Locating Mobile Phones using Signalling System #7

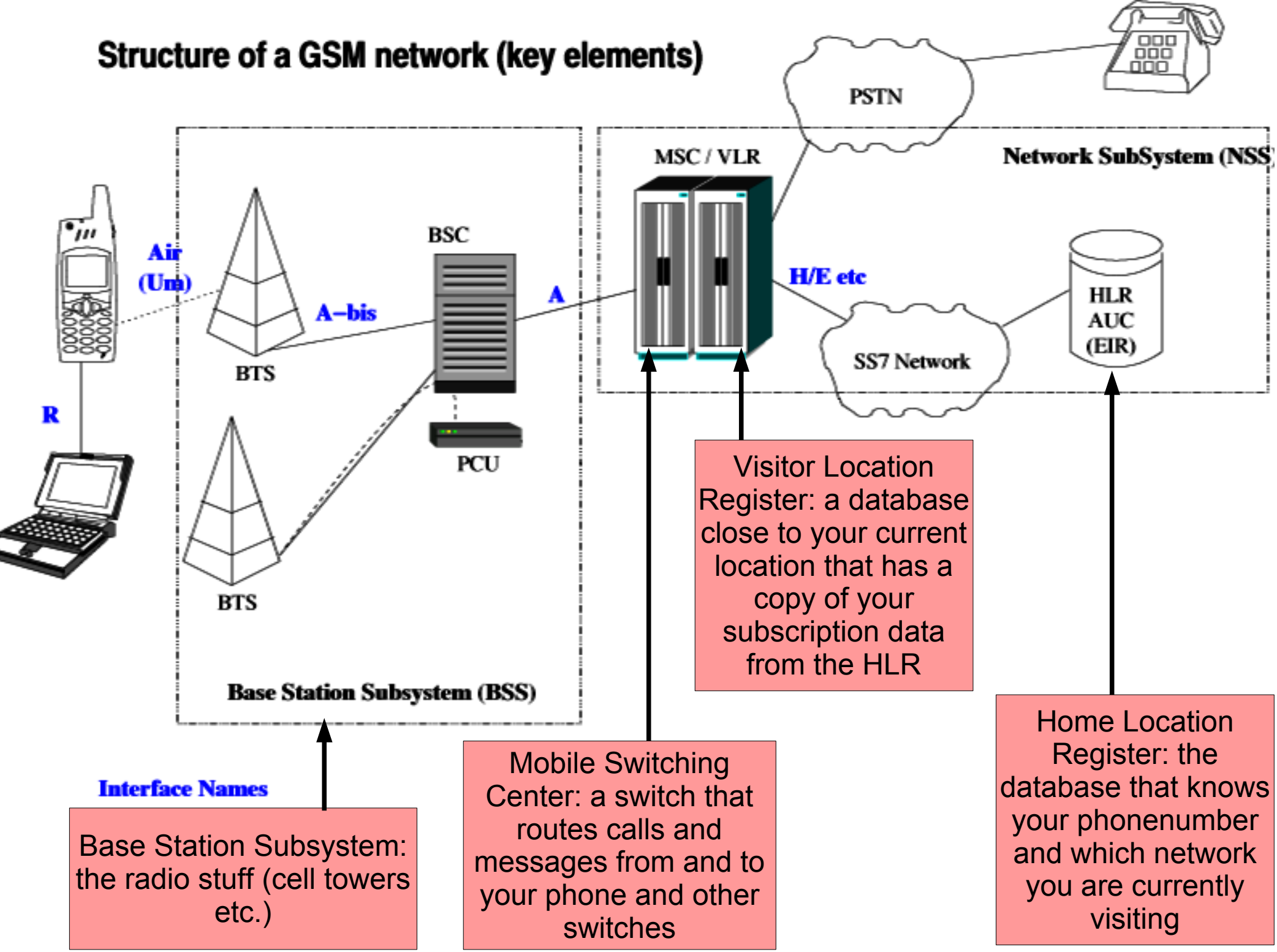
Tobias Engel <tobias@ccc.de>
twitter: @2b_as

What is Signalling System #7?

- protocol suite used by most telecommunications operators throughout the world to talk to each other
- standardized in ITU-T Q.700 series
- when it was designed, there were only few telecoms operators, and they were either state controlled or really big corporations
- trusted each other, so no authentication built in
- today, everybody can be an operator (e.g. VoIP), so SS7 access is easier to get

Mobile Application Part (MAP)

- part of SS7 that specifies additional signalling that is required for mobile phones to work (roaming, SMS, etc.)
- standardized in 3GPP TS 29.002
- in order for two network operators to talk MAP to each other they usually need a roaming agreement


Structure of a GSM network (key elements)
PSTN
MSC / VLR
Network SubSystem (NSS)
Air
(Um)
BSC
A
A–bis
H/E etc
HLR
AUC
(EIR)
SS7 Network
BTS
BTS
PCU
R
Base Station Subsystem (BSS)
Interface Names
Base Station Subsystem: the radio stuff (cell towers etc.)
Mobile Switching Center: a switch that routes calls and messages from and to your phone and other switches
Visitor Location Register: a database close to your current location that has a copy of your subscription data from the HLR
Home Location Register: the database that knows your phonenumber and which network you are currently visiting

What does the network know about your location?

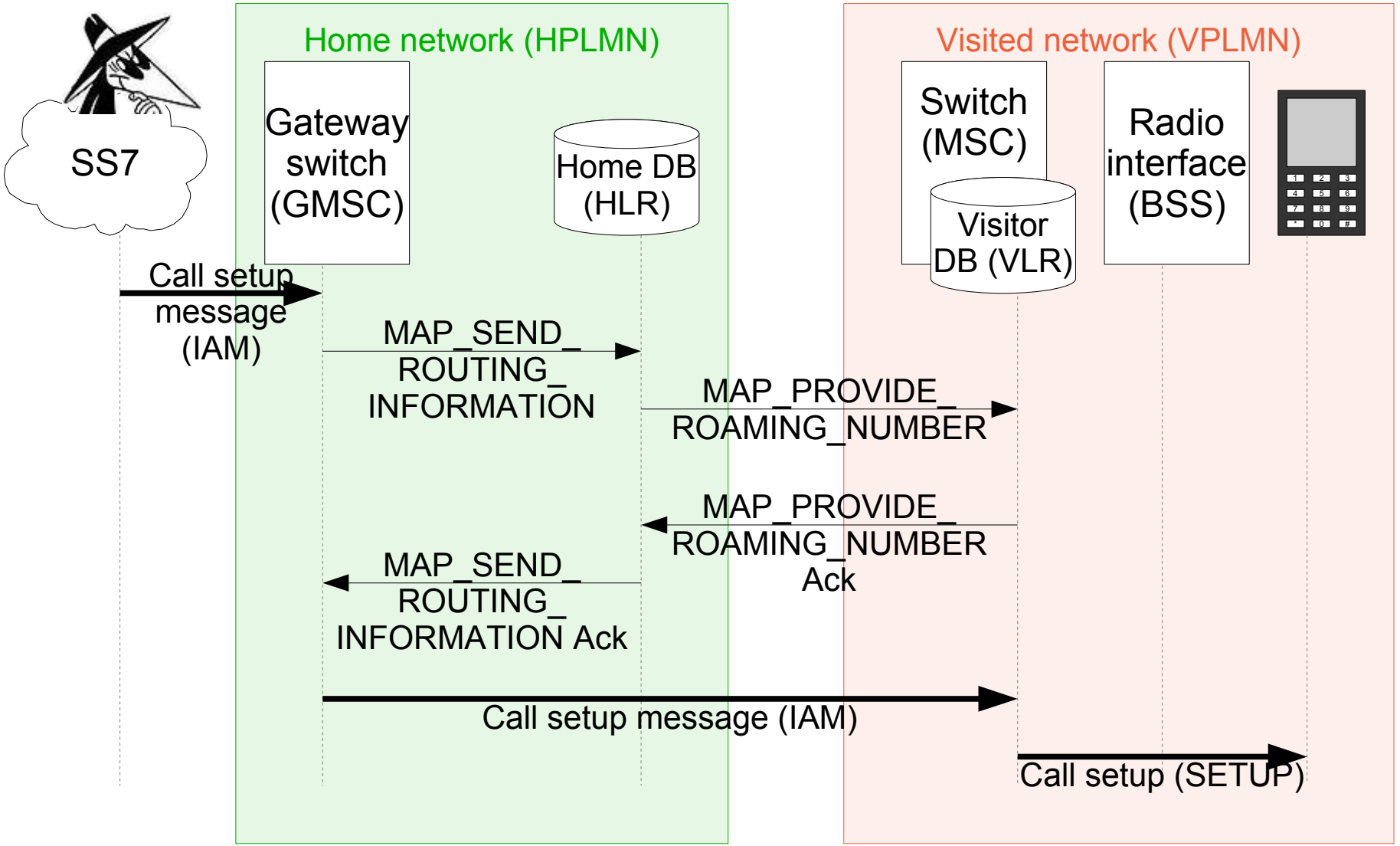
- the location of the cell tower is also a pretty good approximation of *your* location
- but that information is only known to the network you are currently logged into
- restricted to technical operation of the network - exceptions:
  - "Locate my phone" services
    - have to assure the operator that they have the consent of the phone's owner
    - doesn't work anymore as soon as you are logged into a network that is not your home network
  - Law enforcement
    - have to call the operator of the network you are currently logged into (*not* your home network operator)

Can somebody with SS7/MAP access find out your location?

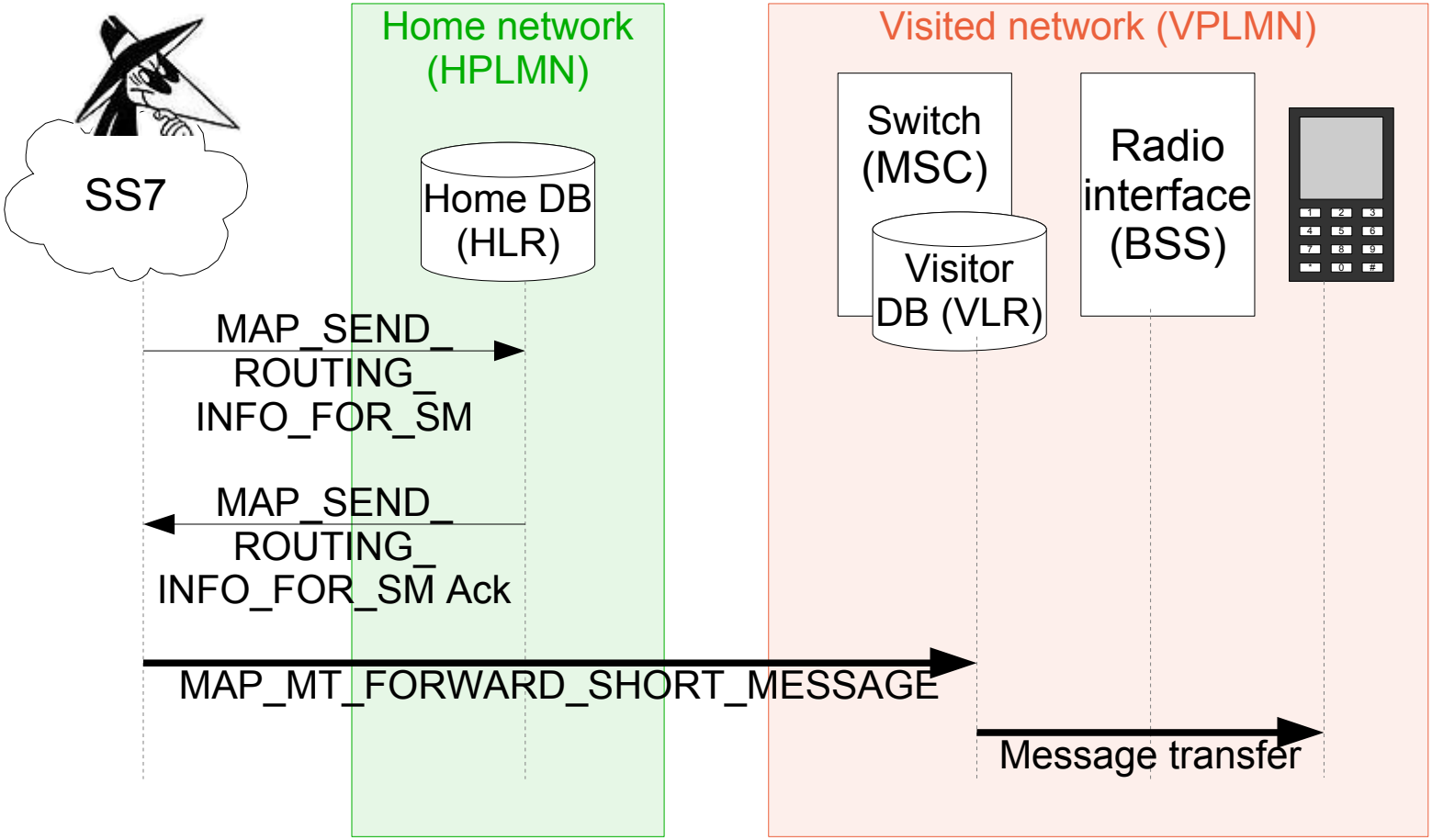
- services that can be initiated to your phone number from almost anywhere in the global SS7 network are
  - voice calls
  - short messages

Let's see if these services give any indication of your location...

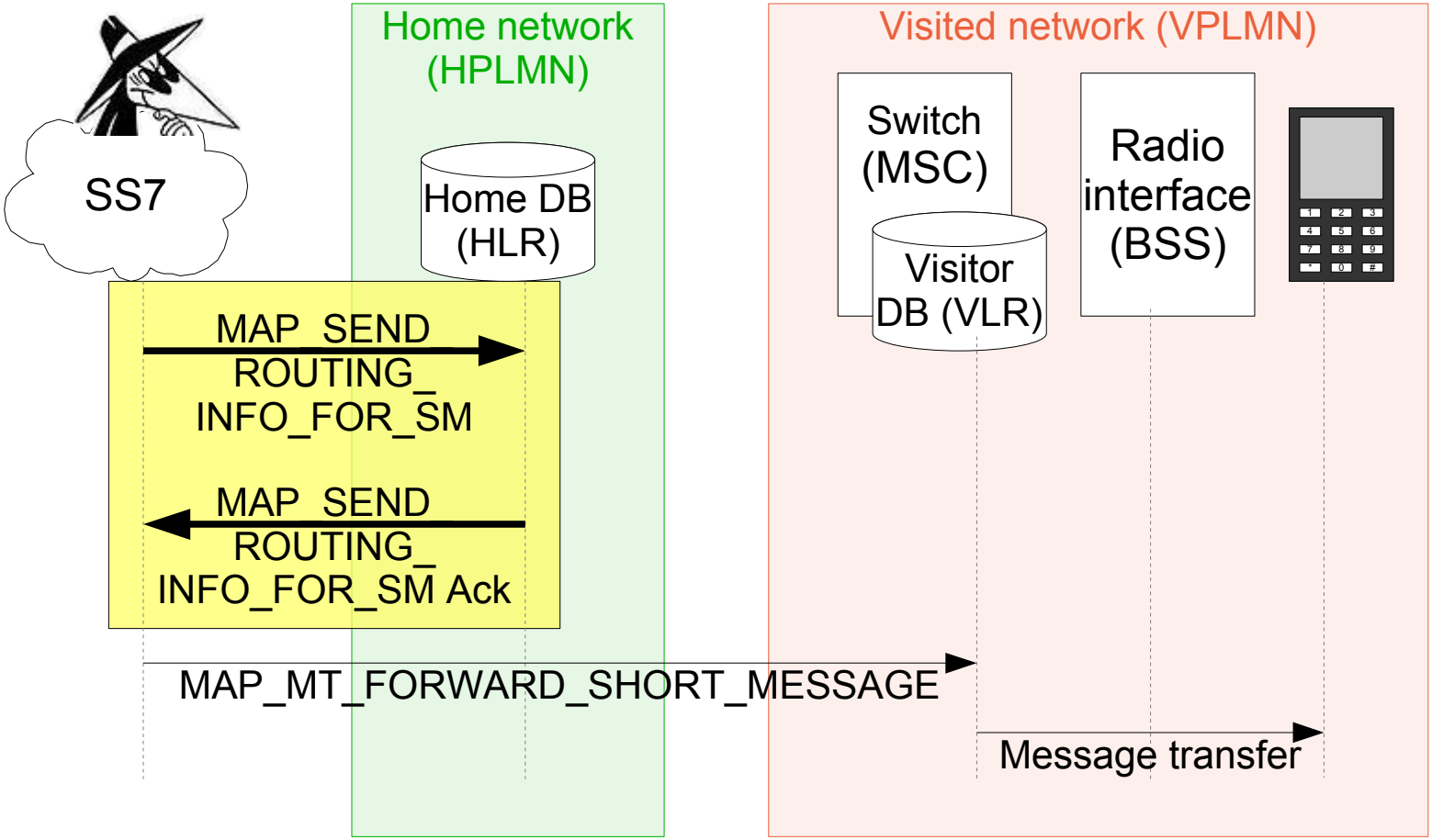
Call setup


SS7
Home network (HPLMN)
Gateway switch (GMSC)
Home DB (HLR)
Visited network (VPLMN)
Switch (MSC)
Visitor DB (VLR)
Radio interface (BSS)
Call setup message (IAM)
MAP_SEND_ ROUTING_ INFORMATION
MAP_PROVIDE_ ROAMING_NUMBER
MAP_PROVIDE_ ROAMING_NUMBER Ack
MAP_SEND_ ROUTING_ INFORMATION Ack
Call setup message (IAM)
Call setup (SETUP)

Sending a short message



Sending a short message



MAP-SEND-ROUTING-INFO-FOR-SM (3GPP TS 29.002)

- no correlation between requesting routing info for a message and actually sending a message
- SMS are sent directly from the SMSC of the sender to the MSC that you are currently using

- successful request returns:
  - your IMSI ("real" phone number)
  - global title of MSC you are using
  - user error (e.g. "Absent subscriber" == your phone is off)

Mobile Switching Center (MSC)

- handles calls and SMS
- can only handle a certain amount of calls, so in big cities there might be more than one MSC for each network, while in the countryside one MSC might serve a really large area
- global title of the MSC tells us which country you are currently in, because it starts with the country code
- maybe also the network, if mobile networks in that country can be identified by their area code
- other than that: numbering is operator internal

  ... but that doesn't mean that we cannot get further information from the number by looking at it long enough

MSC global title (examples)

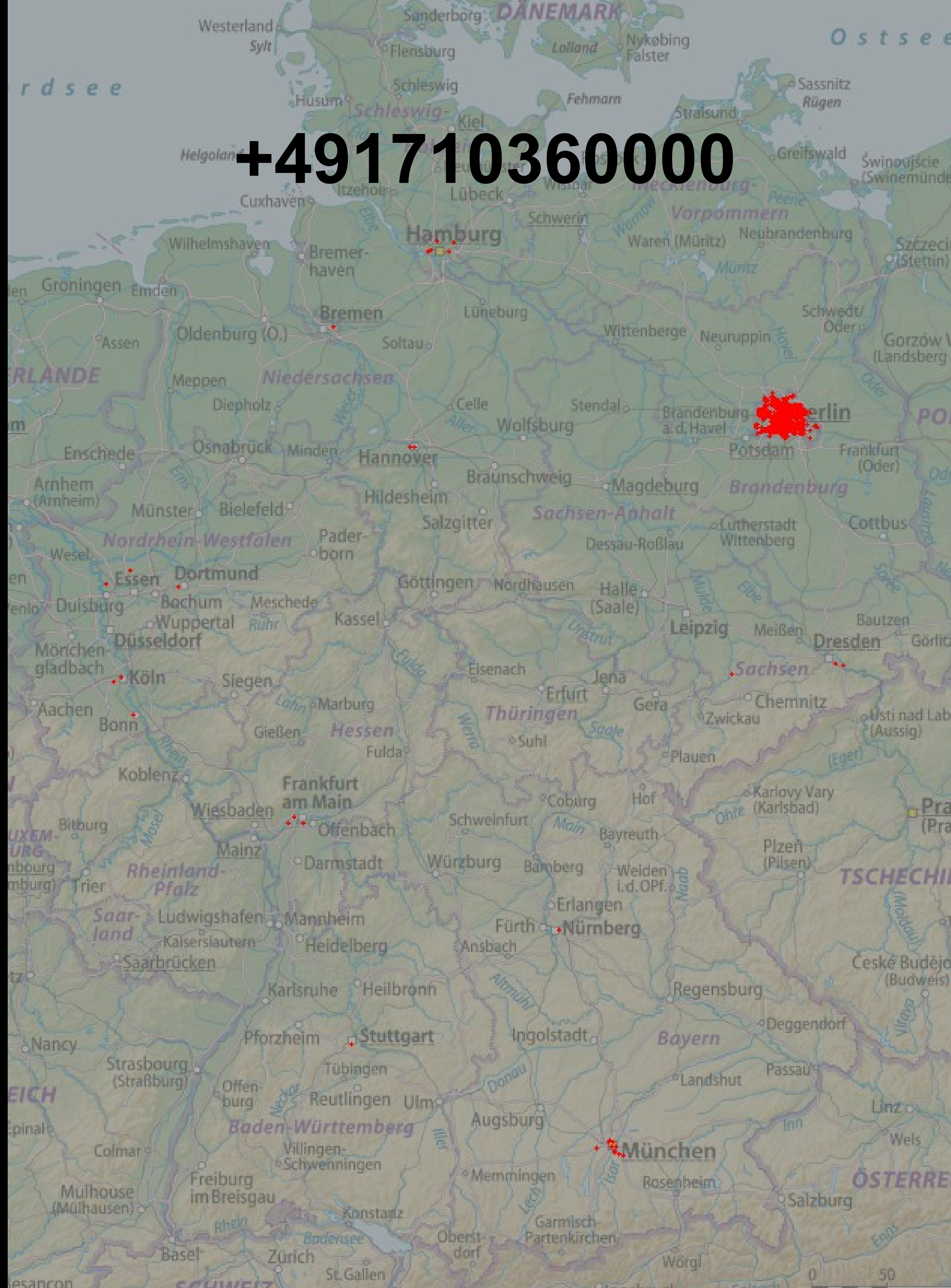
	T-Mobile Germany	Vodafone Germany
Berlin	+491710360000	+491720012097
Hamburg	+491710400000	+491720022097
Frankfurt	+491710650000	+491720061097
Stuttgart	+491710700000	+491720076097
München	+491710870000	+491720082097

MSC global title (examples)

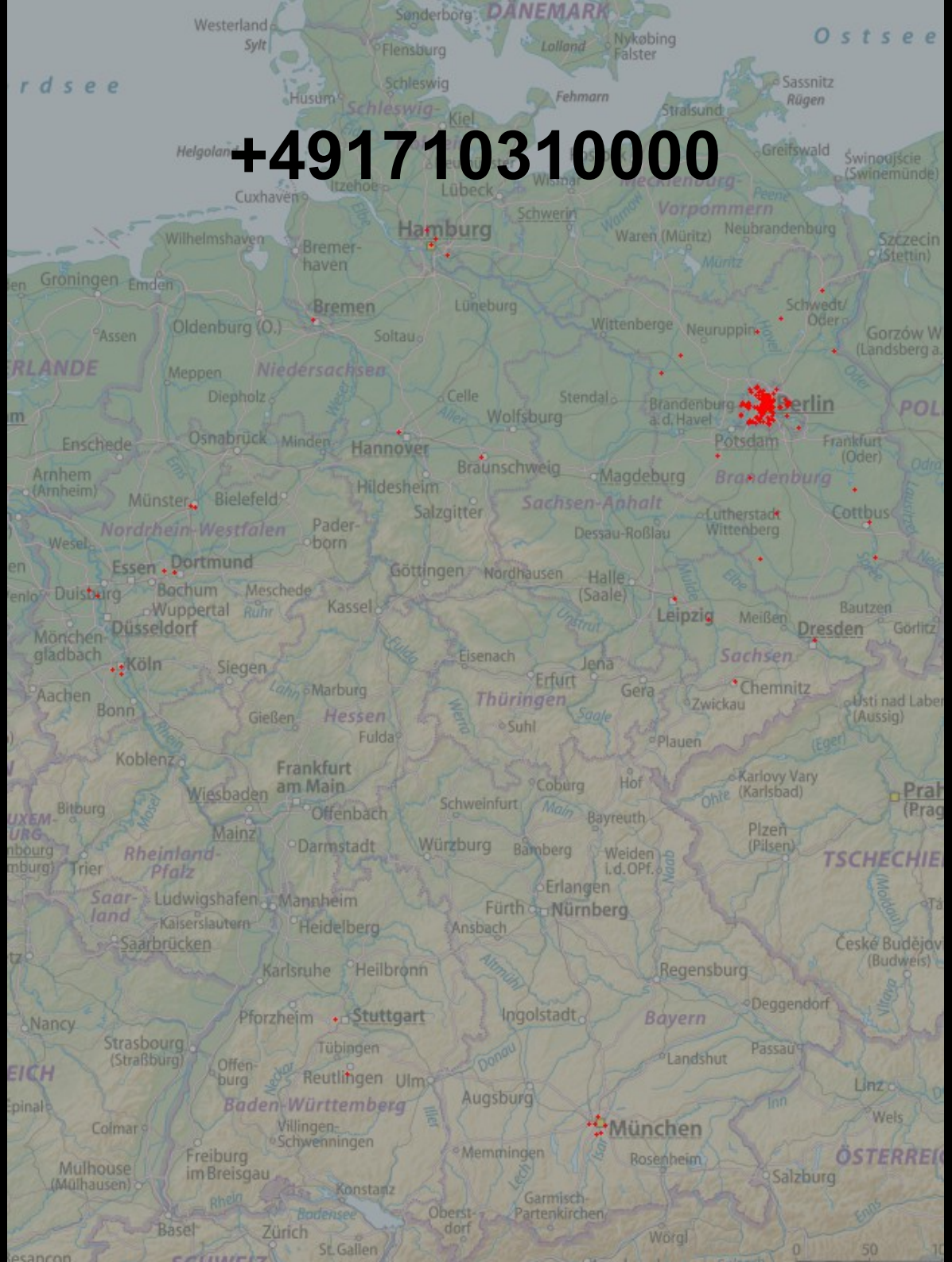
	T-Mobile Germany	Vodafone Germany
	First digit of area code	First digit of ZIP code
Berlin	+4917103600**0**0	+4917200**1**2097
Hamburg	+4917104000**0**0	+4917200**2**2097
Frankfurt	+4917106500**0**0	+4917200**6**1097
Stuttgart	+4917107000**0**0	+4917200**7**6097
München	+4917108700**0**0	+4917200**8**2097

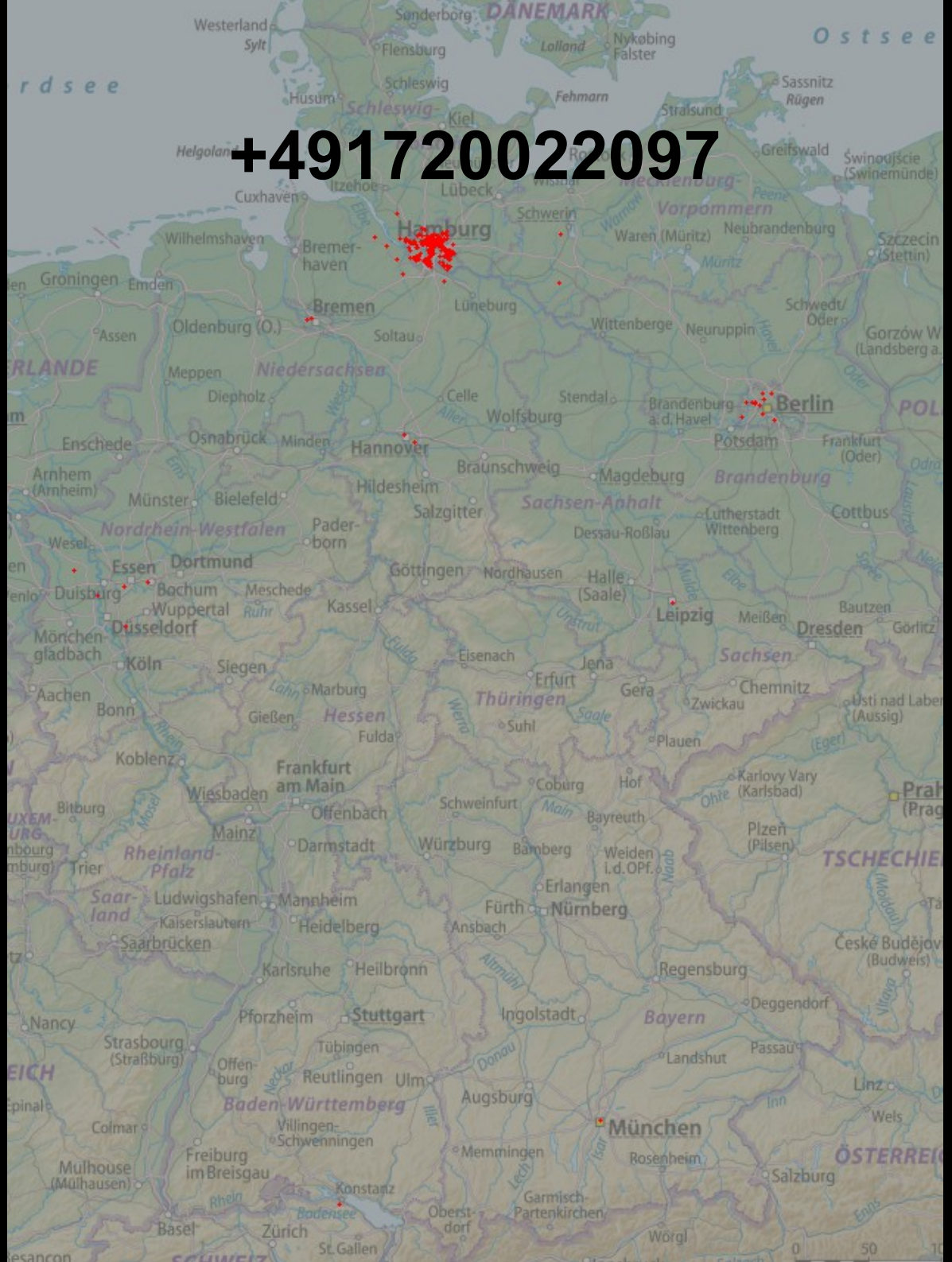
Automated approach to narrow down the area an MSC is serving (1/2)

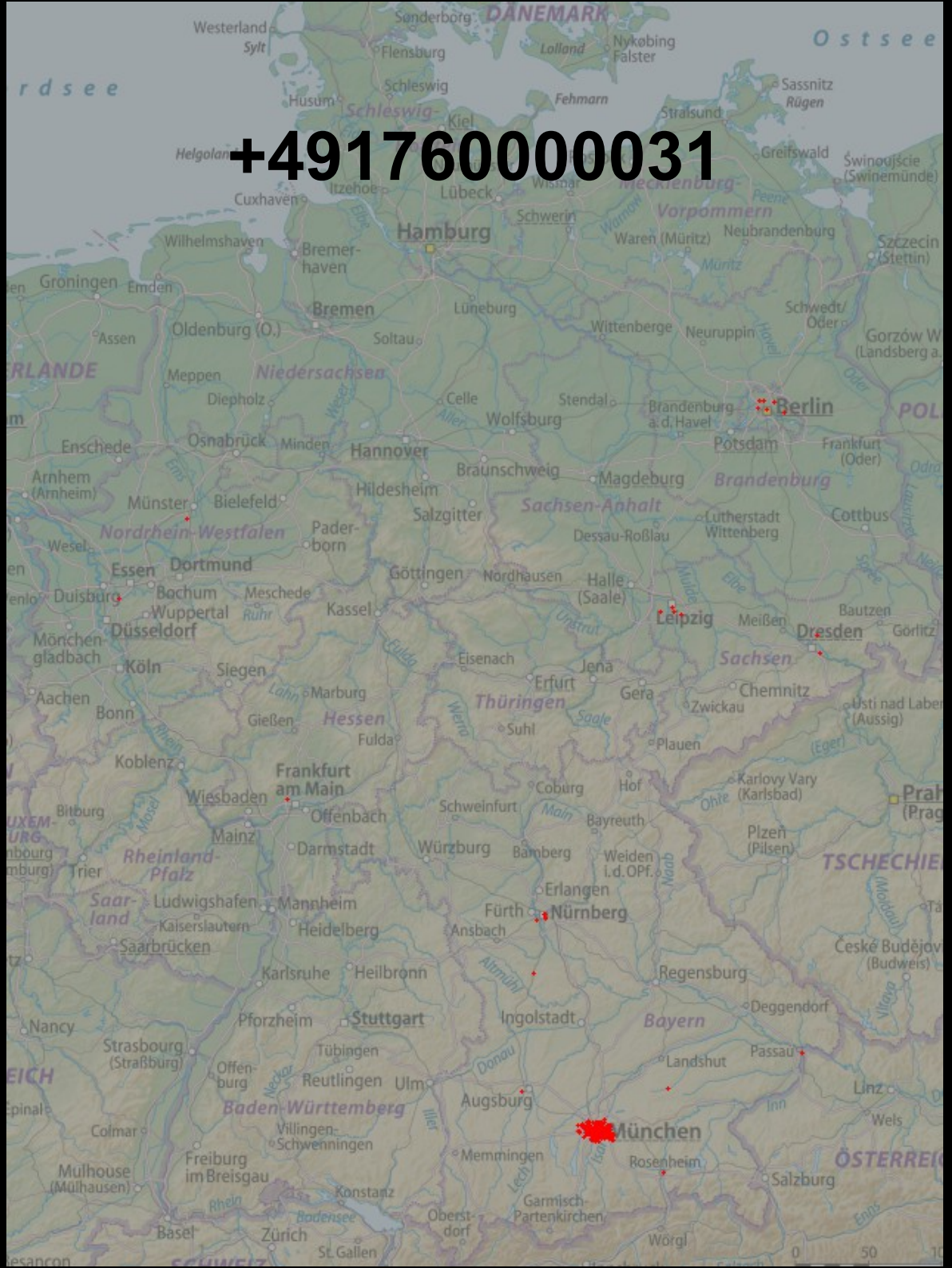
- Rop had a great idea: if we have a lot of mobile phone numbers and already know their location, we could query the network for the current MSC of these numbers, thus creating a MSC ↔ geolocation mapping
- thanks to erdgeist, we have a decoded copy of the "Das Telefonbuch" CD
- sent tens of thousands of MAP_SEND_ROUTING_INFO_FOR_SM requests for numbers from the phonebook
  - requests where done at night, when most people are at home
  - removed the obvious errors

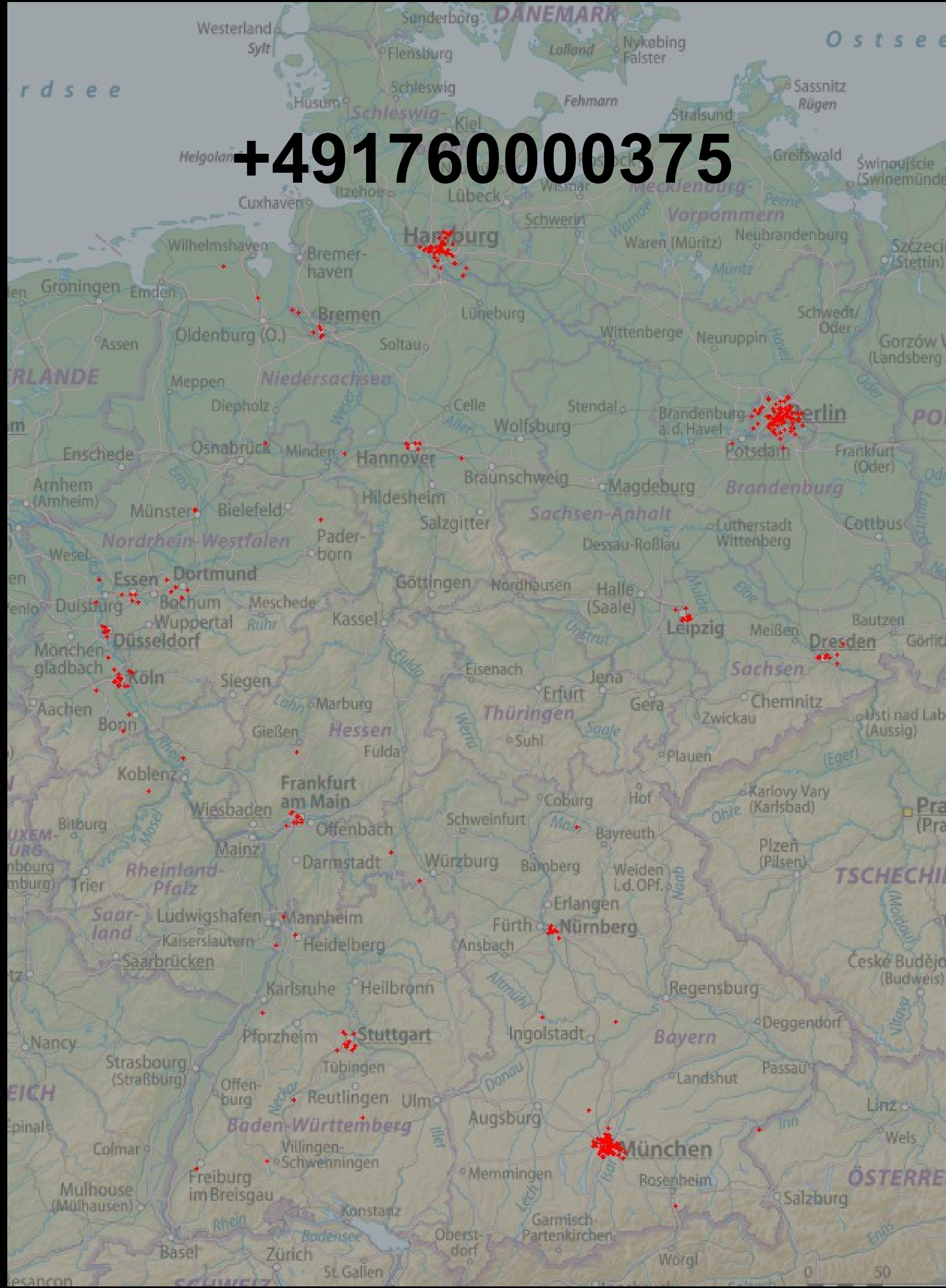


+491710360000
DÄNEMARK
Ostsee
Nordsee
Westerland
Sylt
Sønderborg
Flensburg
Schleswig
Husum
Kiel
Lolland
Nykøbing Falster
Fehmarn
Sassnitz
Rügen
Stralsund
Greifswald
Świnoujście (Swinemünde)
Helgoland
Itzehoe
Lübeck
Wismar
Mecklenburg-Vorpommern
Cuxhaven
Schwerin
Hamburg
Wilhelmshaven
Bremerhaven
Waren (Müritz)
Neubrandenburg
Szczecin (Stettin)
Groningen
Emden
Bremen
Lüneburg
Oldenburg (O.)
Assen
Soltau
Wittenberge
Neuruppin
Schwedt/Oder
Gorzów W (Landsberg a.
Meppen
Niedersachsen
Diepholz
Celle
Stendal
Brandenburg a.d. Havel
Berlin
Wolfsburg
Enschede
Osnabrück
Minden
Hannover
Potsdam
Frankfurt (Oder)
Braunschweig
Magdeburg
Brandenburg
Arnhem (Arnheim)
Hildesheim
Münster
Bielefeld
Salzgitter
Sachsen-Anhalt
Cottbus
Nordrhein-Westfalen
Paderborn
Lutherstadt Wittenberg
Dessau-Roßlau
Wesel
Essen
Dortmund
Göttingen
Nordhausen
Halle (Saale)
Duisburg
Bochum
Meschede
Wuppertal
Kassel
Leipzig
Meißen
Bautzen
Dresden
Görlitz
Mönchengladbach
Düsseldorf
Köln
Eisenach
Jena
Sachsen
Siegen
Erfurt
Gera
Chemnitz
Aachen
Marburg
Thüringen
Zwickau
Bonn
Gießen
Hessen
Suhl
Fulda
Plauen
Koblenz
Frankfurt am Main
Coburg
Hof
Karlovy Vary (Karlsbad)
Wiesbaden
Schweinfurt
Bayreuth
Bitburg
Offenbach
Mainz
Darmstadt
Würzburg
Bamberg
Weiden i.d.OPf.
Plzeň (Plzen)
Rheinland-Pfalz
Trier
Erlangen
Saarland
Ludwigshafen
Mannheim
Fürth
Nürnberg
Kaiserslautern
Heidelberg
Ansbach
Saarbrücken
Karlsruhe
Heilbronn
Regensburg
České Budějovice (Budweis)
Nancy
Pforzheim
Stuttgart
Ingolstadt
Bayern
Deggendorf
Strasbourg (Straßburg)
Tübingen
Offenburg
Reutlingen
Ulm
Landshut
Passau
Baden-Württemberg
Augsburg
Linz
Colmar
Villingen-Schwenningen
München
Wels
Freiburg im Breisgau
Memmingen
Rosenheim
Salzburg
Mulhouse (Mülhausen)
Konstanz
Bodensee
Garmisch-Partenkirchen
Basel
Zürich
Oberstdorf
Wörgl
St. Gallen
ÖSTERREICH
TSCHECHIEN


+491710310000
Berlin
Hamburg
München
Hannover
Bremen
Dortmund
Essen
Köln
Düsseldorf
Frankfurt am Main
Stuttgart
Nürnberg
Leipzig
Dresden
Niedersachsen
Nordrhein-Westfalen
Sachsen-Anhalt
Brandenburg
Sachsen
Thüringen
Hessen
Rheinland-Pfalz
Baden-Württemberg
Bayern
Mecklenburg-Vorpommern
DÄNEMARK
Ostsee
Nordsee


+491720022097
Hamburg
Berlin
Bremen
Hannover
Dortmund
Essen
Duisburg
Bochum
Wuppertal
Düsseldorf
Köln
Frankfurt am Main
Stuttgart
München
Nürnberg
Leipzig
Dresden
Niedersachsen
Nordrhein-Westfalen
Hessen
Thüringen
Sachsen
Sachsen-Anhalt
Brandenburg
Mecklenburg-Vorpommern
Rheinland-Pfalz
Saarland
Baden-Württemberg
Bayern
Schleswig-Holstein
DÄNEMARK
TSCHECHIEN
ÖSTERREICH


+491760000031
Westerland
Sylt
Sønderborg
DÄNEMARK
Flensburg
Lolland
Nykøbing
Falster
Ostsee
Schleswig
Husum
Fehmarn
Sassnitz
Rügen
Stralsund
Kiel
Helgoland
Greifswald
Świnoujście
(Swinemünde)
Cuxhaven
Itzehoe
Lübeck
Mecklenburg-
Vorpommern
Schwerin
Hamburg
Wismar
Warnow
Peene
Waren (Müritz)
Neubrandenburg
Szczecin
(Stettin)
Müritz
Wilhelmshaven
Bremer-
haven
Groningen
Emden
Bremen
Lüneburg
Schwedt/
Oder
Oldenburg (O.)
Soltau
Wittenberge
Neuruppin
Gorzów W
(Landsberg a.
Assen
Meppen
Niedersachsen
Diepholz
Celle
Stendal
Berlin
Wolfsburg
Brandenburg
a. d. Havel
Potsdam
Frankfurt
(Oder)
Enschede
Osnabrück
Minden
Hannover
Braunschweig
Magdeburg
Brandenburg
Arnhem
(Arnhem)
Hildesheim
Münster
Bielefeld
Salzgitter
Sachsen-Anhalt
Lutherstadt
Wittenberg
Cottbus
Dessau-Roßlau
Nordrhein-Westfalen
Pader-
born
Wesel
Essen
Dortmund
Göttingen
Nordhausen
Halle
(Saale)
Duisburg
Bochum
Meschede
Kassel
Leipzig
Meißen
Bautzen
Wuppertal
Ruhr
Unstrut
Dresden
Görlitz
Mönchen-
gladbach
Düsseldorf
Eisenach
Jena
Sachsen
Köln
Siegen
Erfurt
Gera
Chemnitz
Aachen
Marburg
Thüringen
Zwickau
Bonn
Gießen
Hessen
Suhl
Fulda
Plauen
Koblenz
Frankfurt
am Main
Coburg
Hof
Karlovy Vary
(Karlsbad)
Wiesbaden
Schweinfurt
Bayreuth
Bitburg
Offenbach
Mainz
Darmstadt
Würzburg
Bamberg
Weiden
i. d. OPf.
Plzeň
(Pilsen)
Trier
Rheinland-
Pfalz
Erlangen
Saar-
land
Ludwigshafen
Mannheim
Fürth
Nürnberg
Kaiserslautern
Heidelberg
Ansbach
Saarbrücken
České Budějovice
(Budweis)
Karlsruhe
Heilbronn
Regensburg
Deggendorf
Nancy
Pforzheim
Stuttgart
Ingolstadt
Bayern
Strasbourg
(Straßburg)
Tübingen
Passau
Landshut
Offen-
burg
Reutlingen
Ulm
Linz
Augsburg
Baden-Württemberg
Wels
Colmar
München
Villingen-
Schwenningen
Memmingen
Rosenheim
Freiburg
im Breisgau
Salzburg
Mulhouse
(Mülhausen)
Konstanz
Garmisch-
Partenkirchen
Basel
Zürich
Oberst-
dorf
Wörgl
St. Gallen
0
50


+4917600000375
DÄNEMARK
Ostsee
Nordsee
Westerland
Sylt
Sønderborg
Flensburg
Lolland
Nykøbing Falster
Sassnitz
Rügen
Schleswig
Husum
Fehmarn
Schleswig-
Kiel
Stralsund
Helgoland
Greifswald
Świnoujście (Swinemünde)
Itzehoe
Lübeck
Wismar
Mecklenburg-
Vorpommern
Cuxhaven
Schwerin
Hamburg
Wilhelmshaven
Bremerhaven
Waren (Müritz)
Neubrandenburg
Szczecin (Stettin)
Groningen
Emden
Bremen
Lüneburg
Schwedt/Oder
Oldenburg (O.)
Assen
Soltau
Wittenberge
Neuruppin
Gorzów W (Landsberg a.
NIEDERLANDE
Meppen
Niedersachsen
Diepholz
Celle
Stendal
Brandenburg a.d. Havel
Berlin
Wolfsburg
Enschede
Osnabrück
Minden
Hannover
Potsdam
Frankfurt (Oder)
Braunschweig
Magdeburg
Brandenburg
Arnhem (Arnheim)
Hildesheim
Münster
Bielefeld
Salzgitter
Sachsen-Anhalt
Lutherstadt Wittenberg
Cottbus
Nordrhein-Westfalen
Paderborn
Dessau-Roßlau
Wesel
Essen
Dortmund
Göttingen
Nordhausen
Halle (Saale)
Duisburg
Bochum
Meschede
Wuppertal
Kassel
Leipzig
Bautzen
Meißen
Mönchengladbach
Düsseldorf
Dresden
Görlitz
Eisenach
Sachsen
Köln
Siegen
Erfurt
Jena
Chemnitz
Aachen
Marburg
Gera
Thüringen
Zwickau
Ústí nad Labem (Aussig)
Bonn
Gießen
Hessen
Suhl
Fulda
Plauen
Koblenz
Frankfurt am Main
Coburg
Hof
Karlovy Vary (Karlsbad)
Wiesbaden
Praha (Prag)
Bitburg
Offenbach
Schweinfurt
Bayreuth
Mainz
Plzeň (Pilsen)
Rheinland-Pfalz
Darmstadt
Würzburg
Bamberg
Weiden i.d.OPf.
Trier
TSCHECHIEN
Erlangen
Saarland
Ludwigshafen
Mannheim
Fürth
Nürnberg
Kaiserslautern
Heidelberg
Ansbach
Saarbrücken
České Budějovice (Budweis)
Karlsruhe
Heilbronn
Regensburg
Deggendorf
Nancy
Pforzheim
Stuttgart
Ingolstadt
Bayern
Strasbourg (Straßburg)
Tübingen
Landshut
Passau
Offenburg
Reutlingen
Ulm
Augsburg
Linz
Baden-Württemberg
Épinal
Villingen-Schwenningen
München
Wels
Colmar
Memmingen
Freiburg im Breisgau
Rosenheim
ÖSTERREICH
Mulhouse (Mülhausen)
Salzburg
Konstanz
Garmisch-Partenkirchen
Bodensee
Oberstdorf
Basel
Zürich
Wörgl
St. Gallen
Besançon
SCHWEIZ

Automated approach to narrow down the area an MSC is serving (2/2)

- big thanks to itsme, who created such a mapping for the Netherlands

- other countries also possible if there are phone books available

"No one I know is a network operator - so I can be pretty sure that no one who would care finds out my location, right?"

- wrong: there are several companies offering a lookup service where you send them an MSISDN, they perform a MAP-SEND-ROUTING-INFO-FOR-SM request and send the IMSI and MSC they receive from the HLR back to you

- cost per request is in the low single euro cent area

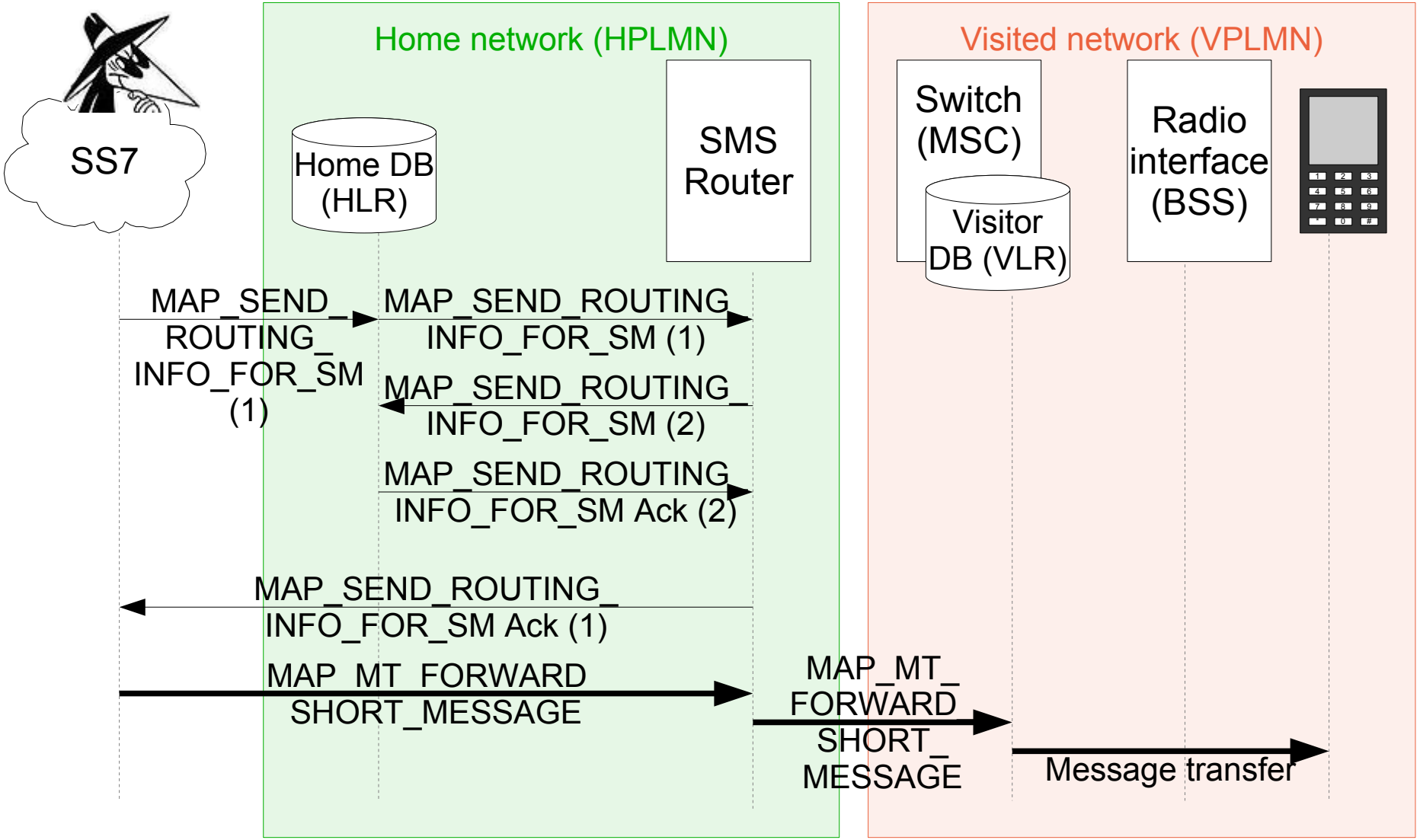
What is the business case for selling this service?

- Evil_Spammer wants to send spam SMS without paying
- he has SS7 access, and can also send MAP requests, but of course he has no roaming agreements with any other operators, so they don't answer his requests
- but: sending a message via MAP_MT_FORWARD_SHORT_MESSAGE does not even require an answer!
- Evil_Spammer just needs to know, to which MSC the message should be sent, so he uses one of these services...
- then he sets the sender address of the SMS request to that of another networks short message center
- the receiving network bills the SMS to that other network → free spam SMS!

I don't want to be located - what can I do? (1/2)

- SMS "home routing" (3GPP TR 23.840) will fix the problem
  - all messages to your phone are routed to an SMS router in your home network
  - that router will then deliver the message to your phone
  - MAP-SEND-ROUTING-INFO-FOR-SM only returns the ISDN number of the SMS router
  - instead of the IMSI, a random "correlation id" will be returned
  - operators will implement this to
    - prevent fraud
    - enable "VAS"
    - enable "lawful interception" of SMS sent to you when you are in another country

SMS "home routing" (3GPP TR 23.840)



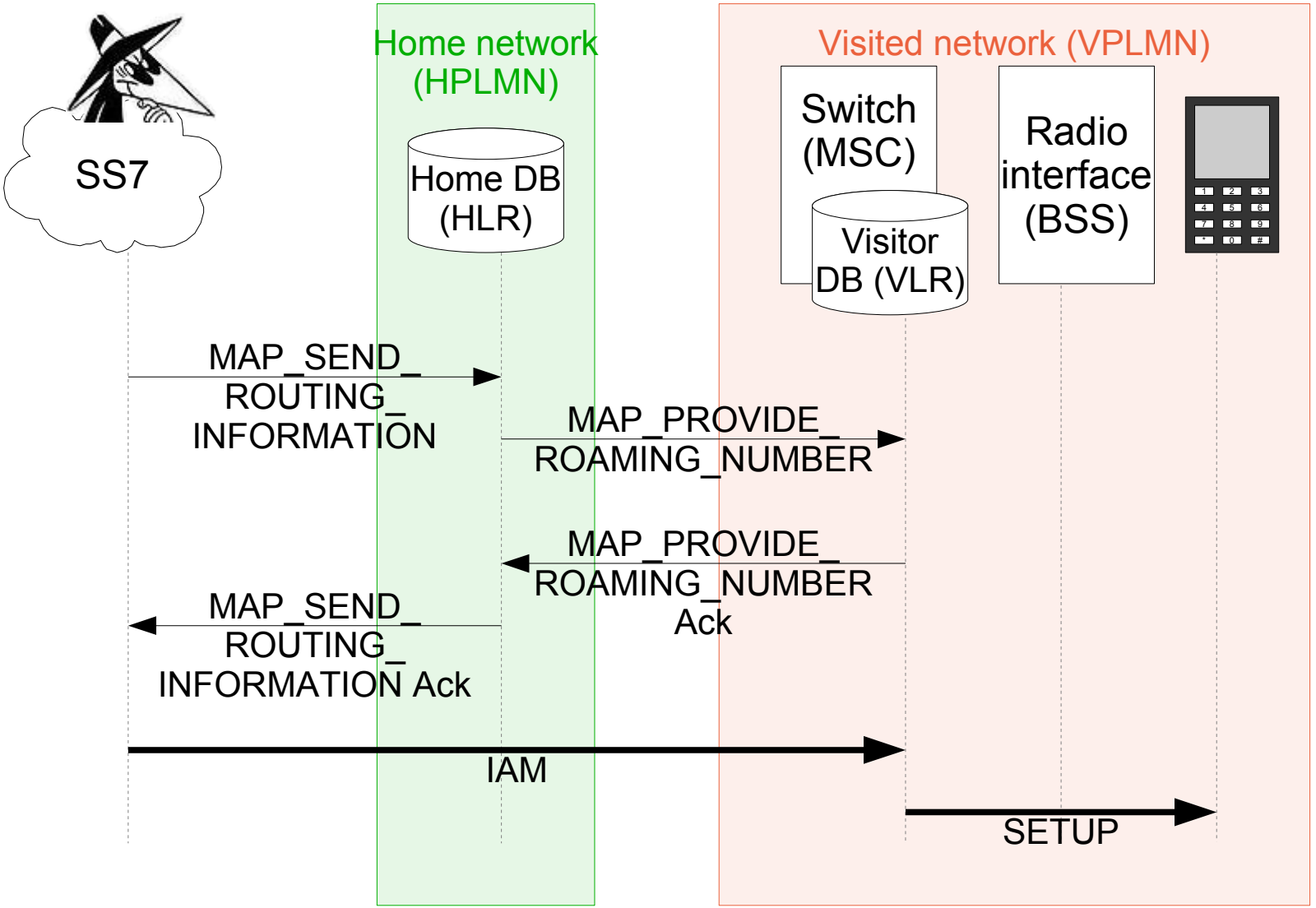
I don't want to be located - what can I do? (2/2)

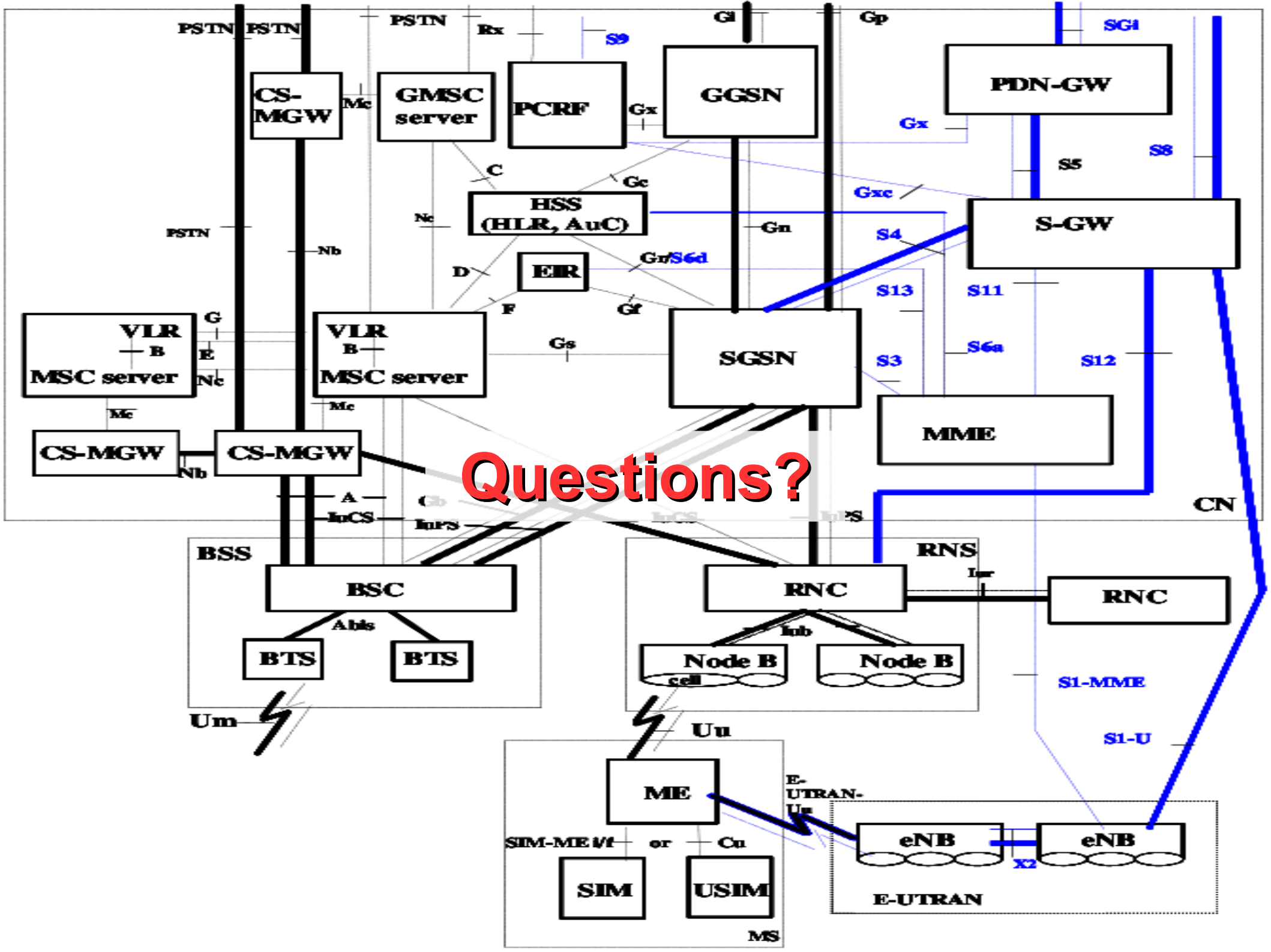
- until home routing is in use:
  - some networks offer multiple SIMs for one phone number and use an SMS router to decide which SIM will receive the SMS (e.g. o2 Germany)
  - let your operator block incoming SMS for your phone number
  - switch your phone off

What's next: Optimal routeing

- Specified in 3GPP TS 23.079
- makes it possible to route calls directly to the network you are currently logged into
- this can only work if the entity that sets up the call has a way of finding out, which MSC you are currently using...
- OR is currently not widely in use
- charging issues have to be worked out

Call setup with Optimal Routeing




PSTN
PSTN
PSTN
Rx
S9
Gi
Gp
SGi
CS-MGW
Mc
GMSC server
PCRF
Gx
GGSN
PDN-GW
Gx
S5
S8
C
Gc
Gxc
HSS (HLR, AuC)
Nc
Gn
S-GW
S4
PSTN
Nb
D
EIR
Gr/S6d
S13
S11
F
Gf
VLR
B
MSC server
G
E
Nc
VLR
B
MSC server
Gs
SGSN
S3
S6a
S12
Mc
Mc
MME
CS-MGW
Nb
CS-MGW
Questions?
A
Gb
IuCS
IuPS
CN
BSS
BSC
RNS
RNC
Iur
RNC
Abis
Iub
BTS
BTS
Node B
cell
Node B
S1-MME
Um
Uu
S1-U
ME
E-UTRAN-Uu
SIM-ME I/f
or
Cu
eNB
eNB
X2
SIM
USIM
E-UTRAN
MS

References

- Signalling System #7, ITU-T Q.700 series: http://www.itu.int/rec/T-REC-Q/e
- Mobile Application Part (MAP) specification, 3GPP TS 29.002: http://www.3gpp.org/ftp/Specs/archive/29_series/29.002/
- Reverse-Engineering für Ortsfremde, Datenschleuder #77 (Seite 26): http://ds.ccc.de/pdfs/ds077.pdf
- Leichtes Spiel mit symboltables, Datenschleuder #86 (Seite 63): http://chaosradio.ccc.de/media/ds/ds086.pdf
- Study into routeing of MT-SMs via the HPLMN, 3GPP TR 23.840: http://www.3gpp.org/ftp/Specs/archive/23_series/23.840/
- Support of Optimal Routeing (SOR), 3GPP TS 23.079: http://www.3gpp.org/ftp/Specs/archive/23_series/23.079/