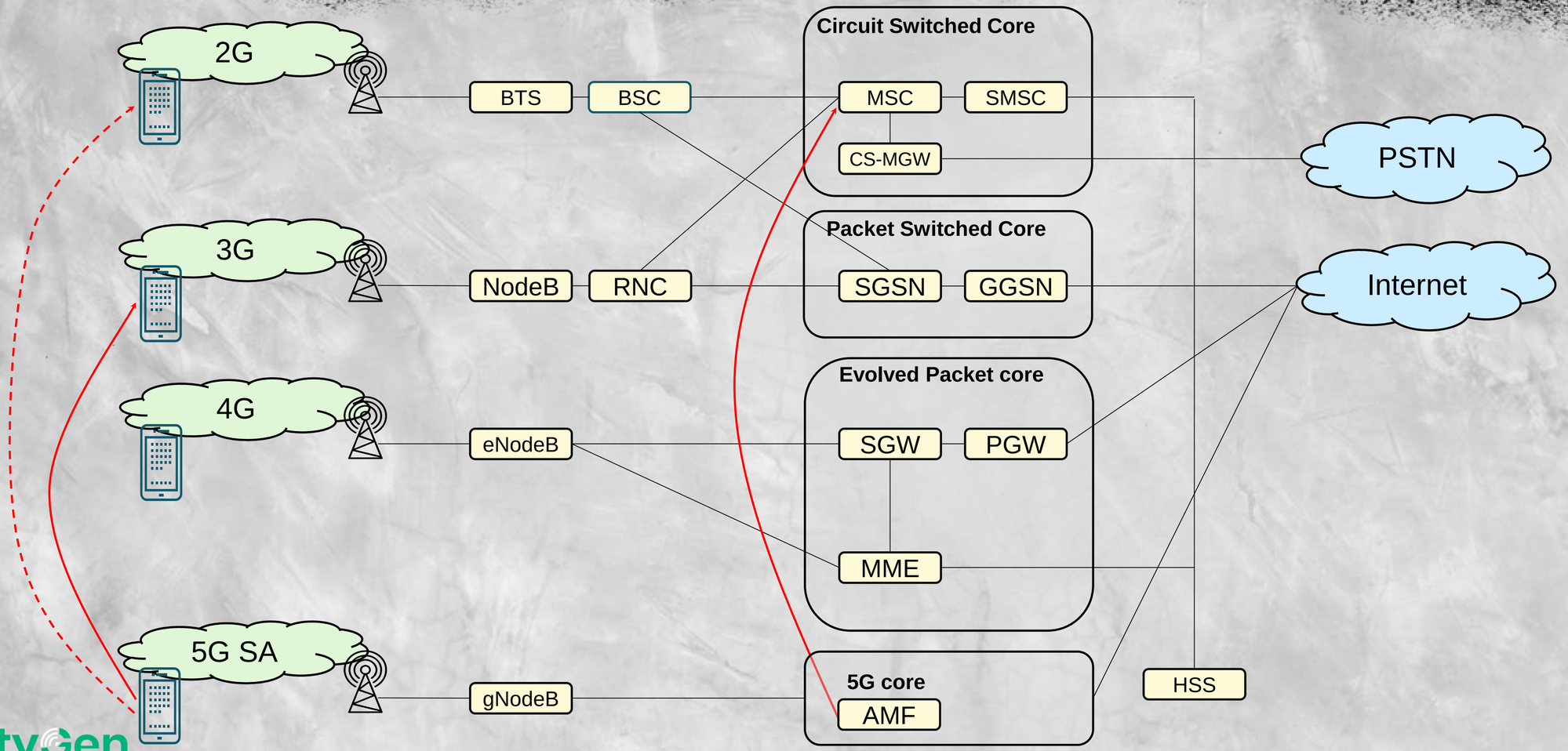
SecurityGen
Telecom Security. Transcending Generations.

5G NSA fallback



SecurityGen
Telecom Security. Transcending Generations.

5G SA fallback



SecurityGen
Telecom Security. Transcending Generations.

Let’s dig into the history

-1st LTE network deployed in December 2009 (TeliaSonera, Sweden + Norway)

SecurityGen
Telecom Security. Transcending Generations.

Let’s dig into the history

-1st LTE network deployed in December 2009 (TeliaSonera, Sweden + Norway)
-1st VoLTE network support in August 2012 (USA) and first VoLTE phone LG Connect 4G.

SecurityGen
Telecom Security. Transcending Generations.

Let’s dig into the history

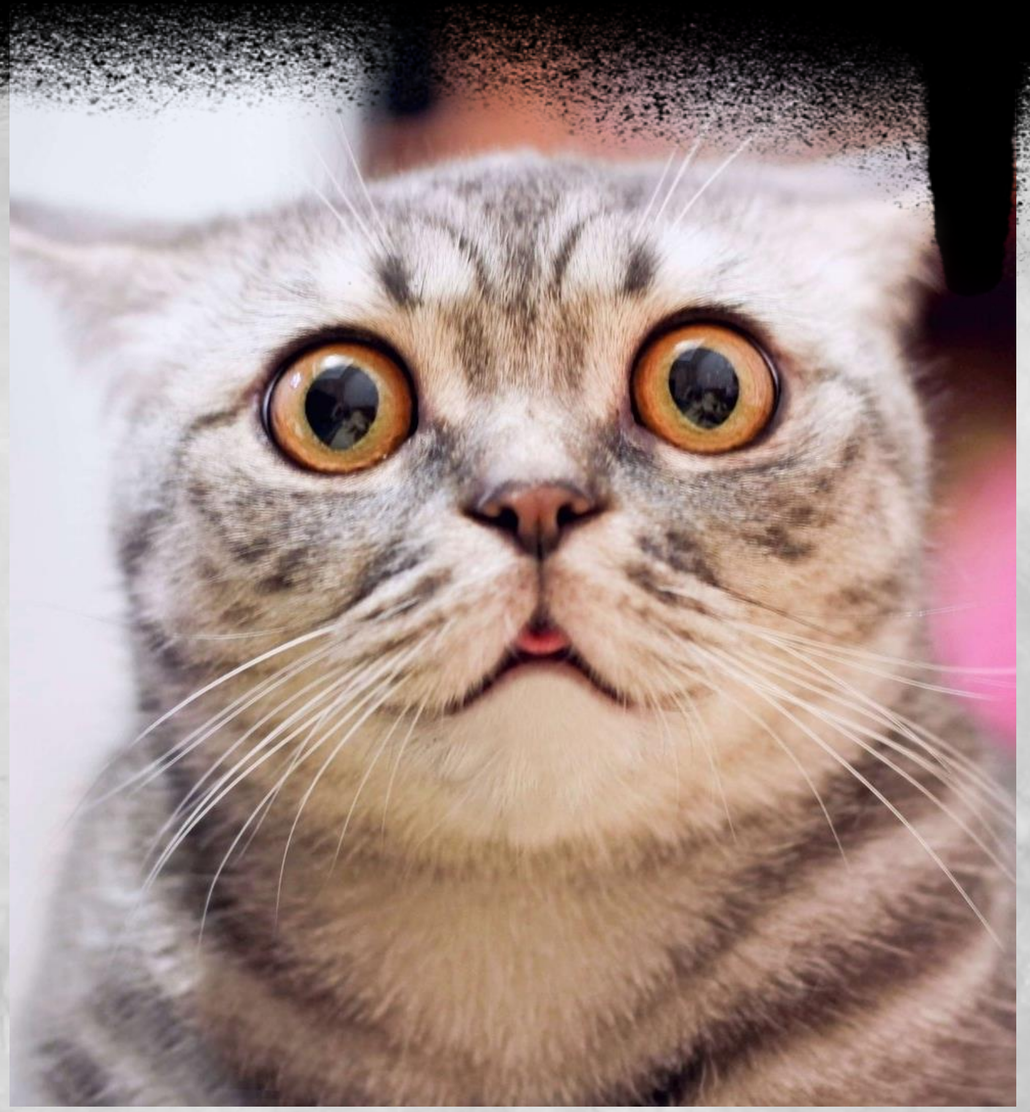
-1st LTE network deployed in December 2009 (TeliaSonera, Sweden + Norway)
-1st VoLTE network support in August 2012 (USA) and first VoLTE phone LG Connect 4G.
-full-featured VoLTE network in May 2014 (Singapore) with only phone Samsung Galaxy Note 3

Let’s dig into the history

-1st LTE network deployed in December 2009 (TeliaSonera, Sweden + Norway)
-1st VoLTE network support in August 2012 (USA) and first VoLTE phone LG Connect 4G.
-full-featured VoLTE network in May 2014 (Singapore) with only phone Samsung Galaxy Note 3
-almost all new phones having VoLTE support in 2020

Let’s dig into the history

Almost all new phones having VoLTE support ONLY in 2020…
10 years after LTE network was deployed



SecurityGen
Telecom Security. Transcending Generations.

MNO: It seems time to deploy VoLTE...

Telco industry

SecurityGen
Telecom Security. Transcending Generations.

Bombshell

Verizon (USA) retire their 2G and 3G network by 31 December 2022

SecurityGen
Telecom Security. Transcending Generations.

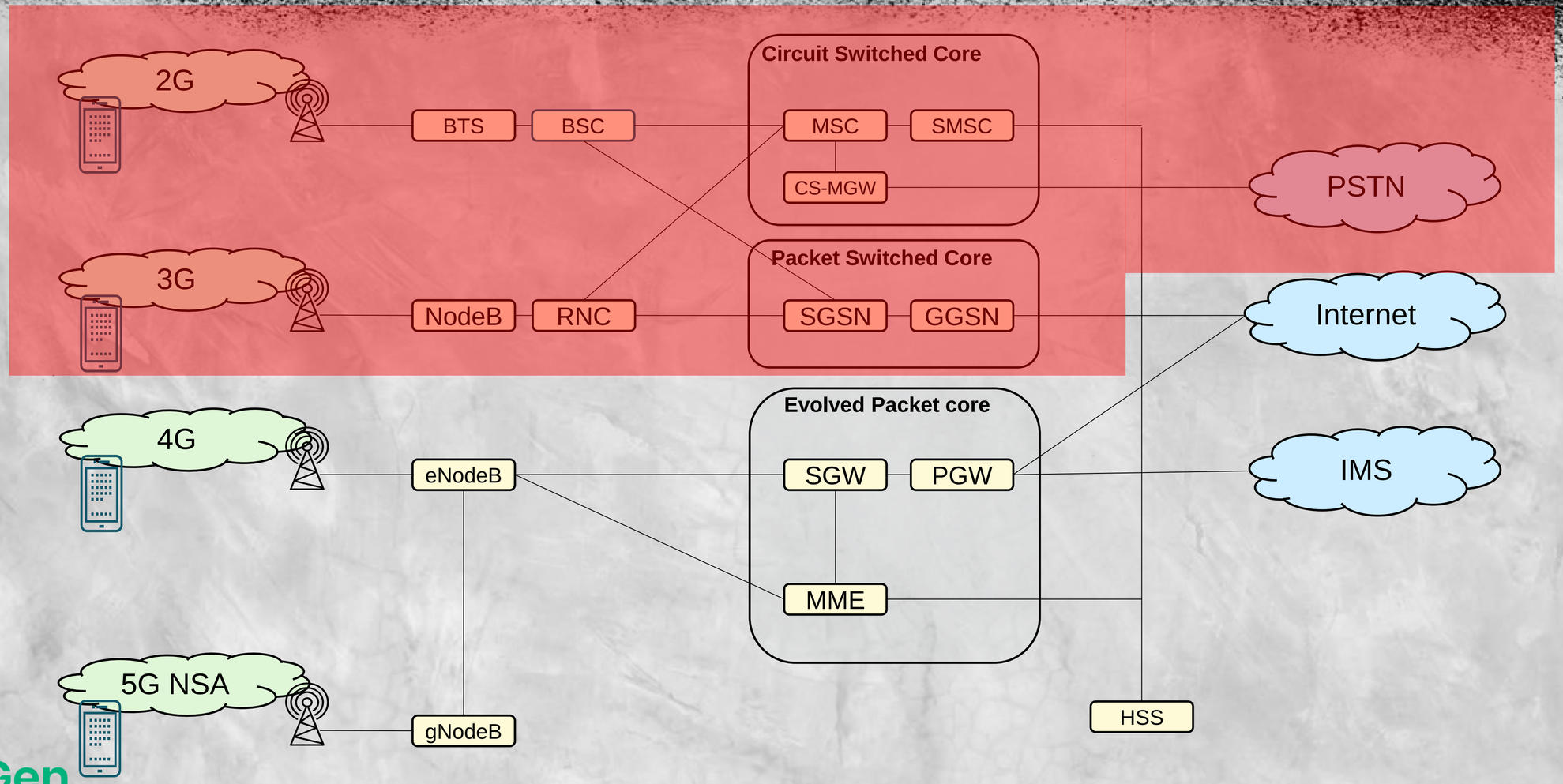
Bombshell

Verizon (USA) retire their 2G and 3G network by 31 December 2022

Initially they said that it will happen in the end of 2019, but they postponed, because industry was not ready, that’s why many other haven’t believed that in the end of 2022 they will do that.

SecurityGen
Telecom Security. Transcending Generations.

2G/3G retire



SecurityGen
Telecom Security. Transcending Generations.

All the networks in the world was affected

- Verizon (USA) retire their 2G and 3G network by 31 December 2022

- It means, that if subscriber of some network without VoLTE goes to the USA, he will not be able to call anymore.

SecurityGen
Telecom Security. Transcending Generations.

All the networks in the world was affected

- Verizon (USA) retire their 2G and 3G network by 31 December 2022

- It means, that if subscriber of some network without VoLTE goes to the USA, he will not be able to call anymore.
- Money and reputation are affected

SecurityGen
Telecom Security. Transcending Generations.

Build VoLTE network in 60 seconds…

- Operators started to build their VoLTE network very fast, many of them built it in few months.

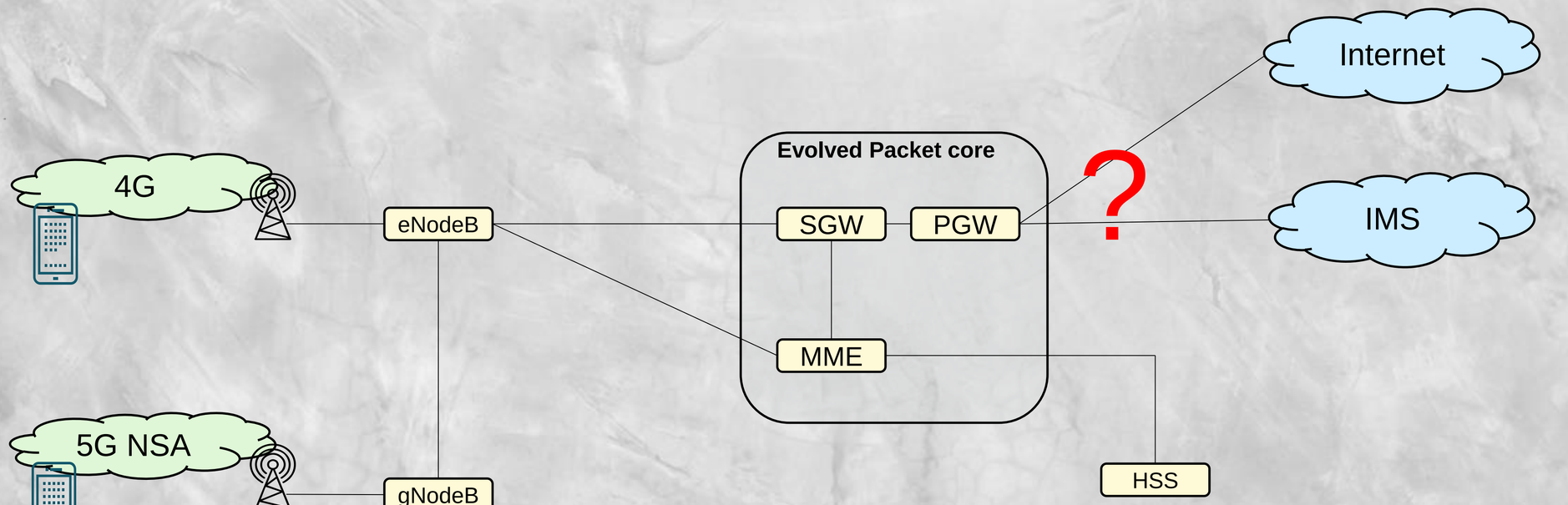
Build VoLTE network in 60 seconds…

- Operators started to build their VoLTE network very fast, many of them built it in few months.
- Many configuration mistakes were made

SecurityGen
Telecom Security. Transcending Generations.

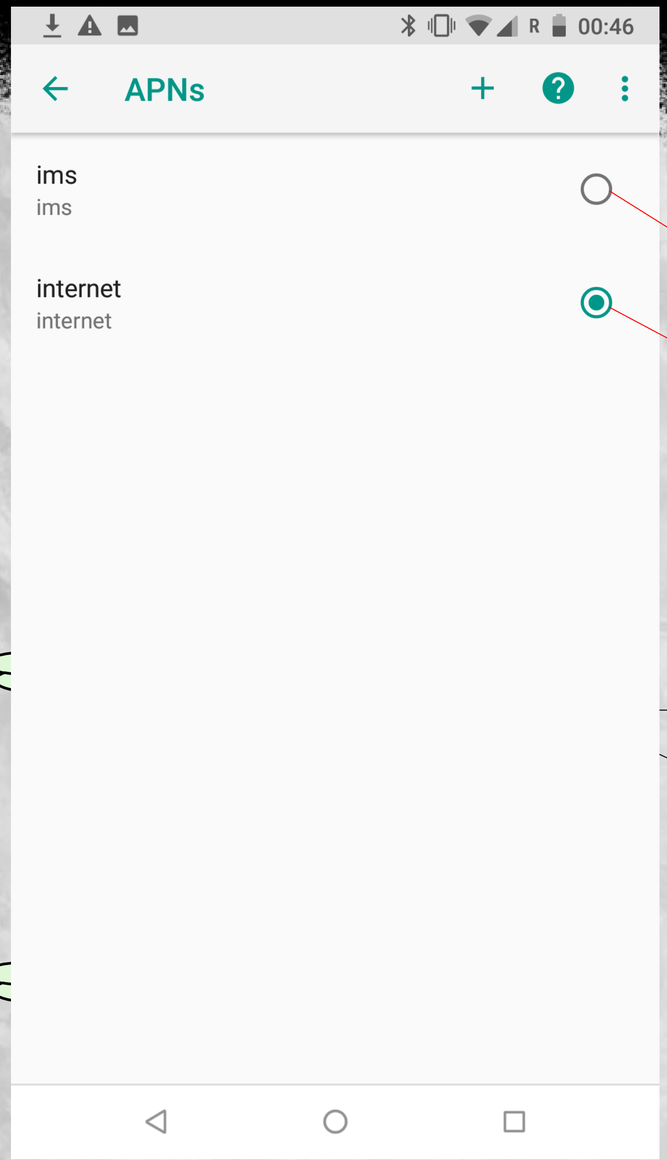
IMS network

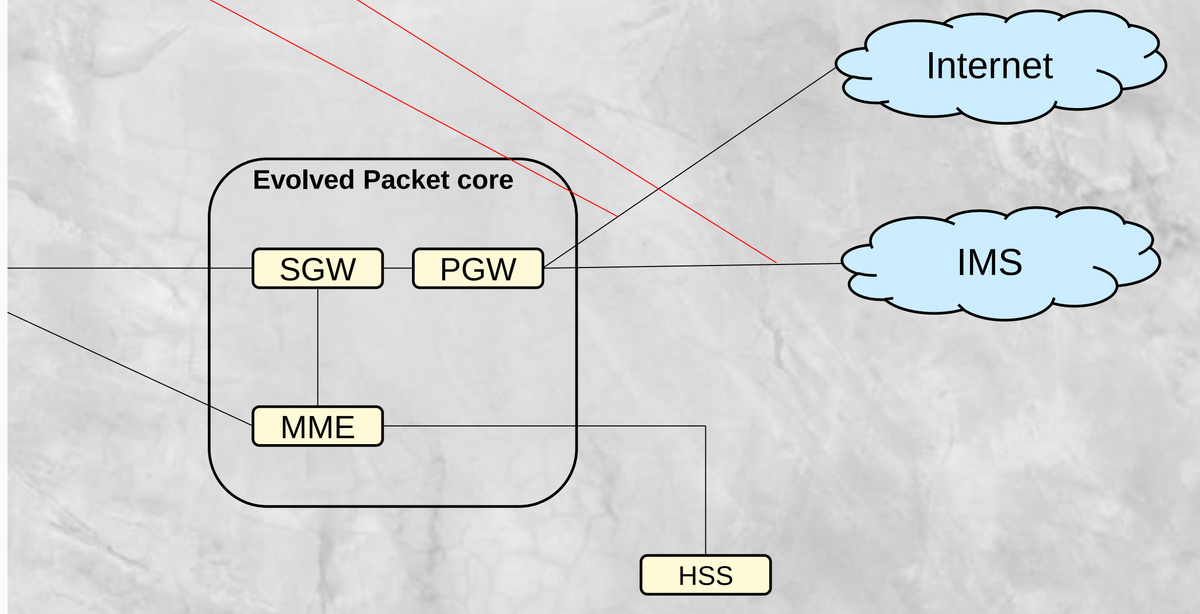
APN – outside network



SecurityGen
Telecom Security. Transcending Generations.

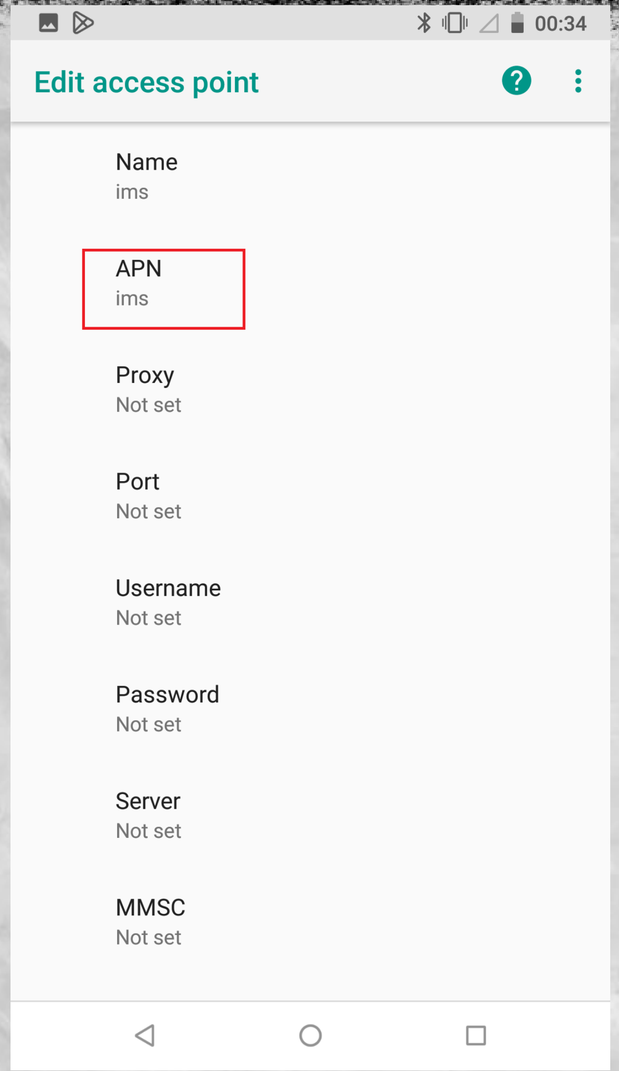
APN – outside network

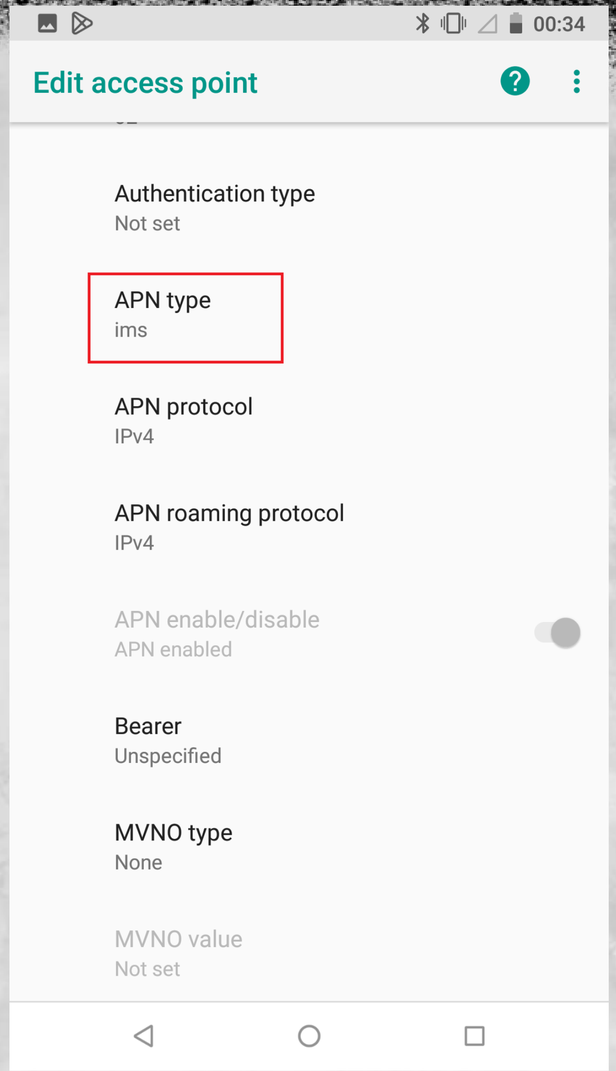




SecurityGen
Telecom Security. Transcending Generations.

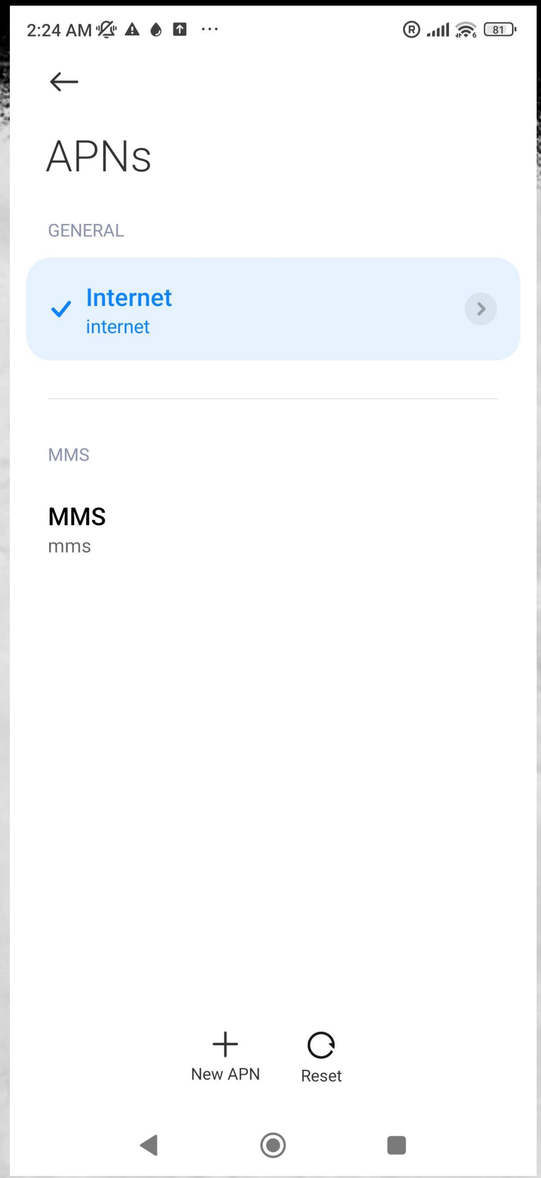
IMS APN


00:34
Edit access point
Name
ims
APN
ims
Proxy
Not set
Port
Not set
Username
Not set
Password
Not set
Server
Not set
MMSC
Not set


00:34
Edit access point
Authentication type
Not set
APN type
ims
APN protocol
IPv4
APN roaming protocol
IPv4
APN enable/disable
APN enabled
Bearer
Unspecified
MVNO type
None
MVNO value
Not set

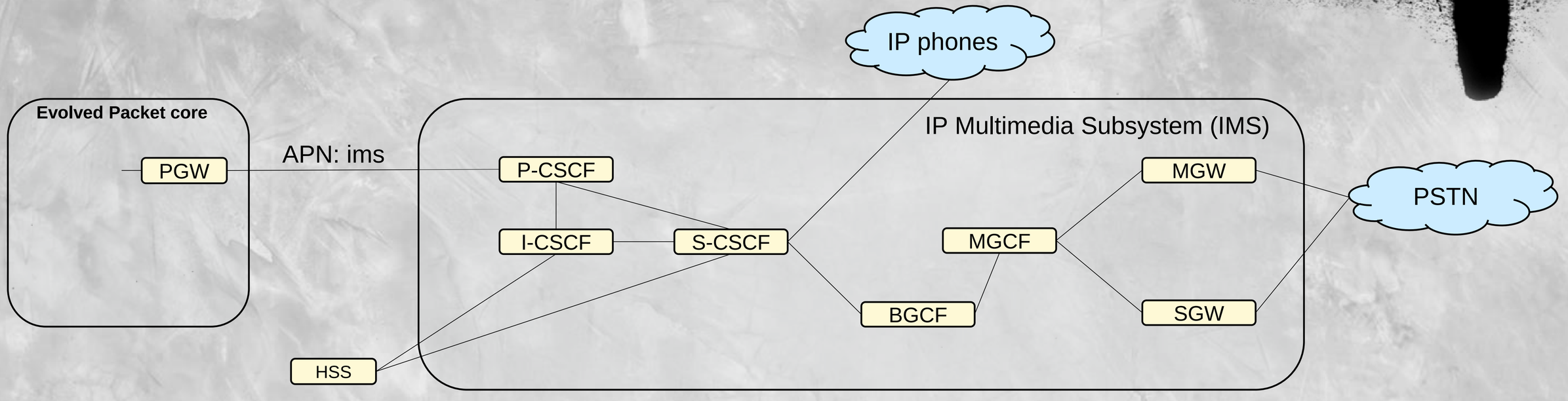
Security by obscurity

Modern phones are hiding IMS APN from list of APNs



SecurityGen
Telecom Security. Transcending Generations.

IMS network

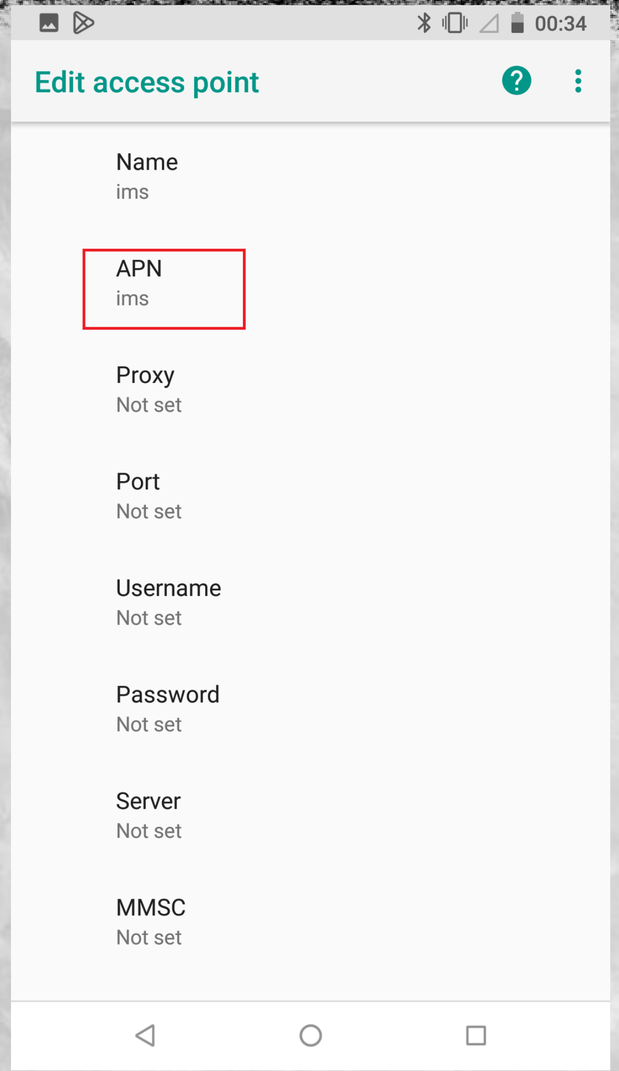

IP phones
Evolved Packet core
PGW
APN: ims
IP Multimedia Subsystem (IMS)
P-CSCF
I-CSCF
S-CSCF
BGCF
MGCF
MGW
SGW
PSTN
HSS

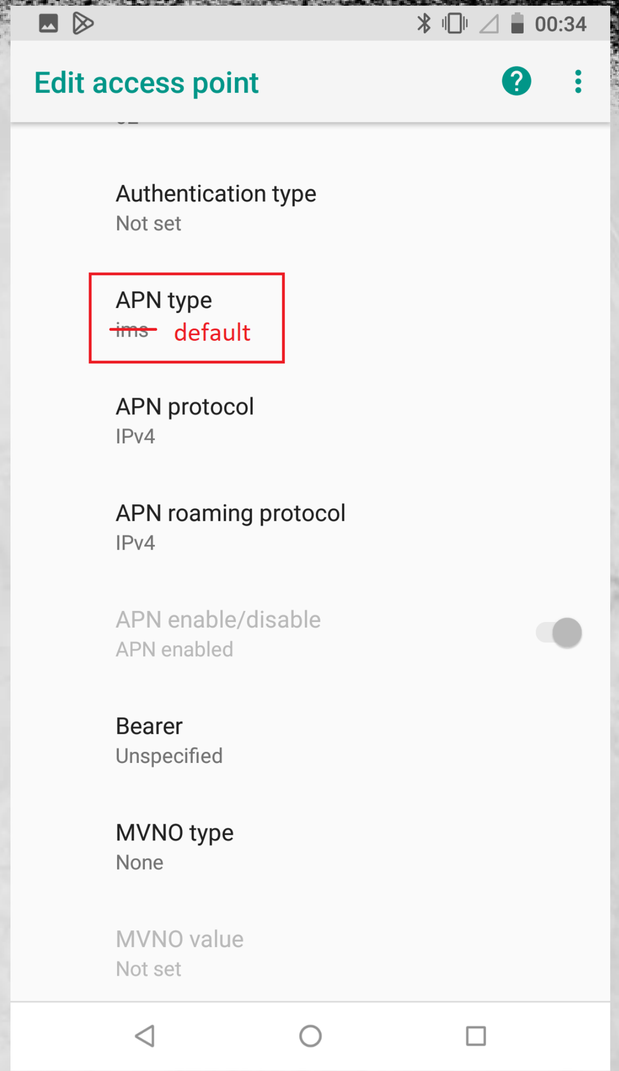
So.. How to hijack VoLTE network?

Break rules!

SecurityGen
Telecom Security. Transcending Generations.

IMS APN





SecurityGen
Telecom Security. Transcending Generations.

Run nmap?

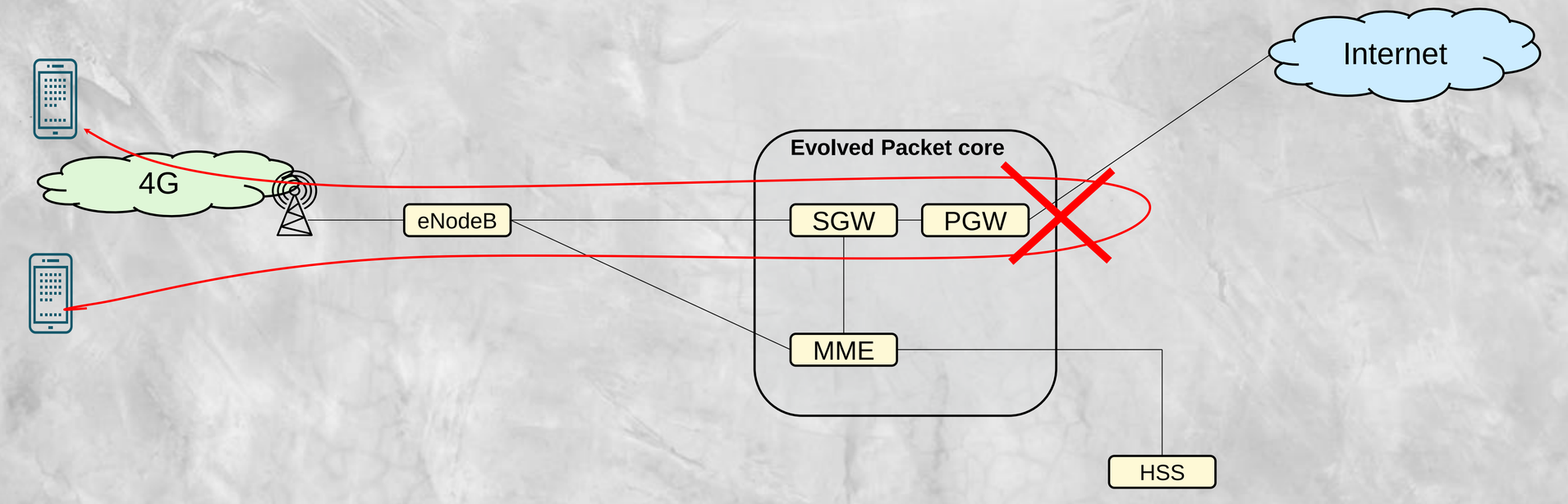
SecurityGen
Telecom Security. Transcending Generations.

Better to use common tools

1. LTE modem + laptop
2. Configure APN: ims
3. Take profit!

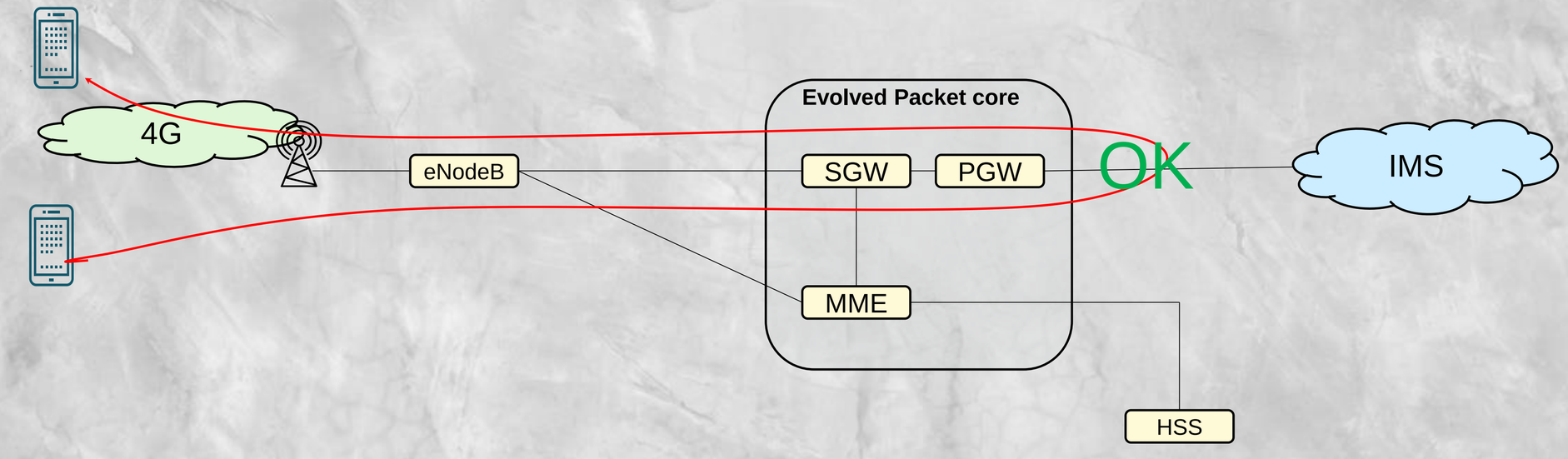
SecurityGen
Telecom Security. Transcending Generations.

Subscriber isolation for internet connection



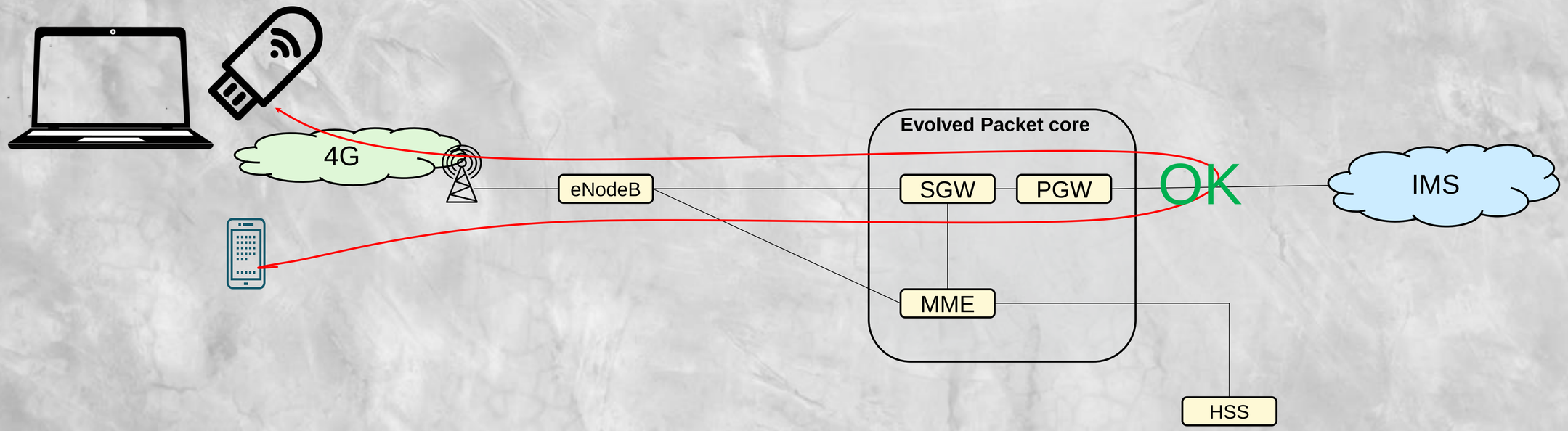
SecurityGen
Telecom Security. Transcending Generations.

No isolation for IMS interface



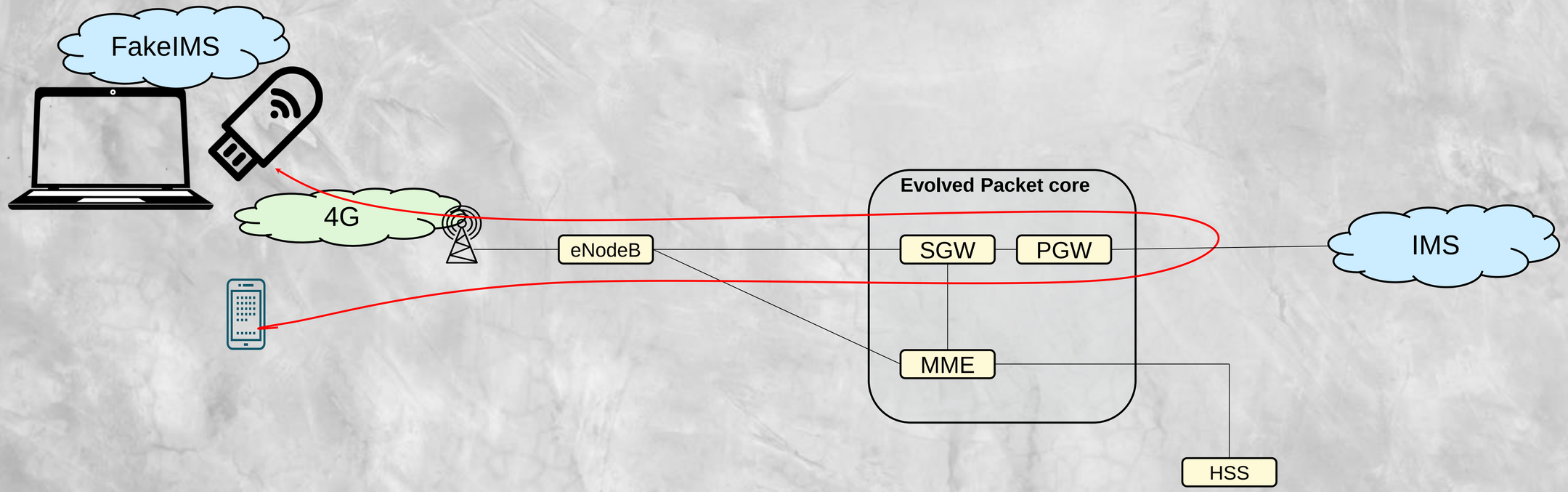
SecurityGen
Telecom Security. Transcending Generations.

Let’s get access as legal subscriber



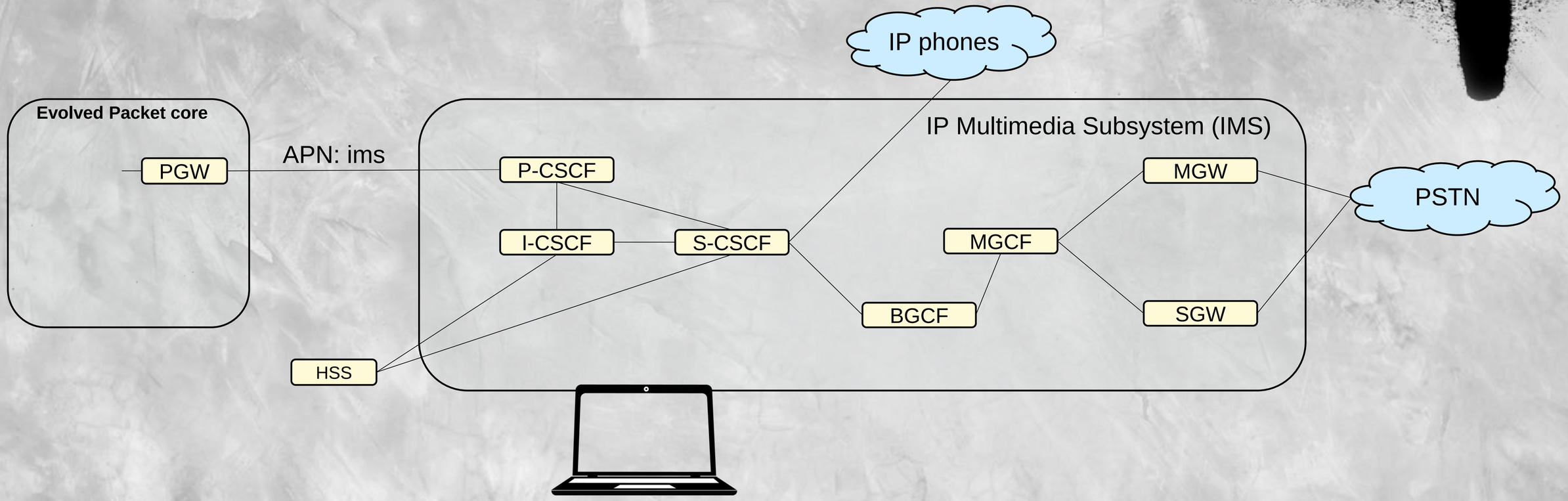
SecurityGen
Telecom Security. Transcending Generations.

Build own fakeIMS infra?

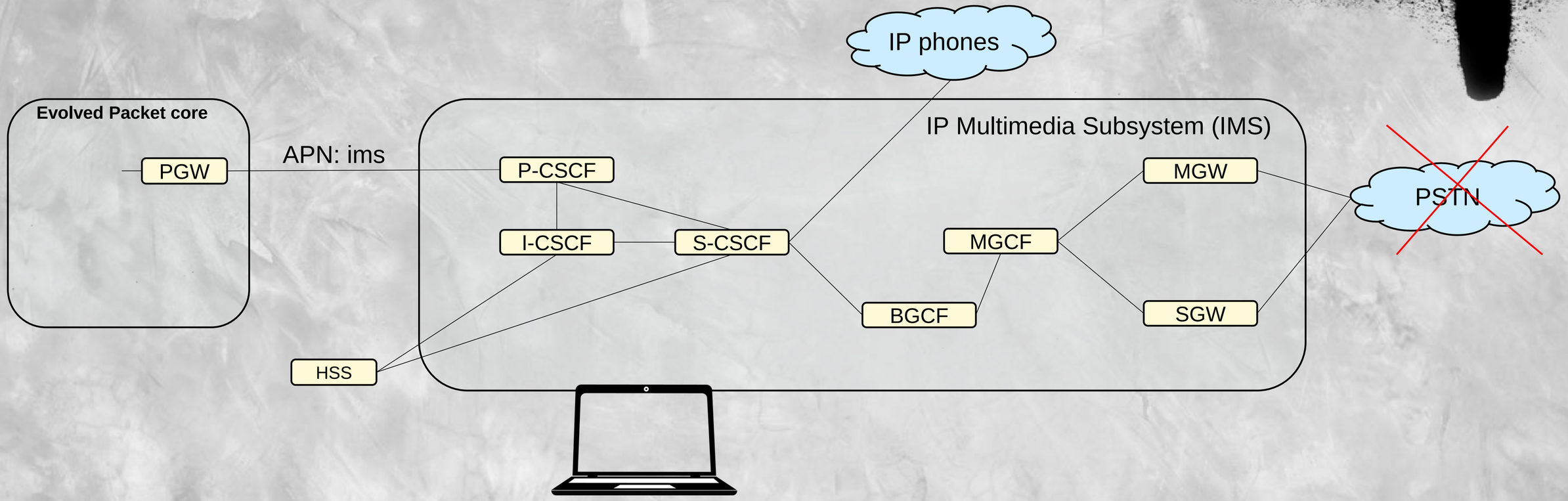


SecurityGen
Telecom Security. Transcending Generations.

Emulate IMS network

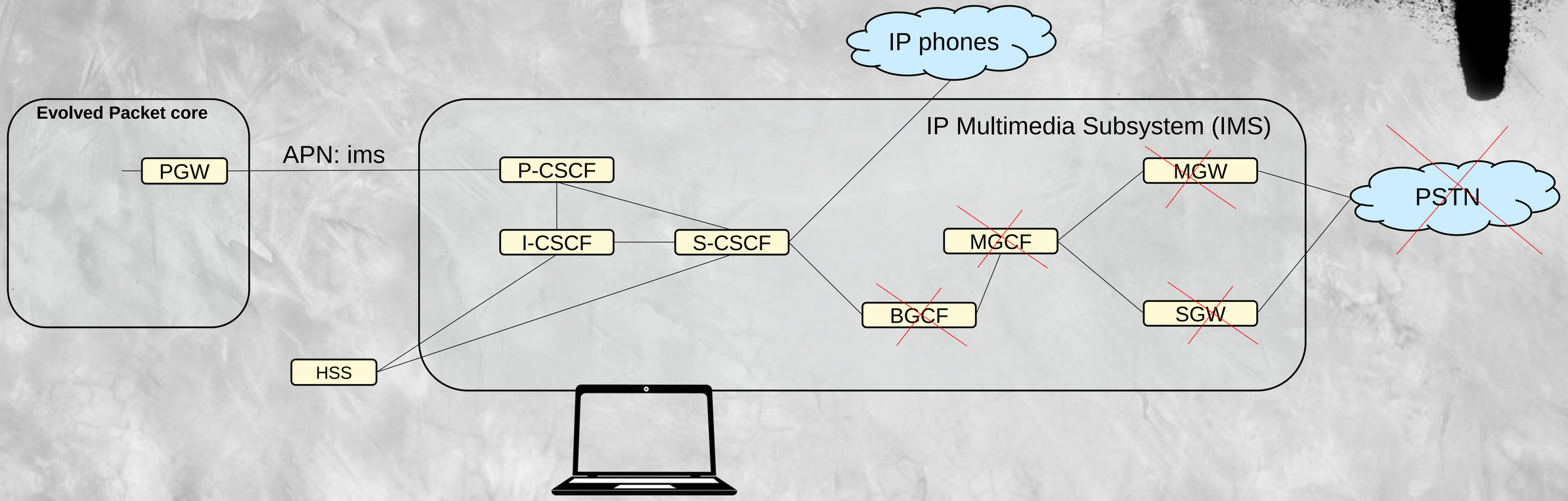


Emulate IMS network



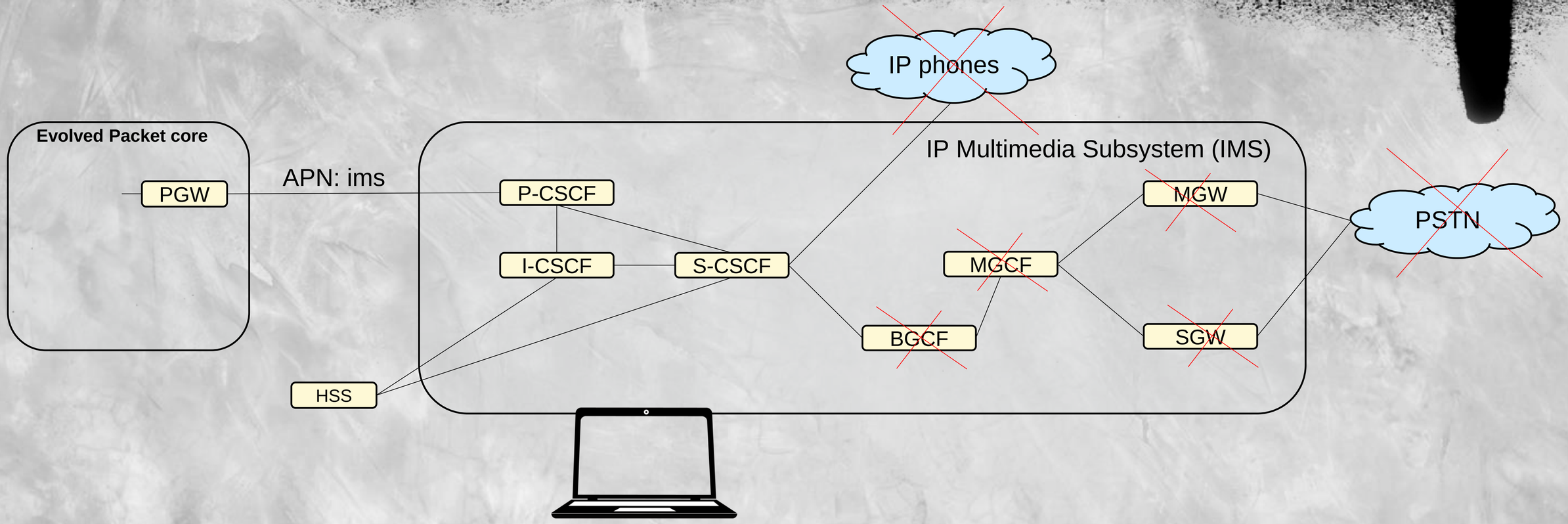
SecurityGen
Telecom Security. Transcending Generations.

Emulate IMS network



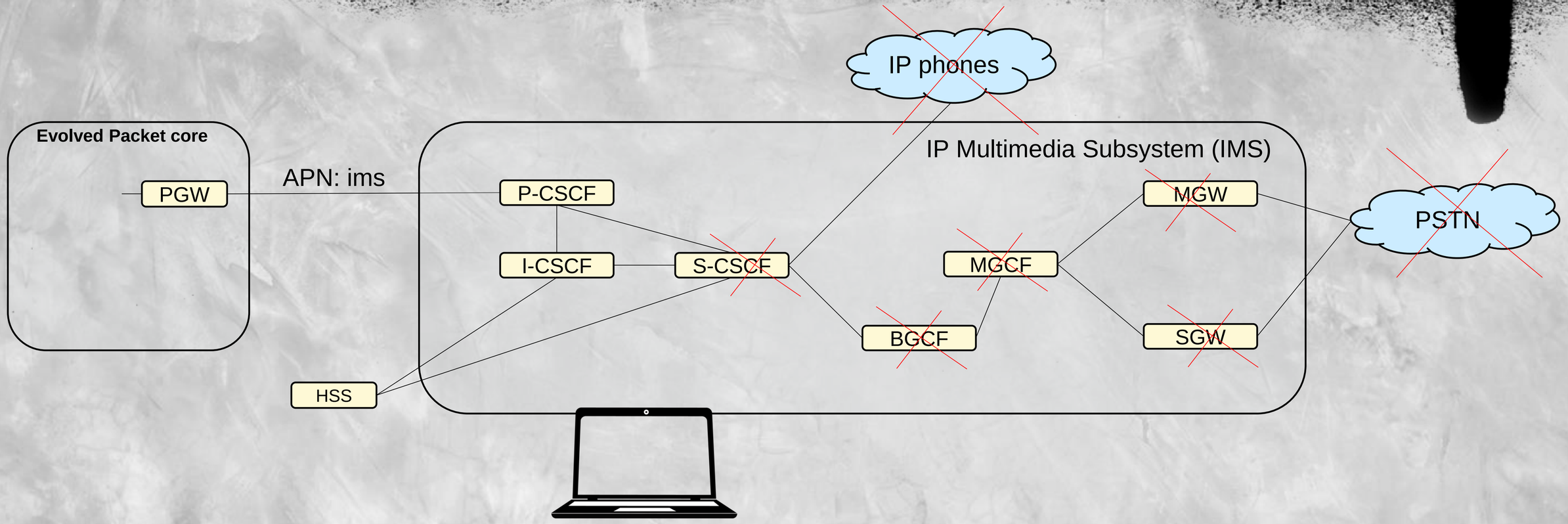
SecurityGen
Telecom Security. Transcending Generations.

Emulate IMS network



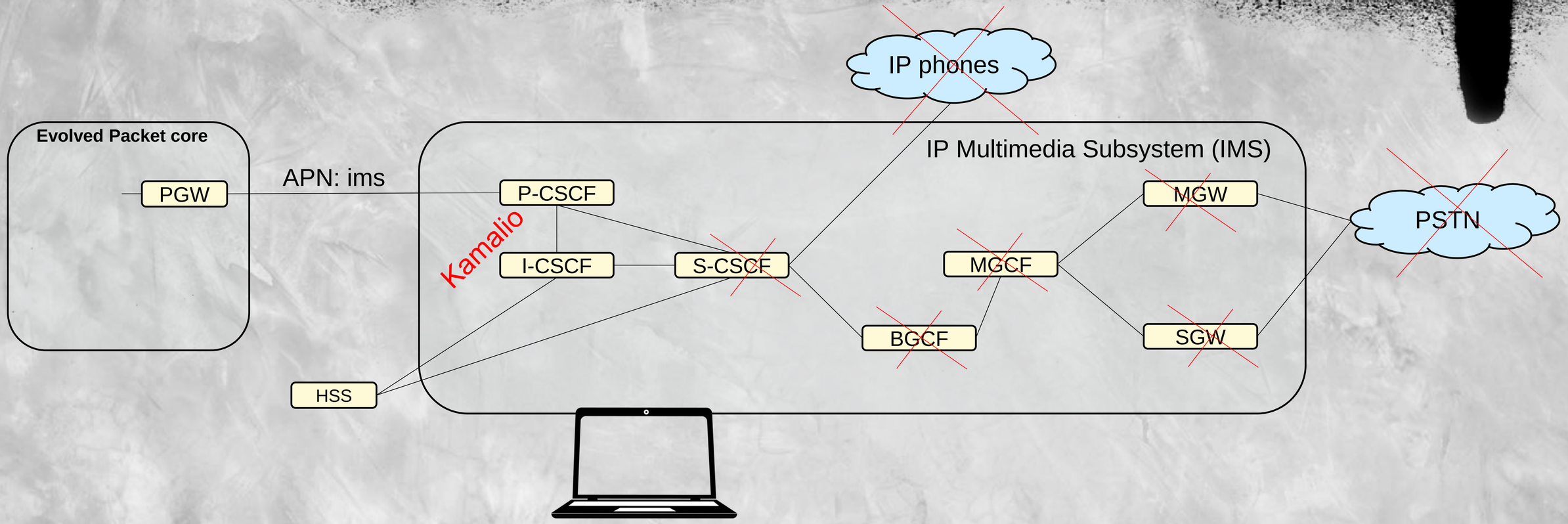
SecurityGen
Telecom Security. Transcending Generations.

Emulate IMS network



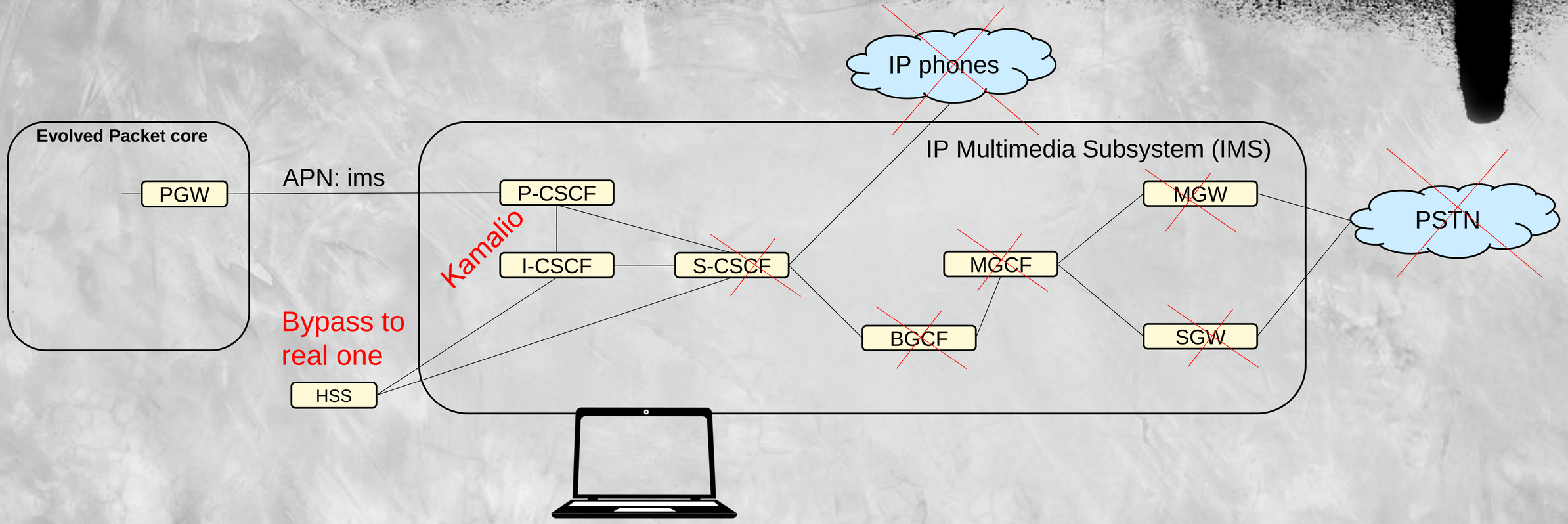
SecurityGen
Telecom Security. Transcending Generations.

Emulate IMS network



SecurityGen
Telecom Security. Transcending Generations.

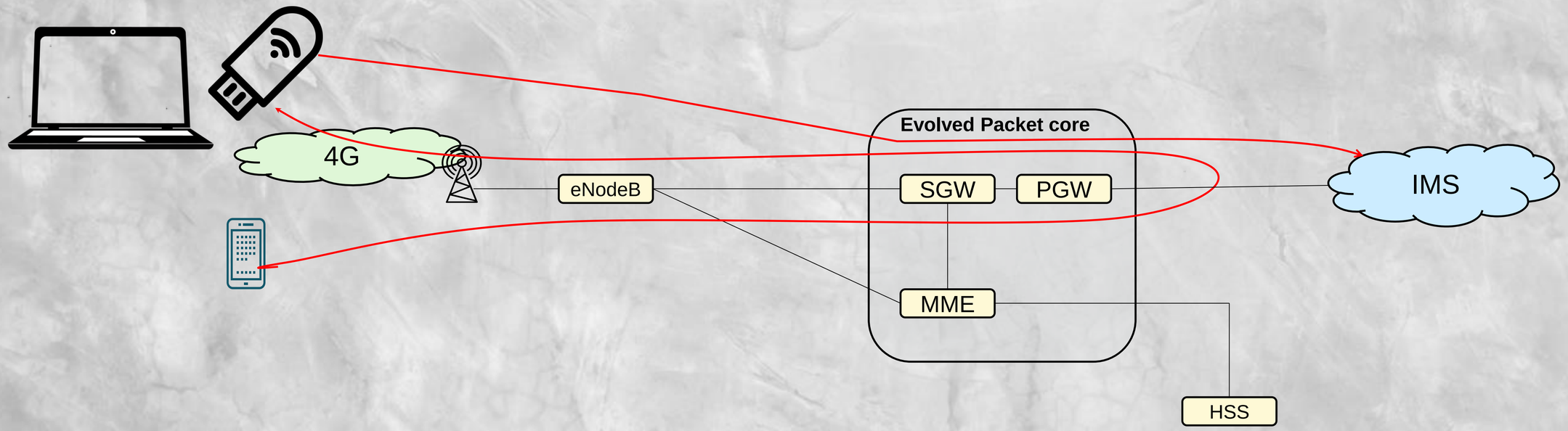
Emulate IMS network



SecurityGen
Telecom Security. Transcending Generations.

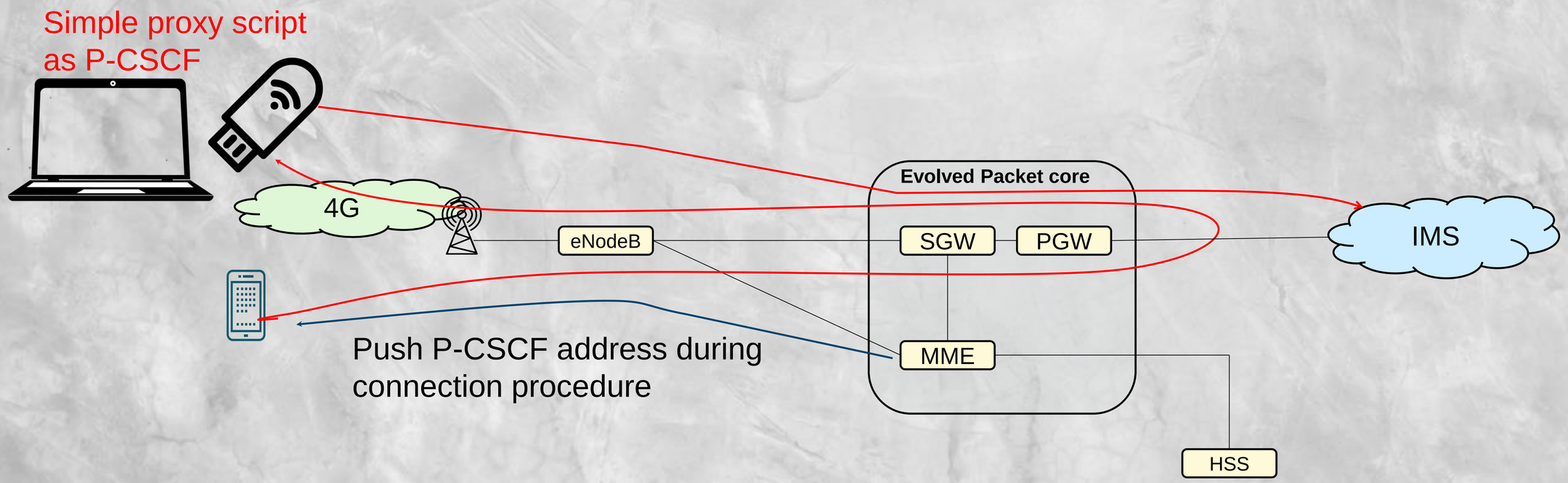
MiTM?

Simple proxy script
as P-CSCF

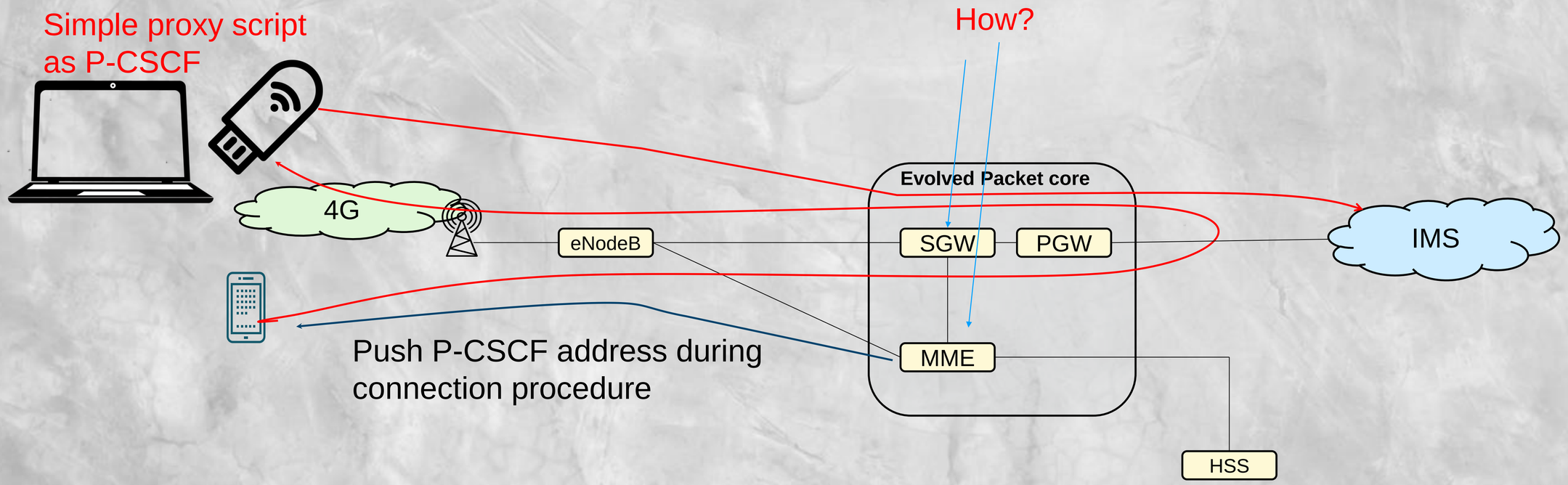


SecurityGen
Telecom Security. Transcending Generations.

Need to push P-CSCF address to the phone

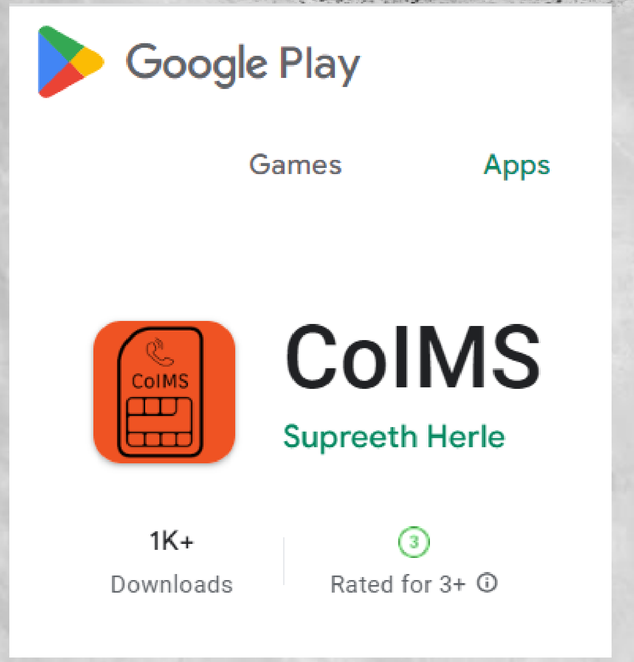


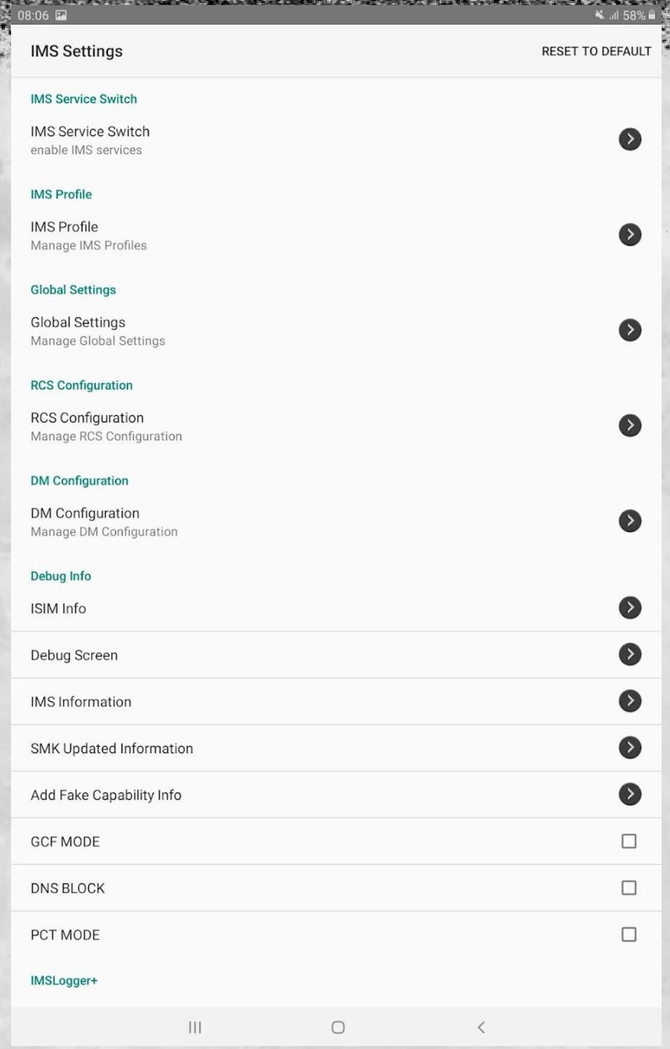
Need to push P-CSCF address to the phone



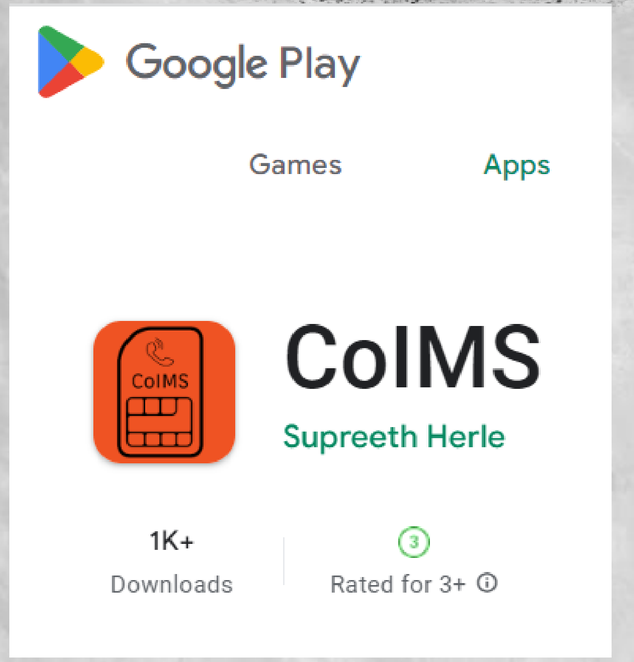
SecurityGen
Telecom Security. Transcending Generations.

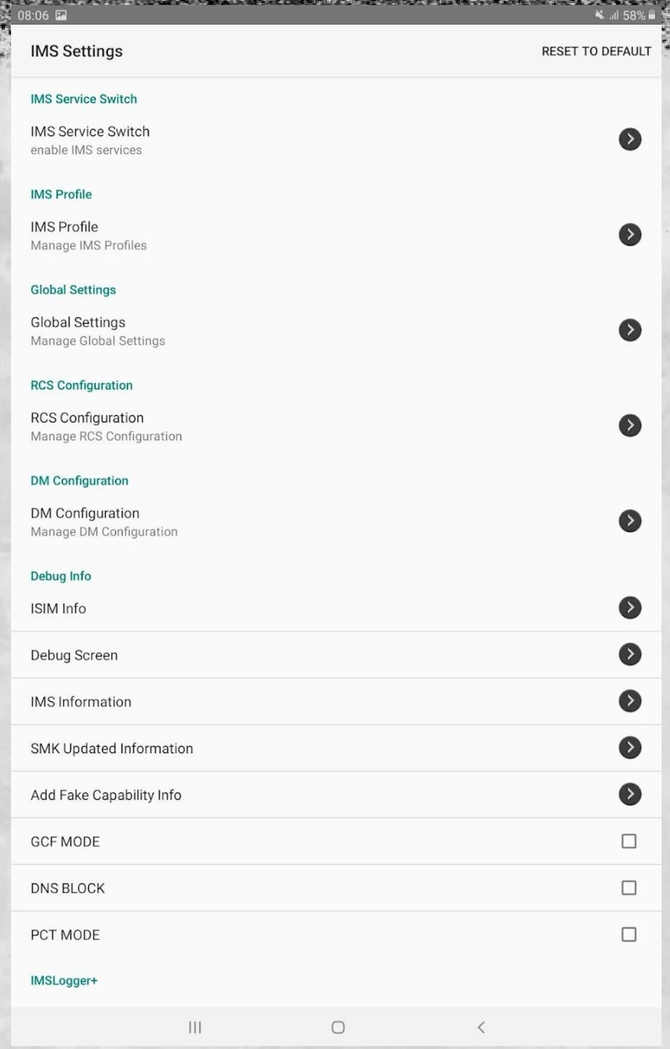
Decided to hack phone





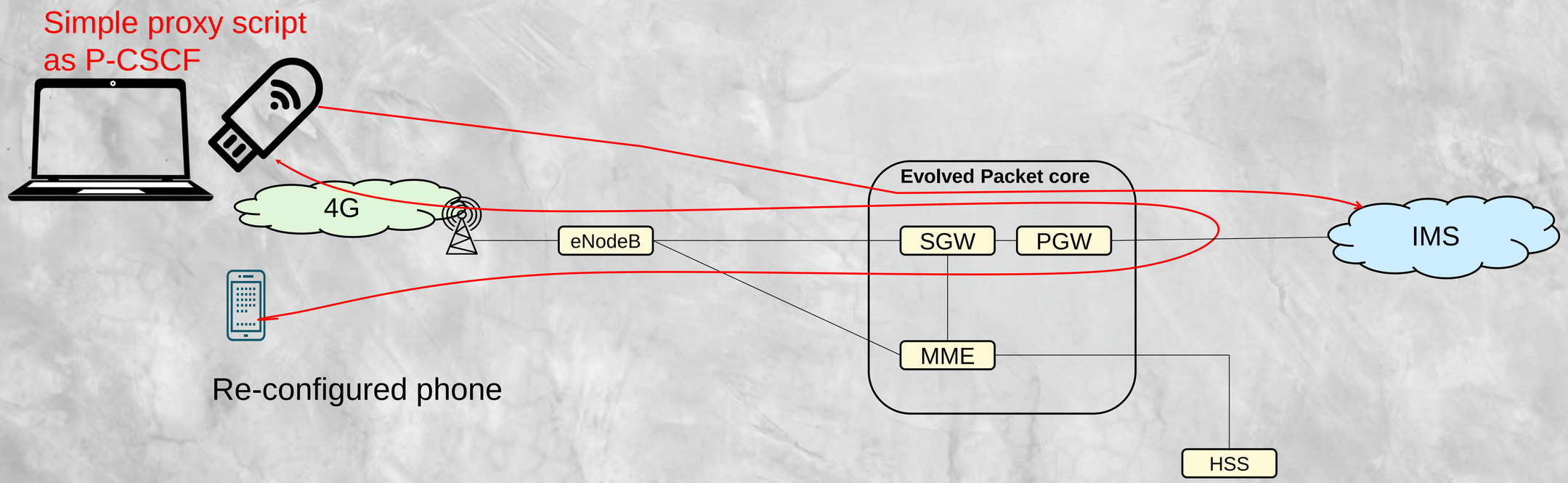
Decided to hack phone





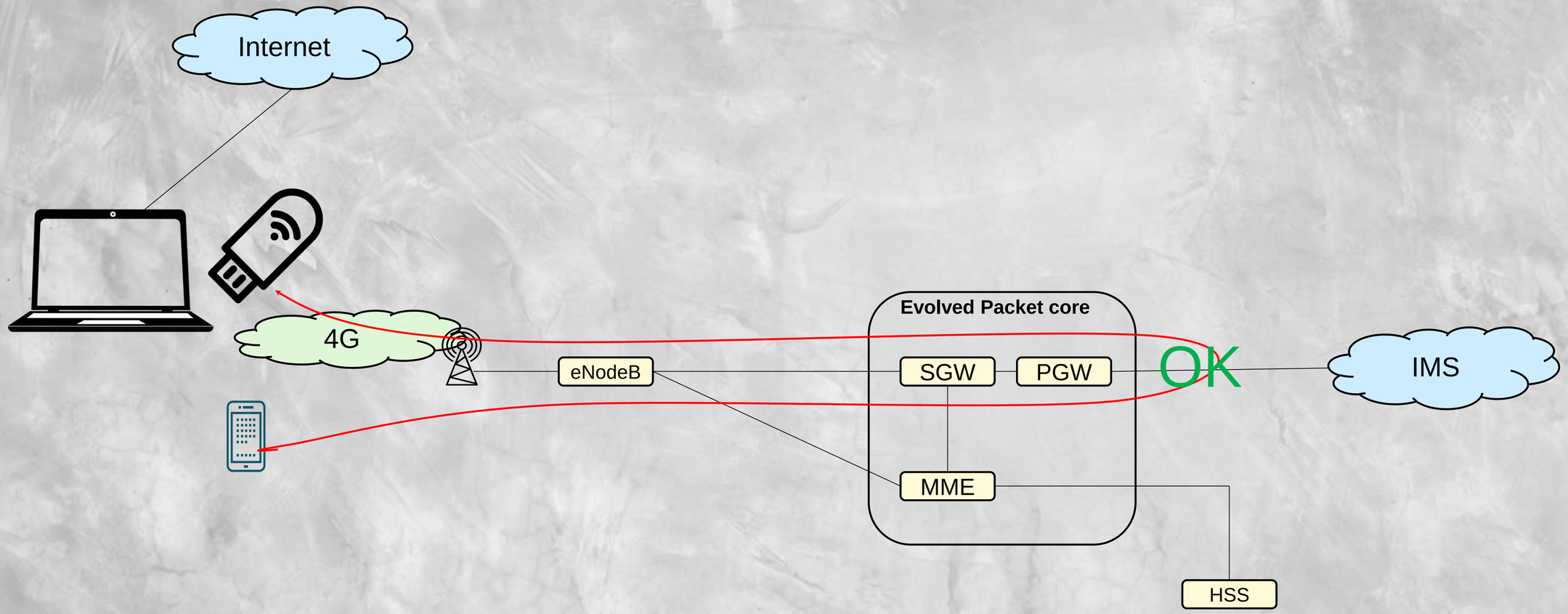
If it is not enough – “root” may help
Or editing “mbn” config on Qualcomm based devices

MiTM successful?



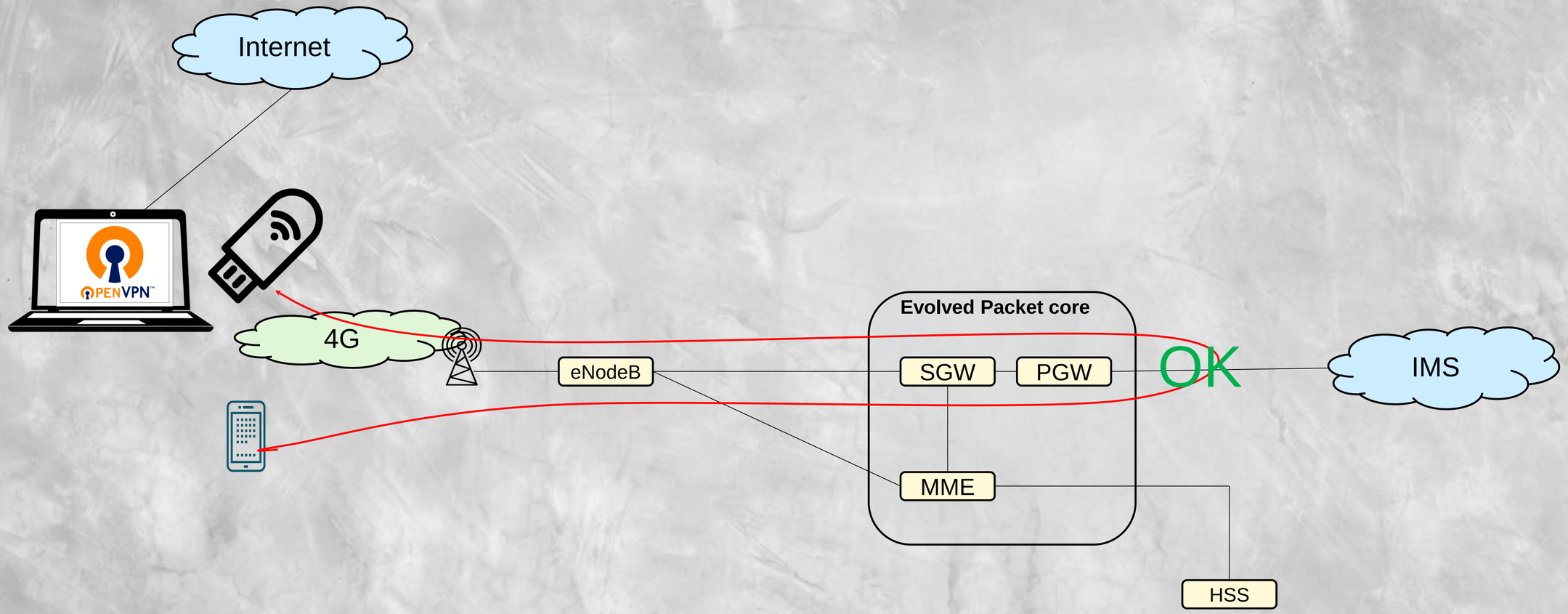
SecurityGen
Telecom Security. Transcending Generations.

Hijack VoLTE network



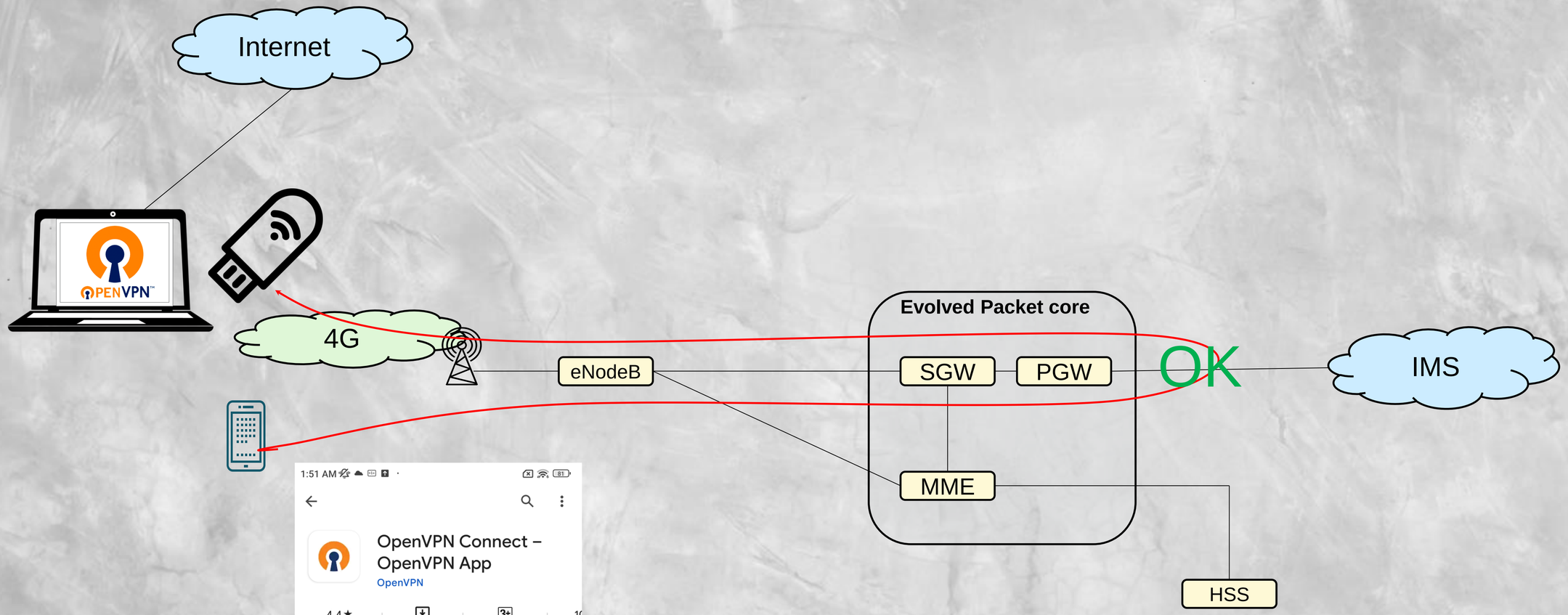
SecurityGen
Telecom Security. Transcending Generations.

Hijack VoLTE network



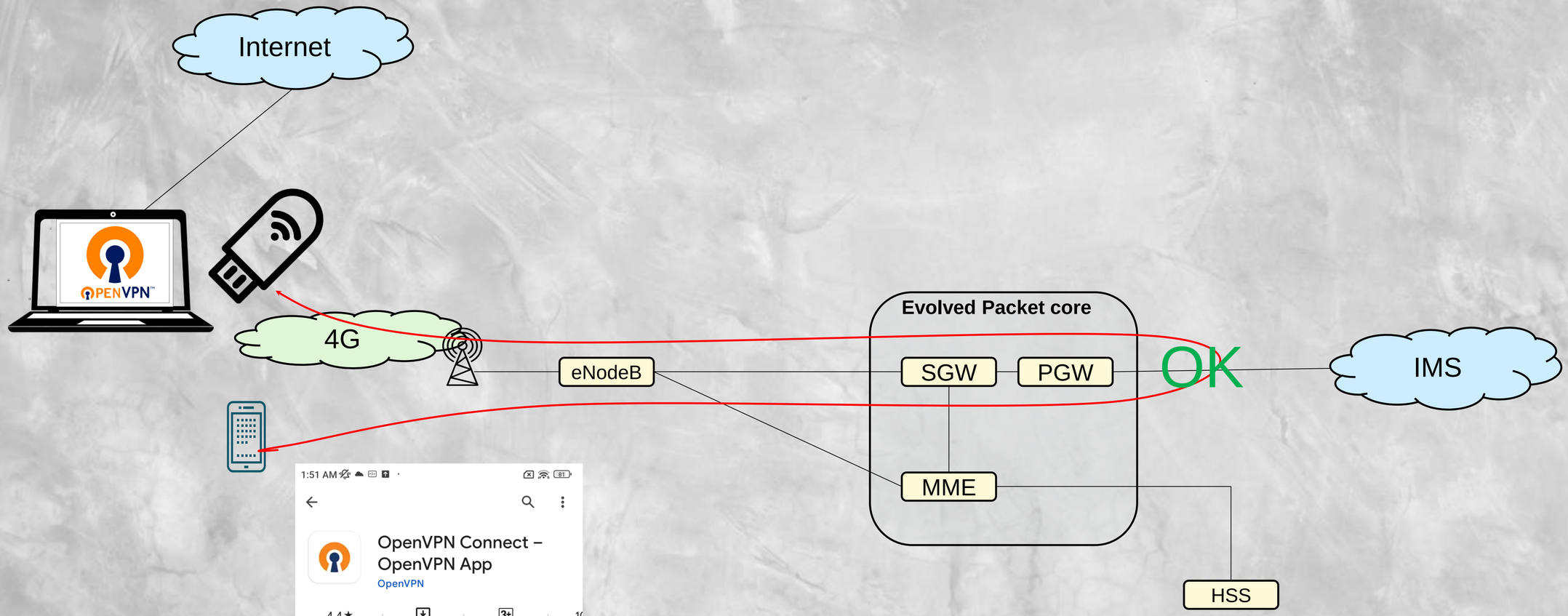
SecurityGen
Telecom Security. Transcending Generations.

Hijack VoLTE network



SecurityGen
Telecom Security. Transcending Generations.

Use internet for free



SecurityGen
Telecom Security. Transcending Generations.

Profit

1. Internet APN charging based on used amount of data, but IMS network charging based on minutes and implemented into IMS infrastructure
2. As we don’t use IMS infrastructure at all, data over IMS APN will not be charged
3. Due to lack of isolation we can establish direct subscriber-to-subscriber communication
4. We can set up OpenVPN tunnel to another subscriber and use his internet
5. Other kind of tunnels are also work, or even p2p networks
6. If network provides VoLTE roaming – then we can implement free internet in Roaming (leaving laptop in home network)

Mitigation for MNO

1. Turn on subscriber isolation, as it is usually done for Internet APN
2. Implement IMS network monitoring

Conclusion

1. Such misconfiguration (lack of subscriber isolation on ims APN) we see in more then 50% of tested network
2. Mobile operators are very big and slow, they were not interested in deploying IMS infrastructure for more then 10 years of LTE network. But now they are in hurry and deploying VoLTE network very fast and not secure.

Thank you!

Pavel Novikov
Pavel.Novikov@security-gen.com

SecurityGen
Telecom Security, Transcending Generations.