KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

„Technologie komunikacji bezprzewodowej”
„Technologia GSM”

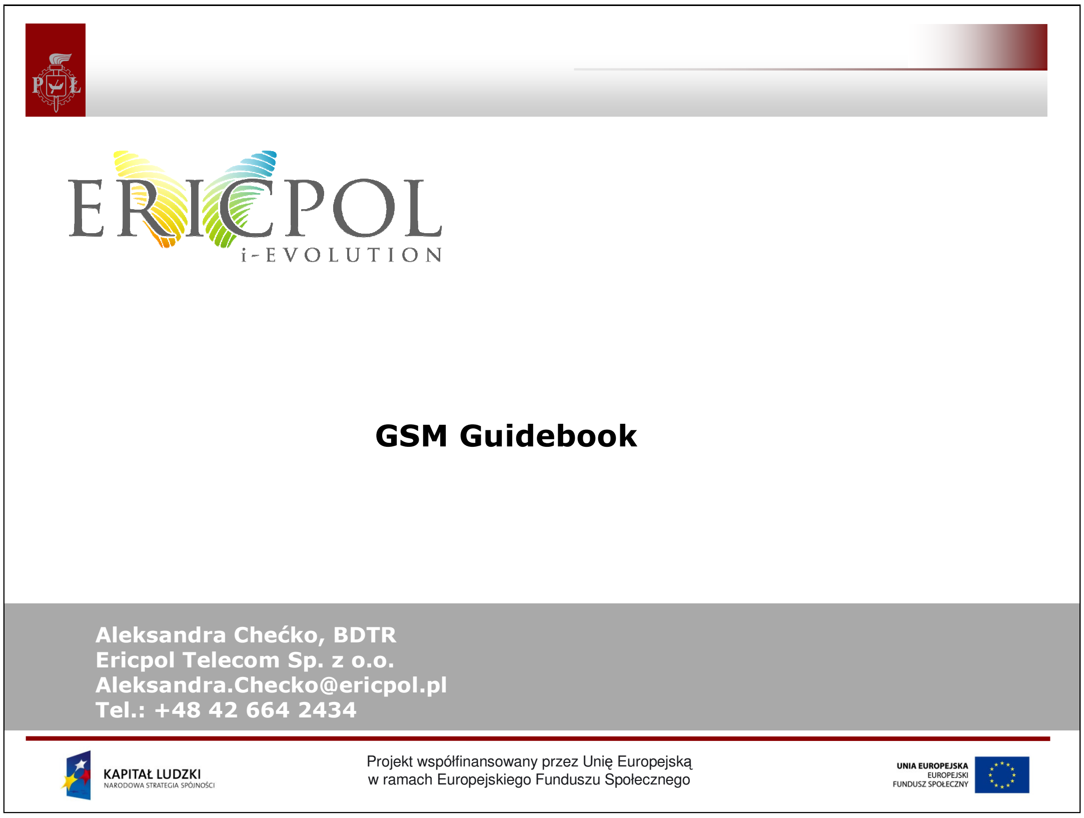
Prezentacja jest współfinansowana przez
Unię Europejską w ramach
Europejskiego Funduszu Społecznego w projekcie pt.

„Innowacyjna dydaktyka bez ograniczeń - zintegrowany rozwój Politechniki Łódzkiej - zarządzanie Uczelnią, nowoczesna oferta edukacyjna i wzmacniania zdolności do zatrudniania osób niepełnosprawnych”

Prezentacja dystrybuowana jest bezpłatnie

Politechnika Łódzka

Politechnika Łódzka, ul. Żeromskiego 116, 90-924 Łódź, tel. (042) 631 28 83
www.kapitalludzki.p.lodz.pl


GSM Guidebook
Aleksandra Chećko, BDTR
Ericpol Telecom Sp. z o.o.
Aleksandra.Checko@ericpol.pl
Tel.: +48 42 664 2434
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Agenda

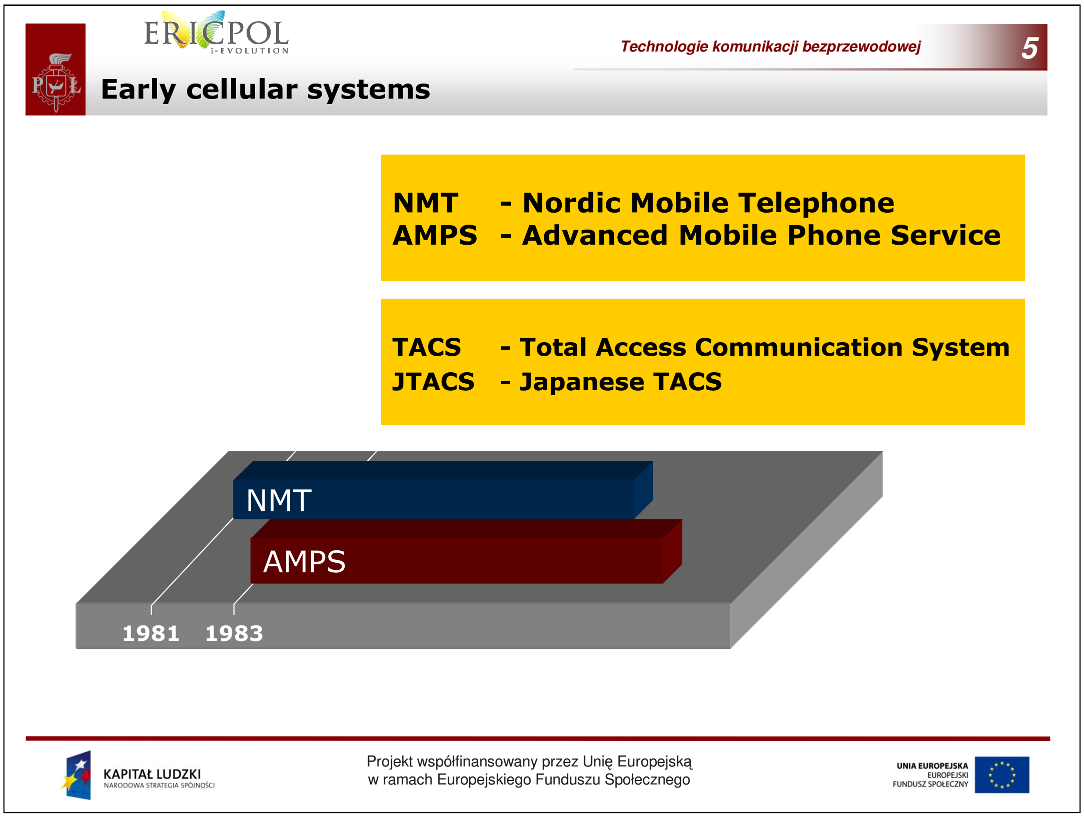
- GSM History and services
- GSM Structure
- Radio Interface
- ID - Numbers
- Traffic Cases

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Agenda

GSM History

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Early cellular systems

Early cellular systems were analog. They are called first generation mobile systems.

NMT450 Nordic Mobile Telephone 450 (1969) – Finland, Norway, Sweden

•Band 450MHz

•Become available in 1981

•First cellular system in Saudi Arabia (1981)

-NMT450 markets: Europe and Middle East

-NMT450 systems were installed in various countries on different frequencies and different channel spacings. This made them incompatible.

-NMT900 is basically NMT450 system moved to 900MHz.

AMPS Advanced Mobile Phone Service

-Band 800MHz

-AMPS markets: North and South America

-Become available in 1983

-AMPS has variants: TACS (Total Access Communication System enhanced AMPS) and JTACS (Japanese version of TACS)

TACS

-Operates at 900MHz frequency range

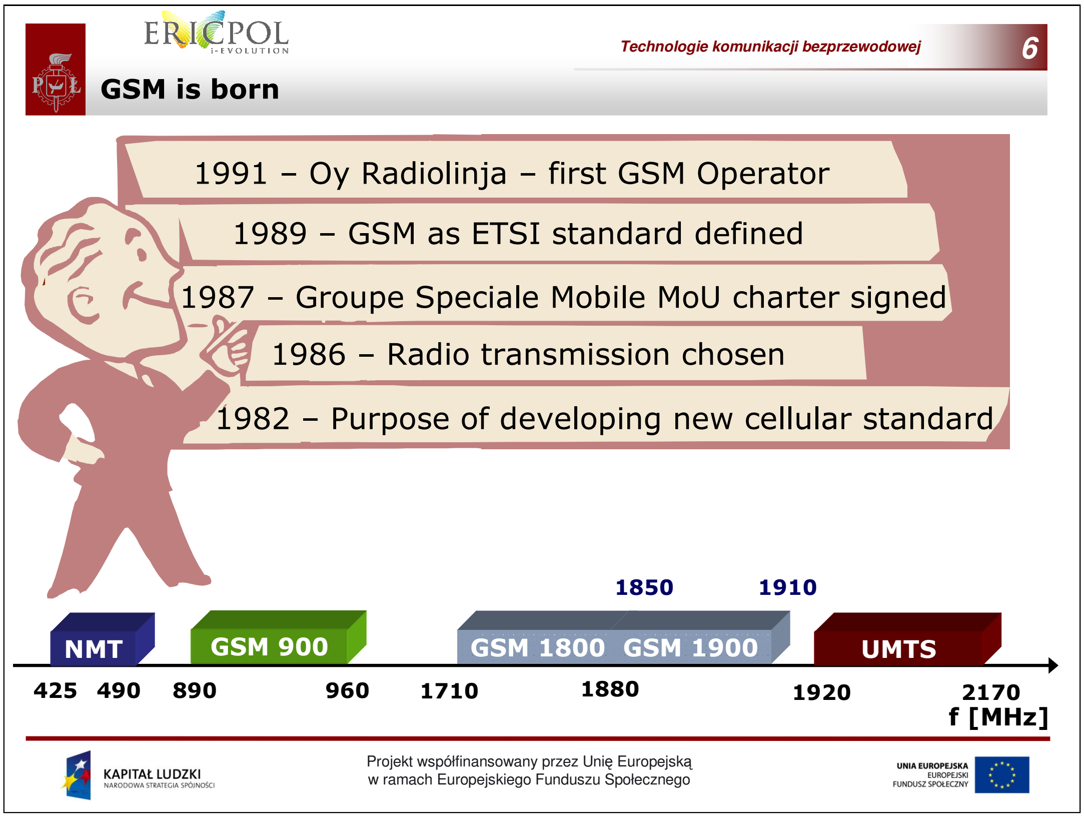
-TACS was developed by Motorola

-TACS was first used in UK in 1985

Note:

First cellular network in New York 1976 – max. 12 connection => 500 subscribers.

In the queue there were waiting 3700 people who would like to be a member of this network.



History of GSM

1982 – CEPT (Conference Europeenne des Postes et Telecommunications) began specifying a new digital cellular standard in the 900MHz band. EC (European Commission) reserves 900MHz band in member countries for GSM in roaming purposes.

1986 – Field tests were held in Paris. The aim was to select transmission technology. The choice was:

-TDMA Time Division Multiple Access

-FDMA Frequency Division Multiple Access

1987 – Transmission technology was selected: combination of TDMA and FDMA. Operators from 12 countries signed GSM MoU (Groupe Speciale Mobile Memorandum of Understanding MoU Headquarters are in Dublin, Ireland) committing themselves to introduce system by 1991.

1988 – Additional 5 countries signed MoU. CEPT began specifying system's implementation. Development was divided into phases.

1989 – Responsibility for GSM specification was transferred from CEPT to ETSI (European Telecommunication Standards Institute). The abbreviation GSM means: Global System for Mobile communication)

1990 – Phase 1 specifications developing was stopped. Manufacturers might start developing equipment.

1991 – New GSM 1800 standard was released. Countries outside CEPT could join MoU.

Oy Radiolinja became first GSM Operator (it was lunched in X instead of VII because of the electric compatibility tests).

First international roaming agreement was signed between Telecom Finland and Vodafone in UK.

1993 – First non-European country (Australia) joined MoU. The number of GSM subscribers reached one million. First commercial GSM1800 system was launched in UK.

1995 – Specification for PCS (Personal Communications Services) was developed in United States. System works at 1900MHz.

1997 – First dual band phone was introduced by Bosch

1999 – 165 million subscribers of GSM900/1800/1900 worldwide.

2000 – 480 million subscribers of GSM900/1800/1900 worldwide

2001 – 500 million subscribers of GSM900/1800/1900 worldwide

March 2002 – 677 million subscribers (source: EMC World Cellular Database)

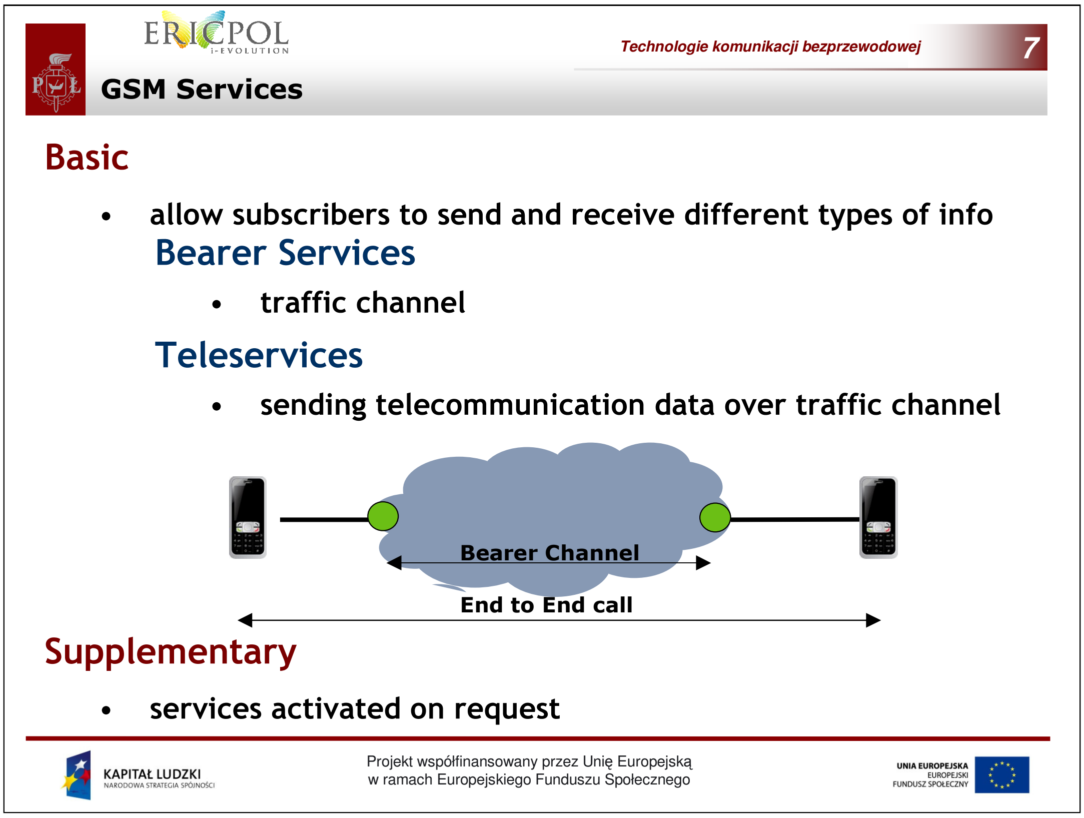
August 2002 – 733 million subscribers (source: EMC World Cellular Database)

February 2004 – 1005 milion subscribers (Cannes GSM Forum)

September 2007 – under 2 bilions subscribers (unique SIM card numbers)

In Europe each user sends an average of 35-40 SMS messages per month. In December 2001 there were 30 billion text messages send.

GSM accounts for over 71% of world's digital market and 69% of world's cellular market.



GSM Services

Basic services allow users to send and receive different types of information. An example of basic service may be sending and receiving SMS messages.

Supplementary services are optional services activated on subscriber's request by network operator. An example of supplementary service may be GPRS that is General Packet Radio Service. Subscriber must additionally pay for the service.

Basic:

-Telephony service

-Emergency calls

-Sms service

-Fax service

Supplementary service

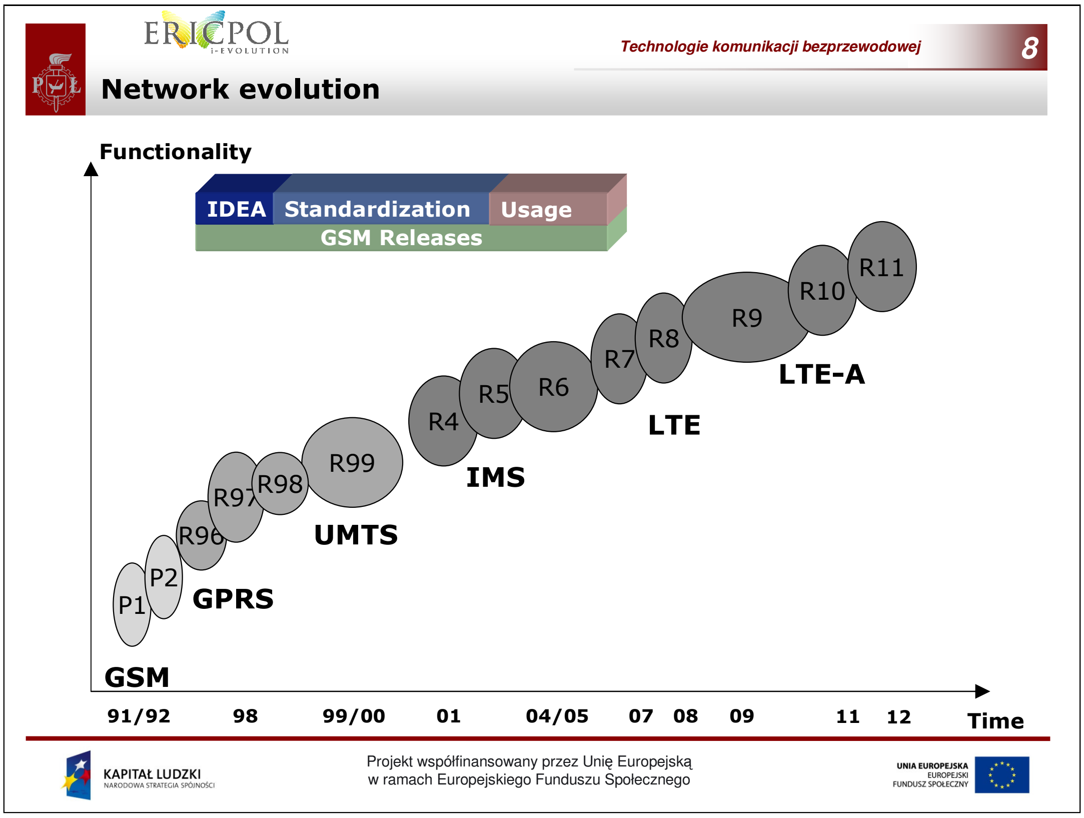
-Call forwarding

-Call barring

-Multiparty calls

-Calling line identification

The basic services are divided into Bearer services and Teleservices.



ETSI + 3GPP releases

GSM Phases

GSM is second generation mobile system. GSM specification was divided into phases. In late 1980 countries involved in developing GSM realized that they would not complete specifying all features of GSM by 1991. They decided to divide specifications into phases so manufacturers could start works on equipment. Each phase has limited services and features and it is to be fully compatible with prior phase. Each phase was built on top of existing one.

As we can see standardization works in GSM Phase 1 began in 1989 and lasted for 2 years. But in the meantime GSM Phase 2 idea were developed and then standardization was performed and so on with GSM Phase 2+. Manufacturers could begin working on equipment while GSM specifications were continued.

UMTS (Universal Mobile Telecommunication System)

UMTS is a 3rd generation mobile system. The UMTS is the multi-service network so called network of networks. UMTS will work with other networks such as PSTN, ISDN, Internet, GSM. UMTS supports both circuit and packet switched services.

Note:

In speaking we use „release” instead of „phase”.

GSM Phase 1 Services

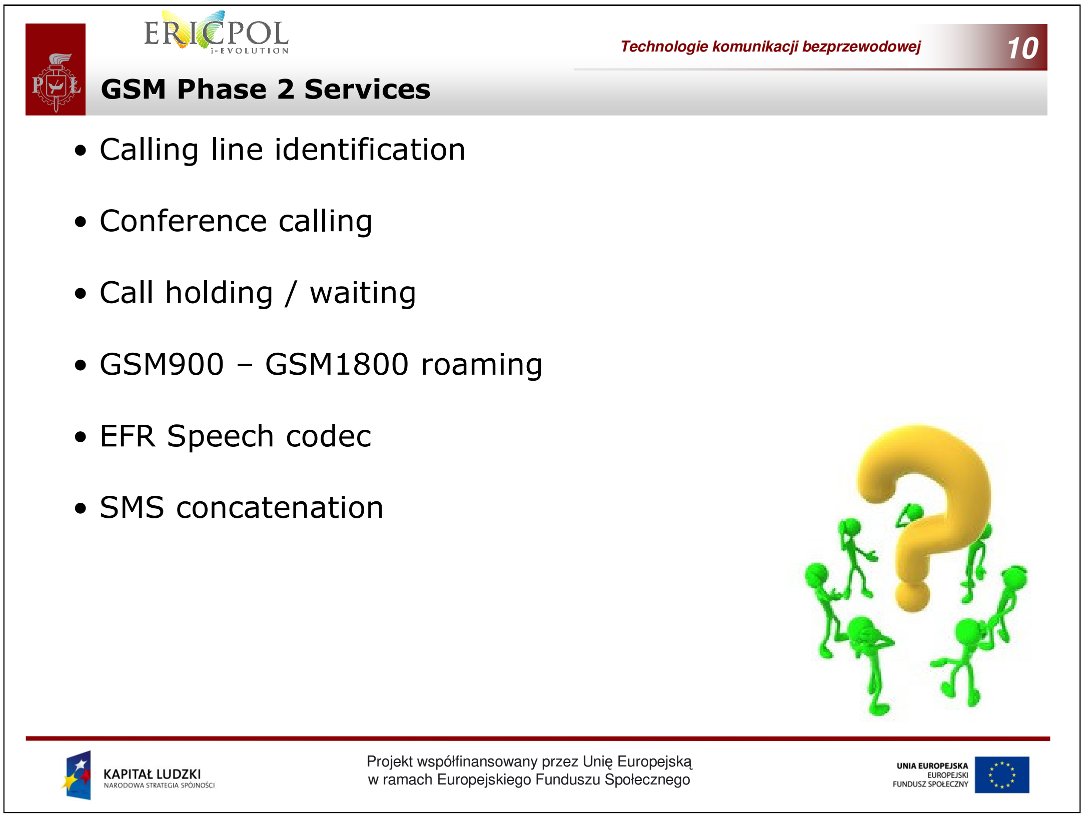
- Speech call
- Managing mobility
- SMS service
- Call barring
- Basic fax/data services
- Ciphering data

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

GSM Phase 1 Services

GSM Phase 1 features:

1. Voice telephony – allows subscribers receiving and sending speech calls.
2. International roaming – allows using MS with existing number outside home country if GSM operators signed appropriate roaming agreement
3. Basic fax/data services
4. SMS – Short Message Service allows sending and receiving text messages up to 160 characters
5. Call Forwarding- allows forwarding a call to another number when:
   - No Answer
   - Engaged
   - Unreachable
6. Call barring
   - Incoming calls
   - Outgoing calls
7. SIM cards In GSM system equipment is separate from network. This solution allows using equipment from different vendors and having all personal setting apart from MS.
8. Ciphering Exchanged information over the air interface is safe due to ciphering.



GSM Phase 2 features

- Multi Party Calling – Conference calls may be performed. Up to 6 calling parties are allowed.

- Call Holding - Places a call on Hold

- Call Waiting - Notifies of another call while on a call

- Mobile Data Services - Allows handsets to communicate with computers

- Mobile Fax Service - Allows handsets to send, retrieve and receive faxes

- Calling Line Identity Service - Allows subscriber to see the telephone number of the incoming call on our handset. Service commonly called CLIP.

- Advice of Charge - Allows keeping track of call costs.

- Cell Broadcast - Allows subscribing to local news channels

- Mobile Terminating Fax - Another number you are issued with that receives faxes that you can then download to the nearest fax machine.

ERICPOL i-EVOLUTION

GSM Release 96-98 Services

- Release 96
  - HSCSD
  - WAP
- Release 97
  - GPRS
  - Location services (LCS)
- Release 98
  - Adaptive Multi-Rate codec
  - EDGE

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

-Majority of the upgrade concerns data transmission, including bearer services and packet switched data at 57.6 kbps (14.4/TS) and above – HSCSD (High-speed circuit-switched data)

-WAP (Wireless Application Protocol) is a messaging service for digital mobile phones and other mobile terminals that will allow browsing Internet content in special text format in WAP enabled GSM phones.

-General Packet Radio Service

-Enhanced Data rates for GSM Evolution

GSM Release 99 Services

- Access to ISP in GPRS Phase 2
- Charging and billing for GPRS
- UMTS support
- Architecture of GSM-UMTS platform
- Service provider number portability
- IP-in-IP tunneling for GPRS
- Noise suppression for Adaptive Multi Rate speech

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

-Access to ISP in GPRS Phase 2 – user can choose an ISP, before that one ISP available for one operator

-Charging and Billing for GPRS – Advice of Charge, Hot Billing, Pre-Paid

-**UMTS Support:** Core based on ATM Transport, Numbering, Addressing and Identities

GSM/UMTS Release 4-6 Services

- Release 4
  - Layered architecture MSC Server-Media Gateway
- Release 5
  - RAN improvements
  - GERAN support for IMS
  - AMR WB
- Release 6
  - Multimedia Broadcast and Multicast service
  - AMR WB +
  - Support of PS handover (A/Gb interface)

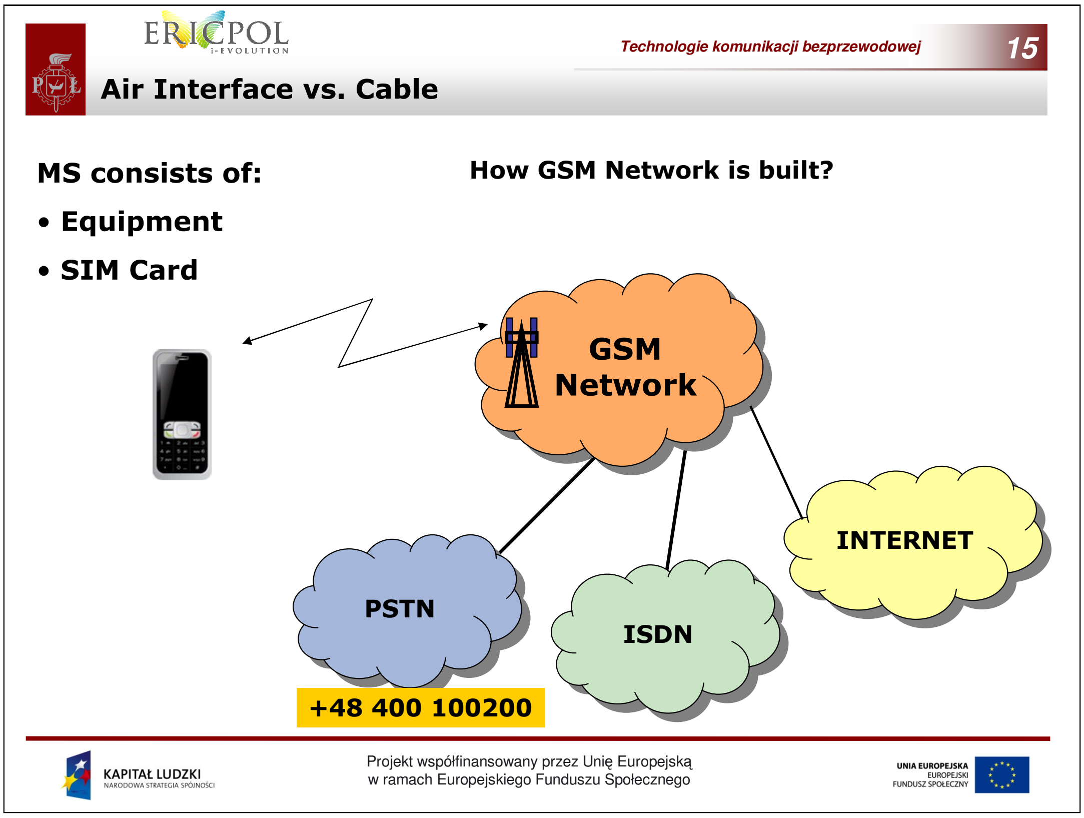
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Only major modifications.
WB – WideBand

GSM Structure

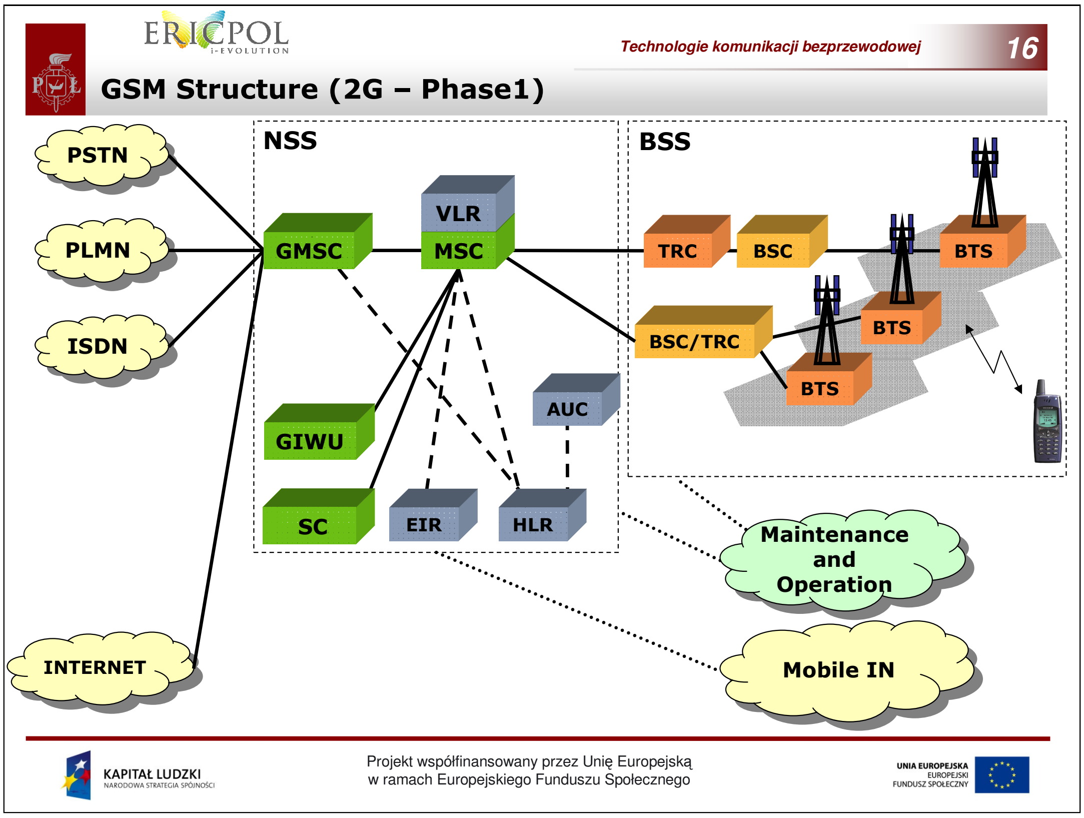
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

GSM Structure



Air Interface vs. Cable

Most of connections within GSM Network are done over the cable. The only air interface is between mobile station (phone) and GSM Network antennas.



Some difficult stuff GSM Structure

GSM structure seems to be very complicated. But when we identify roles of nodes the structure will be clear and straightforward.

Let’s now identify all necessary nodes in GSM network.

We have to assume that

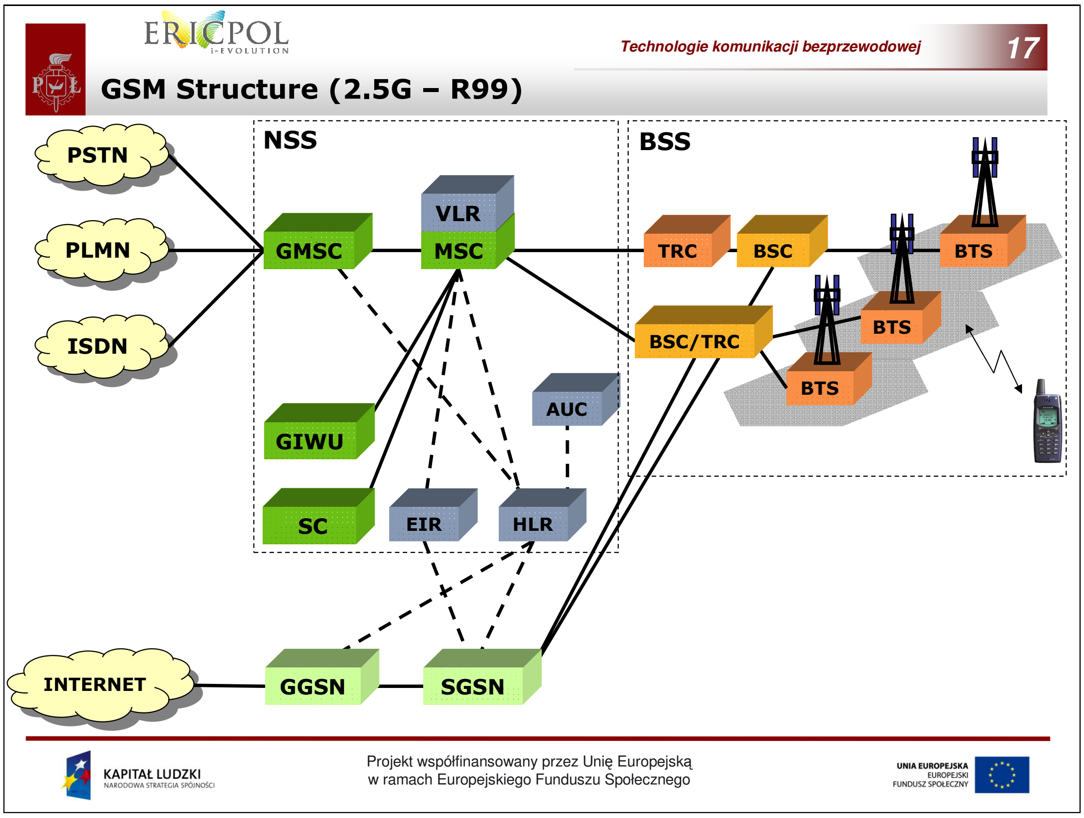
-Subscriber communicates with network via air interface

-Subscribers have different services allowed

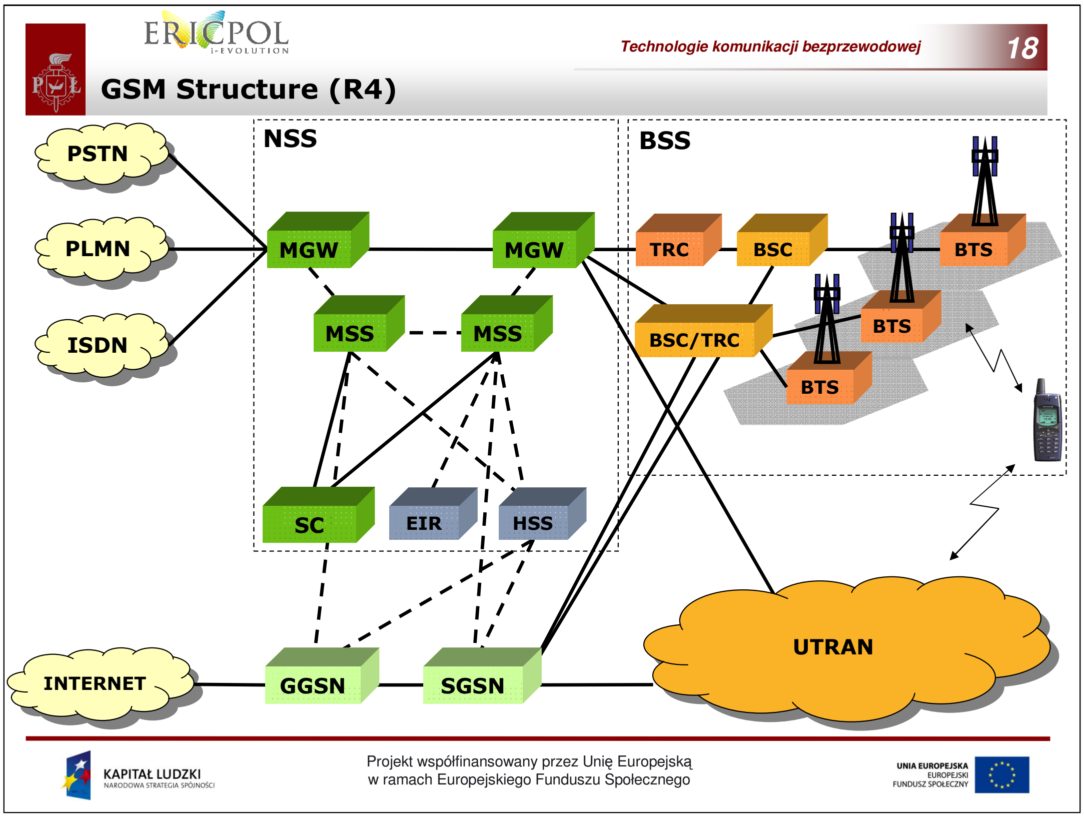
-Subscribers may send and receive calls from different networks

-Subscriber can send or receive SMS messages

-Network will not allow overhearing



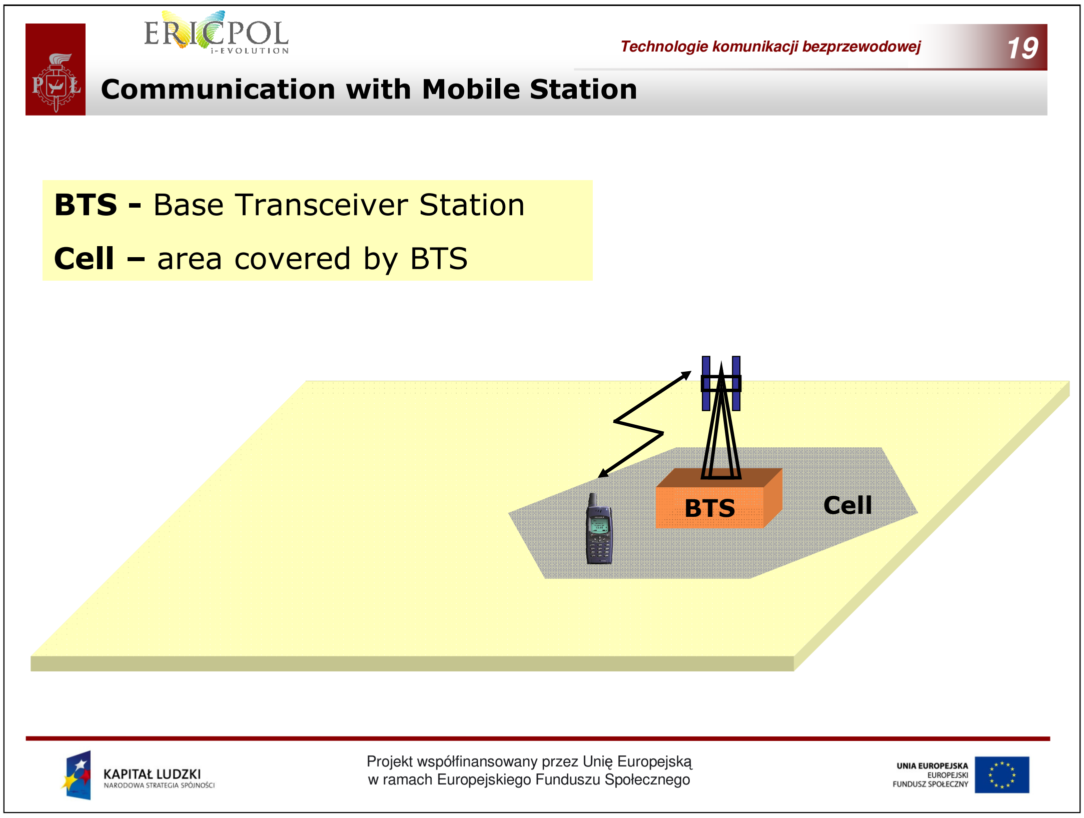
BTS can be connected in sequentialy. One from another BTS, not directly from BSC.



UTRAN – RNC plus multiple NodeB

R4 is second joined core network structure, but the most typical with layered MSC.

HSS – Home Subscriber Server



Communication with Mobile Station

GSM allows subscribers to transmit information over an air interface. Telephone in GSM is called Mobile Station an MS. It has to communicate somehow with the network. On one side of network we have the MS and on the other we have to have a device which sends and receives information from MS. The device is some kind of antenna which is not only an aerial as all may imagine but it has many other functions. In GSM such a device is called Base Transceiver Station a BTS. Area which is covered by one BTS is called a cell.

GSM is called cellular system because its composes of cells.

Single BTS covers limited area. The GSM is global system so it is necessary to have many BTSs to communicate with MSs to cover large area.

Note:

„For many people this is the GSM network” ☺

BTS

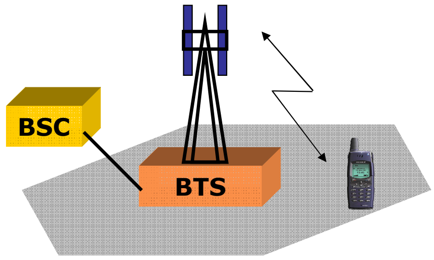
http://upload.wikimedia.org/wikipedia/commons/a/a0/BTS_NodeB_antenna_Sopot.jpg

BTS - Base Transceiver Station

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Base Transceiver Station

- Radio transmission
- Radio signal reception
- Signal processing
- Quality measurements
- Synchronization / maintenance
- Broadcasting system information



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Base Transceiver Station

Base Transceiver Station is responsible for radio related functions. BTS's main function is to provide an air connection with the MS.

BTS functions may be divided into following areas:

-Radio resources

-Configuration and system start: loading software from the BSC and setting transmitter and receiver frequencies, power output Base station Identity Code (BSIC).

-Radio transmission. The BTS transmits several frequencies using the same antenna. Power is controlled from the BSC.

-Radio reception.

-Signal processing. BTS performs signal processing before transmission and after reception.

-Ciphering

-Channel coding

-Interleaving

-Equalization

-Realization of diversity

-Demodulation

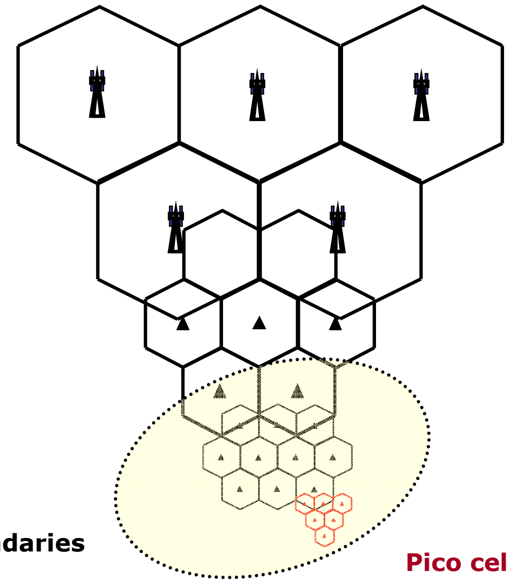
-Signalling link management. BTS manages signalling link between BSC and MS.

-Synchronization

-Local maintenance handling. BTS allows performing operation and maintenance functions without BSC.

-Functional supervision and testing.

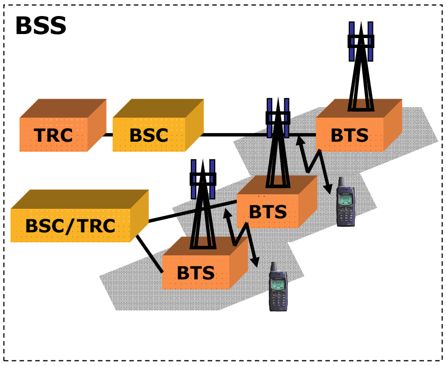
Coverage optimisation



ERICPOL i-EVOLUTION

Technologie komunikacji bezprzewodowej 24

How to control BTSs and MSs



BSC – Base Station Controller

BSS – Base Station System

TRC – Transcoder

TRAU – Transcoder and Rate Adaptation Unit

- Provides bitrate transcoding from 13 kbps -> 16 kbps and 16x4 -> 64 kbps

How to control BTSs

Because there are so many BTSs they have to be controlled somehow. There has to be a master device over BTSs. A device which controls programs run in BTS, radio interface, information sent to MSs. In the GSM such a device is called Base Station Controller a BSC. Single BSC can control limited number of BTSs so in GSM network there is large number of BSC devices. BSC controlls all radio specific parameters so the rest of the network is similar to standard exchange. BSC makes the radio interface transparent to the network.

There are also Transcoders TRCs combined with BSCs. Transcoders are used to perform transcoding and rate adaptation. Transcoder coverts information arriving to BSC to a rate of 16kbps from a rate of 64kbps. Due to this conversion less expensive links may be applied towards BSC. There are two possible solutions to place a TRC. It may be a stand-alone device or it may be placed in the same node as BSC.

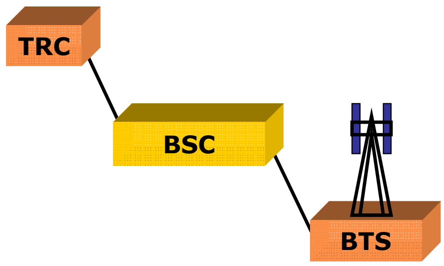
Note:

- Base Station System BSS consists of Base Station Controllers, Transcoders and Base Transceiver Stations.

- In no Ericsson hardware TRC can be also physically located in BTS or MSC.

Base Station Controller

- Radio network management
- BTS administration and control
- Traffic measurements
- Connections handling
- Software handling



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Base Station Controller

Base Station Controller is a central node in Base Station System. It coordinates BTS and TRC. It controls a major part of radio interface. The main functions are:

-Radio Network Management

-Administration of radio network data: cell description, network information data, cell load data

-Traffic Measurements

-Event Measurements

-Idle Channel Measurements, BSC collects statistics about quality and strength of signal from MS

-BTS Management. Relationship between BSC and BTS is master-slave. BSC has logical model of all BTS connected.

oBTS configuration involves defying frequencies to channel combinations and power levels for each cell.

oBTS software handling. BSC controls programs run in BTSs

oBTS equipment maintenance. BTS errors are recorded.

-TRC Management

-Transmission Network Management. BSC controls links to BTS

-Internal BSC Operation and Maintenance

-TRH maintenance

-Processor load control in BSC

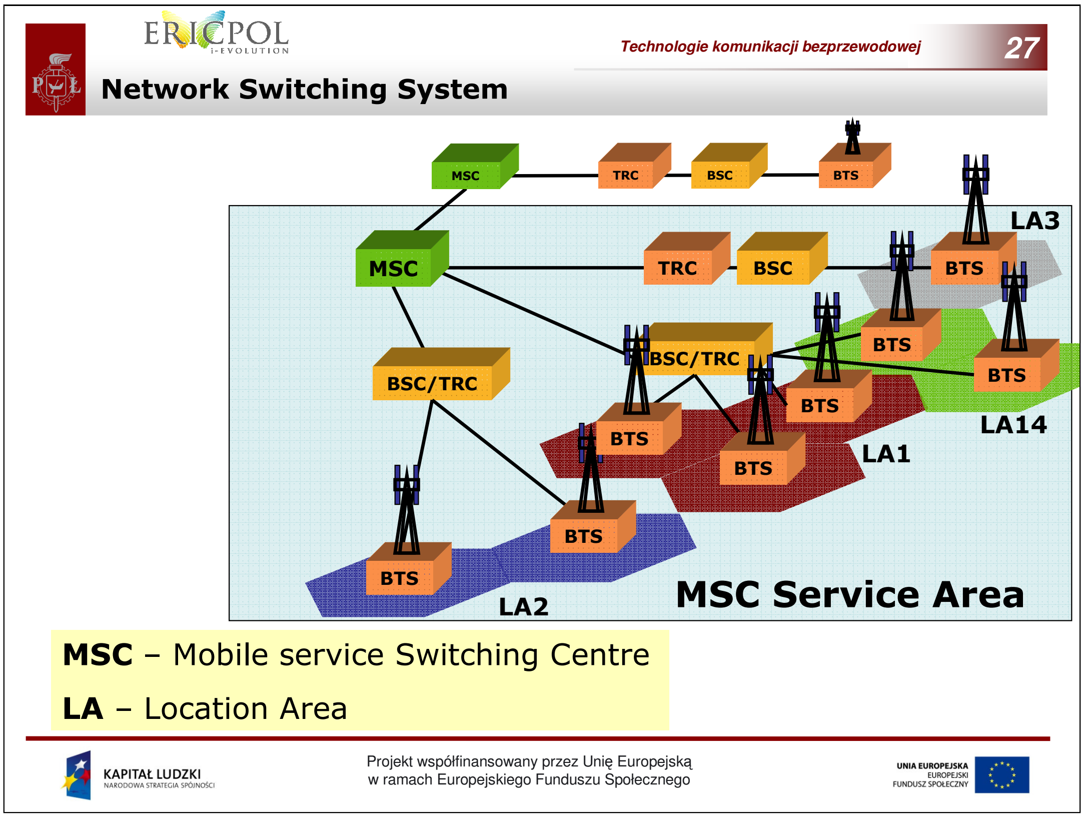
-Handling of MS connections

-BSC performs radio channel assignments

Max number of cell (BTS) in control: 1024 current (2008) 2048 after 09A project (implementation 05.2009)

Base Station Controller

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY



Switching Part

How to control many BSCs?

How to distinguish between different BSCs?

How to set-up and control calls?

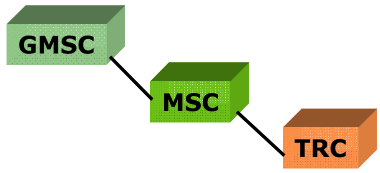
In GSM network Mobile service Switching Center a MSC is used in such purposes. It controls many BSCs. Geographical area controlled by single MSC is called MSC service area. It is also divided into smaller areas called Location Areas. Location Area is used to specify where the MS is. When mobile subscriber moves within Location Area he/she does not have to report it to the network. When there is an MS terminated call GSM network knows where the MS is and does not have to search for subscriber in all network. Network sends message to location area where the MS currently is.

One Location Area can't belong to two different MSC Service Areas. In each MSC there is dedicated for mobile exchange subsystem – MTS (Mobile Telecommunication Subsystem) – which lets to find the relation between BSC's and Location Area's.

There are also Transcoders TRCs on the path between MSC and BSC. Transcoders are used to perform transcoding and rate adaptation. Transcoder coverts information arriving from MSC at a rate of 64kbps to a rate of 16kbps. Due to this conversion less expensive links may be applied towards BSC. There are two possible solutions to place a TRC. It may be a stand-alone device or it may be placed in the same node as BSC.

Mobile services Switching Centre

- Setting up and controlling calls
- Handling speech path continuity for moving subscribers
- Updating mobile subscriber data
- Receiving and delivering short messages
- Charging



Mobile services Switching Center

Mobile services Switching Center is a primary node in the GSM network. It controls calls from and to MS.

-Switching and call routing. MSC controls call set-up, supervision and release. It interacts with other nodes in order to establish a call.

-Charging. MSC contains functions for charging the calls. It applies appropriate charge rate considering time and destination of the call. MSC records this information and stores it after the call.

-Service provisioning. Supplementary services are provided and managed by the MSC.

-Communication with HLR. MSC provides HLR with information about routing information.

-Communication with VLR. MSC communicates with VLR and retrieves information about subscription

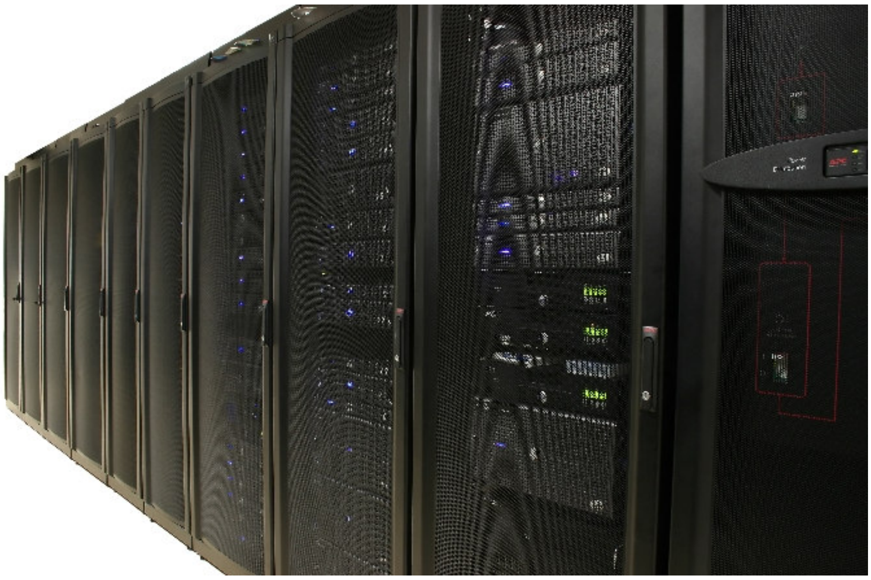
-Communication with other MSC

-Control of connected BSC. MSC controls primary Base Station System's node BSC. MSC can control many BSCs.

-Direct access to Internet services

-ISDN Primary Rate Access. Function provides PRA services to subscribers.

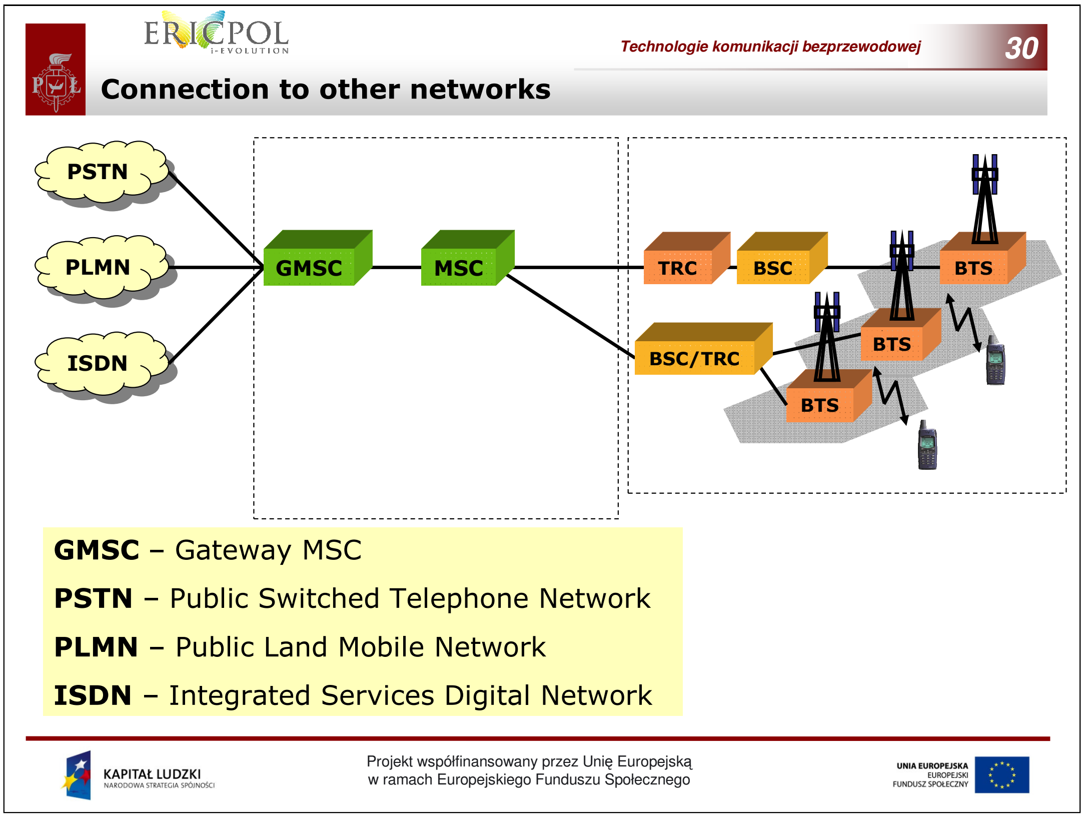
Mobile services Switching Centre



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY



Connection to other networks

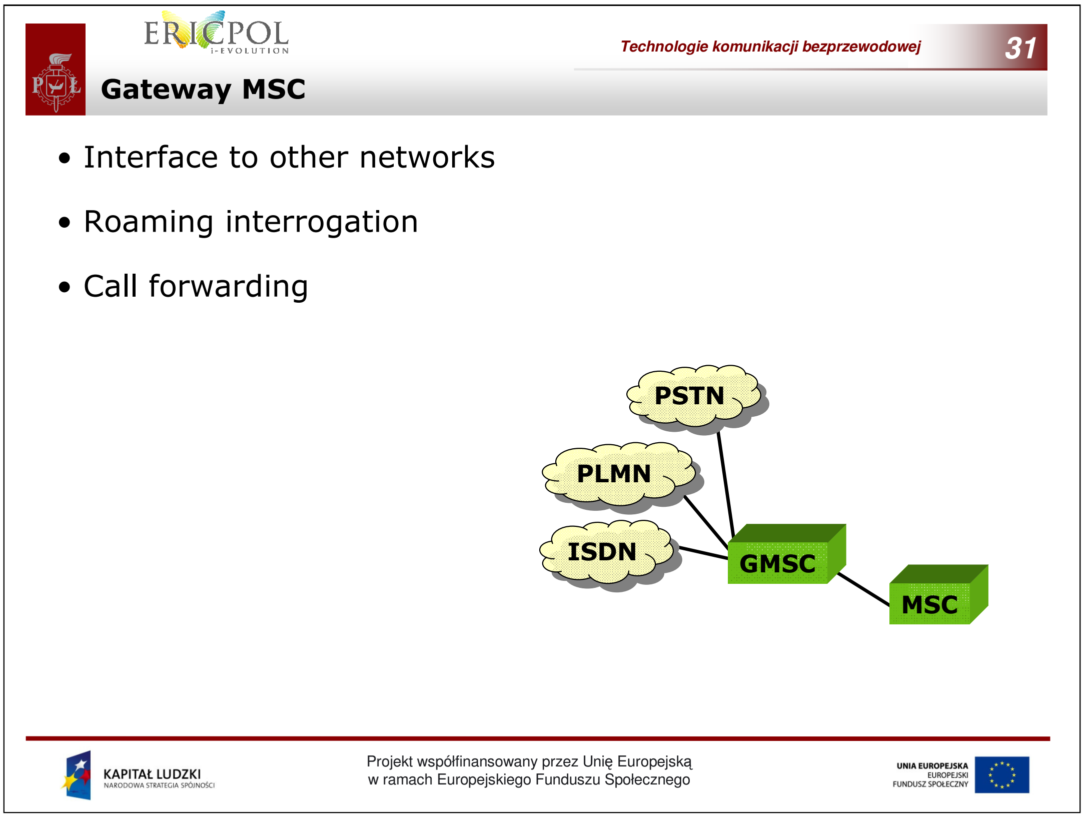
Subscriber of GSM network must be able to communicate with subscribers in other networks and vice versa. Gateway MSC GMSC is a special node in GSM network for these purposes.

GMSC – Gateway Mobile service Switching Centre

ISDN - Integrated Services Digital Network

PLMN – Public Land Mobile Network, mobile networks (different operators, different systems)

PSTN – Public Switched Telephony Network, Fixed network

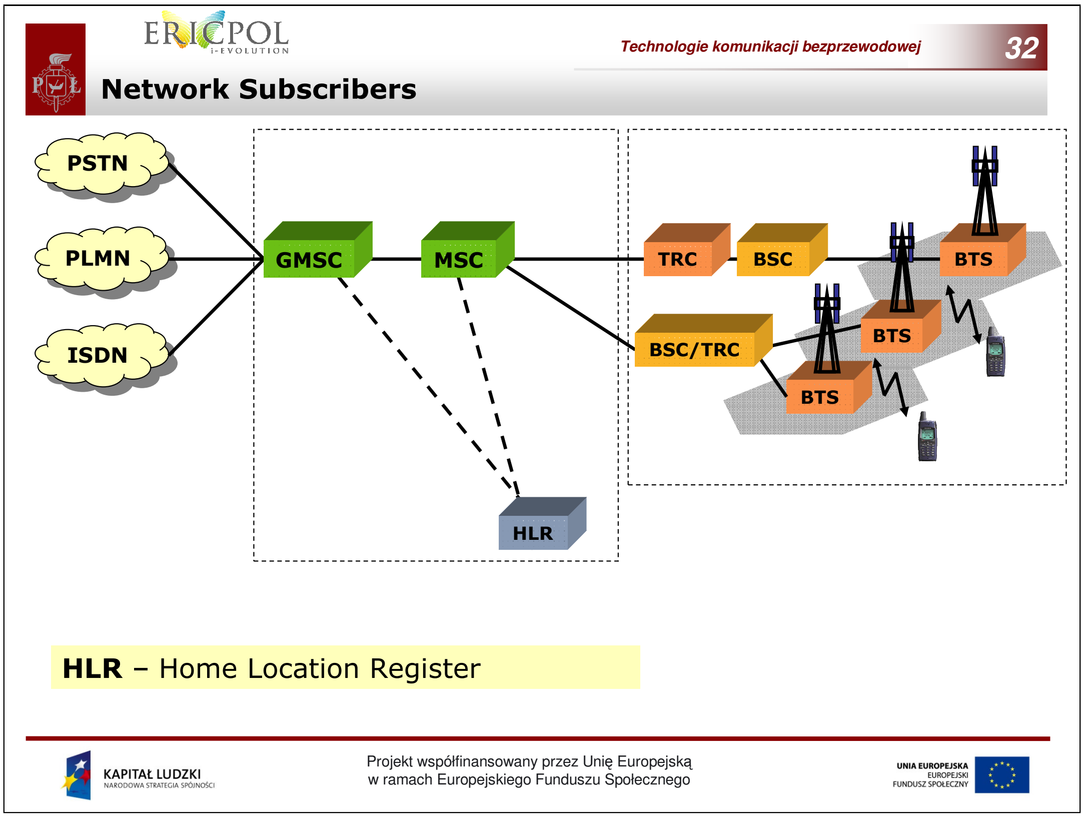


Gateway MSC

GMSC is an interface between GSM network and other networks. GMSC is used when somebody wants to make a call to MS.

<u>Each MS terminated call must be routed via a GMSC in the home PLMN of the called MS.</u>

<u>GMSC is also used when MS makes a call to another MS</u>. GMSC interrogates HLR in order to route a call. HLR provides GMSC with information which MSC/VLR is the MS in. HLR returns MSRN number to set roaming rerouting. HLR may also return Forwarded-to number in case of forwarded call. GMSC may have charging functionality for forwarded call.



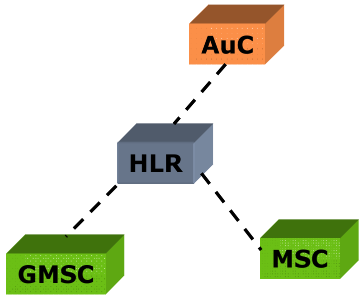
Network Subscribers

GSM Network must identify all its subscribers. It must know who can do what. So there is some kind of database needed. There is a device called Home Location Register for these purposes a HLR. It stores information about subscriber's category, what services it may use. HLR also stores subscriber's telephone number and its current location.

Home Location Register

Database which stores:

- Subscriptions
  - MSISDN number
  - IMSI number
  - list of services
- VLR/MSC address
- Authentication and ciphering data



KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Home Location Register

HLR is a database which stores and manages all subscriptions of PLMN.

HLR functions:

- Information storing:

    -Subscriber's identity (IMSI, MSISDN)

    -Subscriber's supplementary services

    -Subscriber's location (MSC service area)

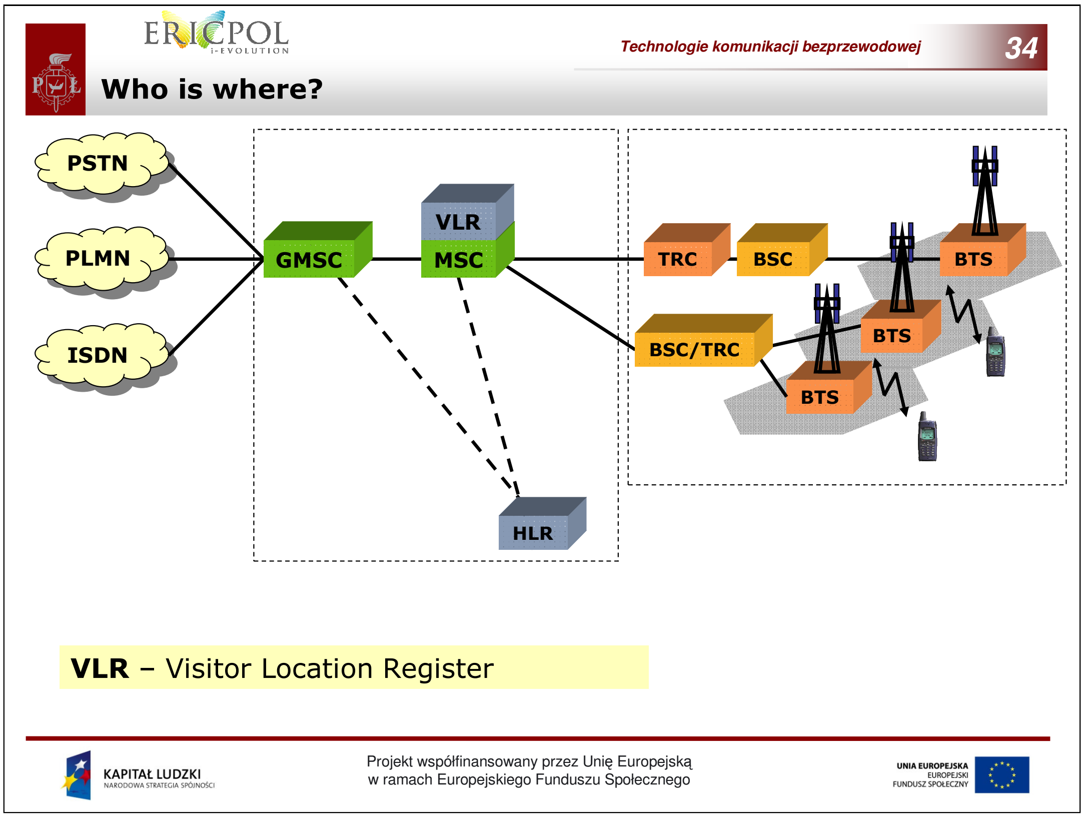
    -Subscriber's authentication information

-Communication with MSC. HLR provides MSC with routing information.

-Communication with GMSC. HLR provides GMSC with information about current MS's MSC service area.

-Communication with AuC. It handles authentication and ciphering data for mobile subscriber.

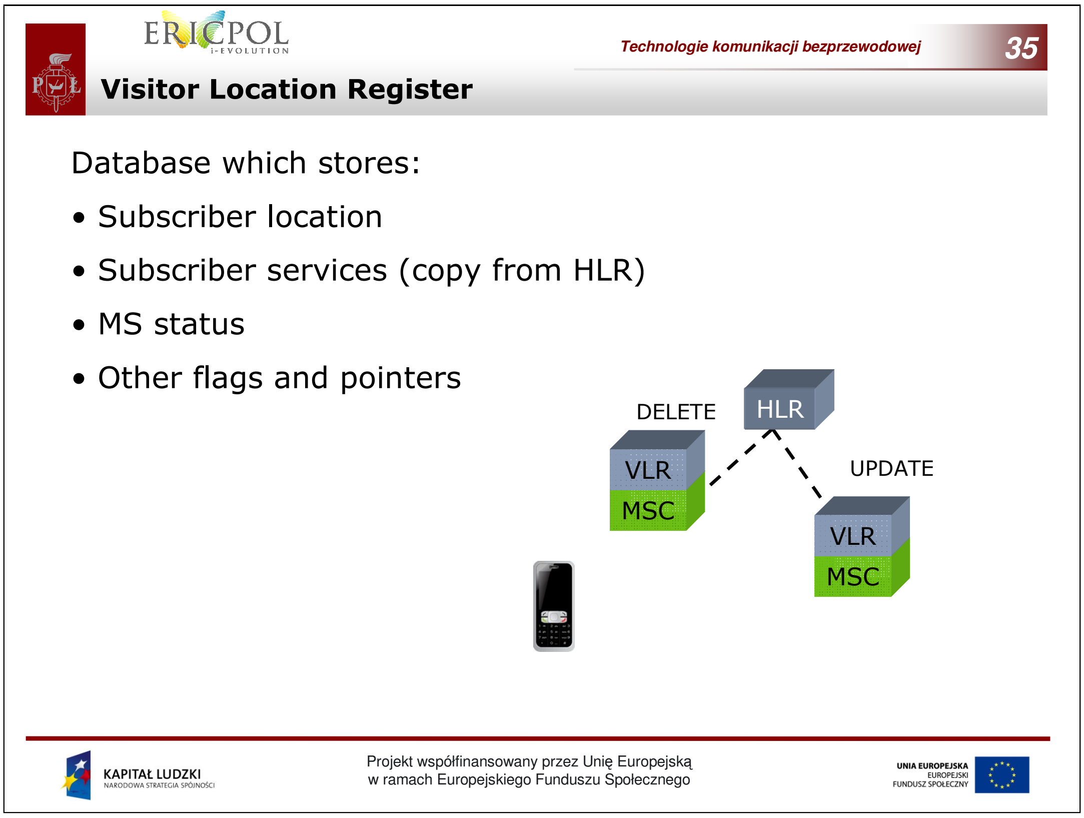
-Communication with VLR. When MS changes MSC service area HLR provides VLR with subscription information, updates data about new MSC service area and orders old VLR to delete subscription information.



Who is where

Visitor Location Register stores information about subscribers which are currently in a MSC service area. It is always combined with MSC. VLR may be seen an distributed HLR.

In Ericsson hardware the VLR is always combined with MSC. It is also possible to have one VLR for several MSC.



Visitor Location Register

VLR is temporary storage for subscription information for MSs which are within particular MSC service area. There is one VLR for each MSC. Each time subscription information is needed within MSC service area MSC does not have to contact HLR to get it. The VLR can be seen as distributed HLR. When the MS roams into particular MSC/VLR service area VLR requests information about the subscriber from HLR and stores it. When the MS makes a call MSC/VLR already has information needed in call set-up.

The VLR contains:

-MS status,

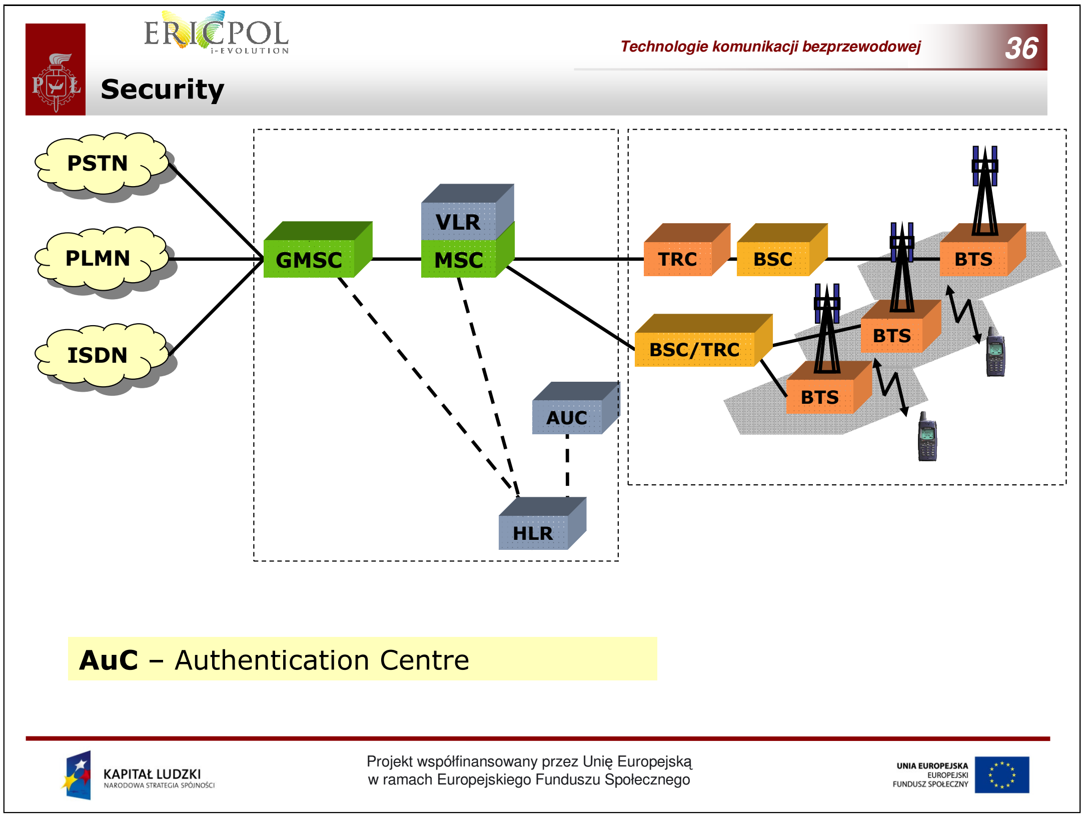
-LAI,

-MSISDN,

-HLR’ s address,

-Subscriber’s categories,

-Triplet.



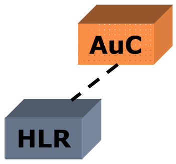
Security

Communication must be secure in the GSM network. There is a separate network node which provides security. It is called Authentication Center AuC. There are information for each subscriber stored. AuC provides HLR with these information on its request.

Authentication Centre

Node which generates:

- Subscribers triplets
  - RANDom number – RAND
  - Signed RESponse – SRES
  - Ciphering Key – Kc



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Authentication Center

AuC's main function is to provide MSC/VLR with information which is used in authentication purposes. Information is also used in ciphering procedures on radio path between network and MS.

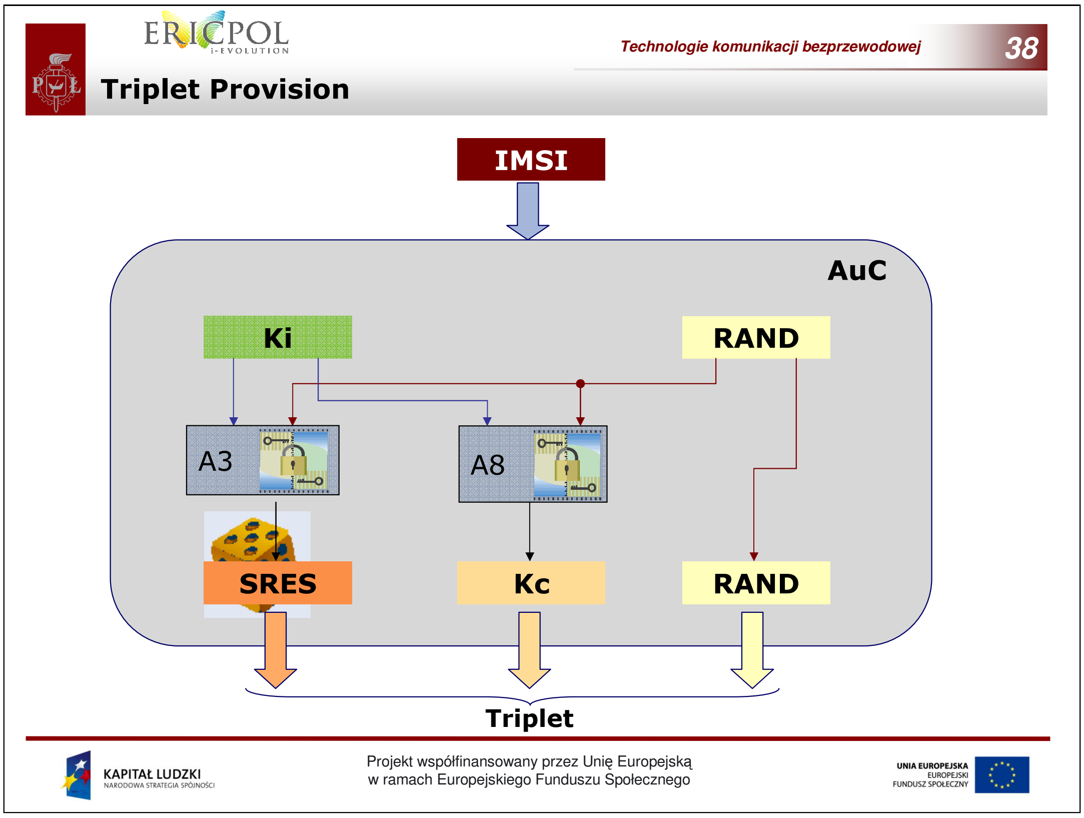
Subscriber's authentication information is called triplet. It consist of:

-RAND (Random number)

-SRES (Signed Response)

-Kc (Ciphering Key)

At subscription time each subscriber is provided with authentication Key (Ki). Ki is stored in the AuC with subscriber's IMSI. Ki and IMSI are also stored in subscriber's SIM card. Ki and IMSI are used in providing a triplet. Triplets are delivered to HLR on request.



Triplet Provision

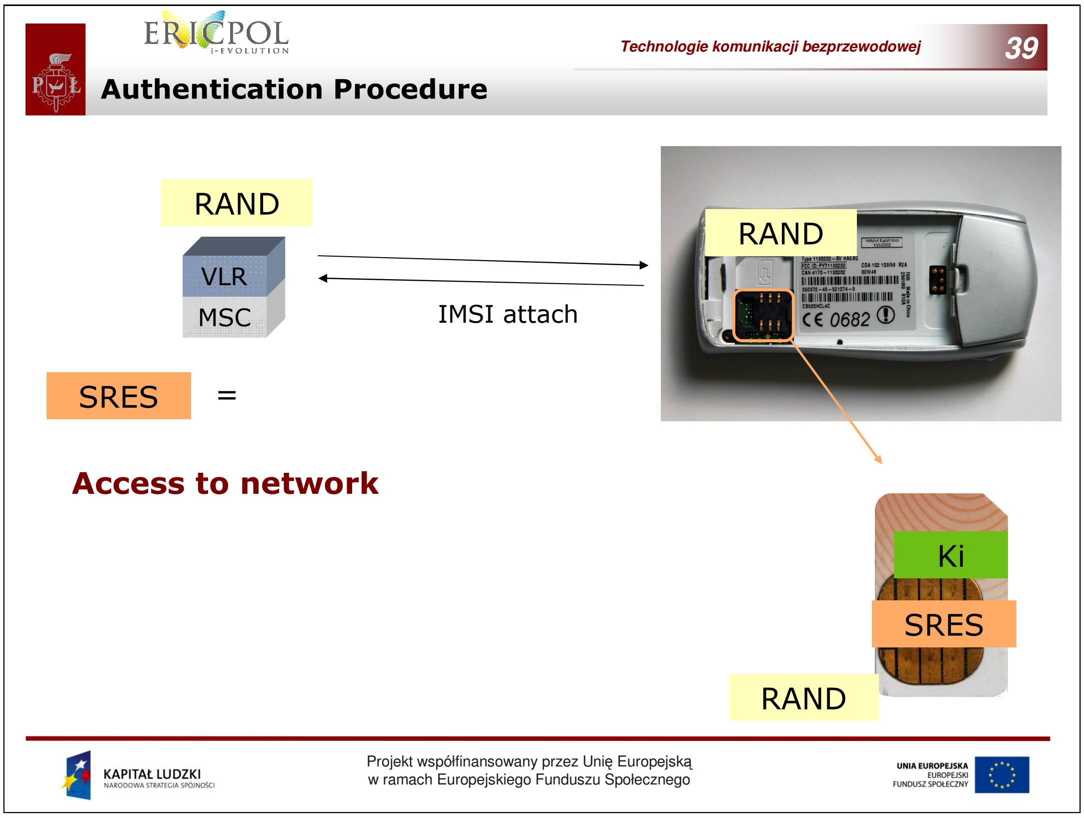
1. Non-predictable random number is generated
2. RAND and Ki are used to calculate SRES using A3 algorithm
3. RAND and Ki are used to calculate Kc using A8 algorithm

Note:

0 < RAND < 2^128 – 1 => 10^36 possibilities

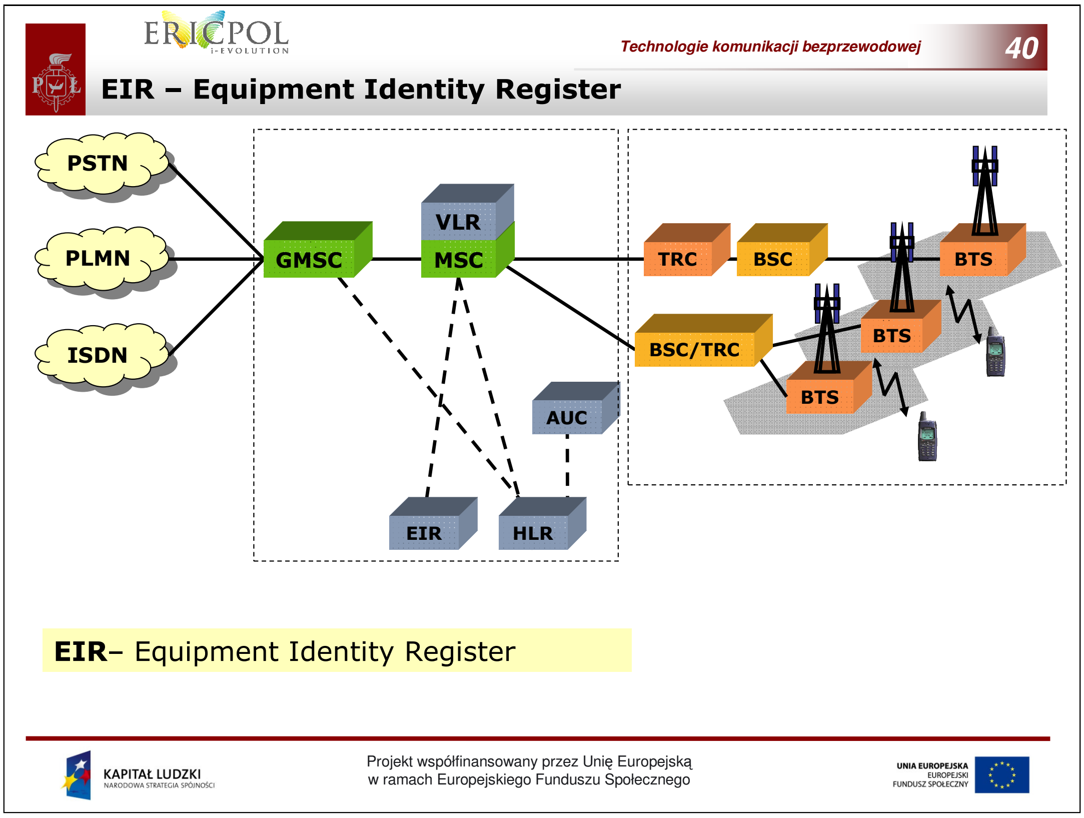
A3 isn't described in GSM standards.

SRES – 32 bits



Authentication Procedure

1. MSC sends RAND number to the MS.
2. The MS calculates SRES number from RAND and authentication key Ki using A3 algorithm. Ki number is stored within SIM card.
3. SRES signature is sent to the MSC. MSC performs authentication. It check if SRES from the MS and SRES from AuC match. If so subscriber is allowed using the network. If not access to network is denied.



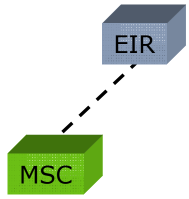
Equipment Identification

There is a possibility to ban access to network for stolen, faulty equipment in GSM system.

Equipment Identity Register

Database which stores:

- IMEI number
- Provides information about
  - stolen equipment (black list)
  - faulty equipment (grey list)
  - unknown equipment



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Equipment Identity Register

In GSM equipment itself must be checked to fulfill identification requirement because subscription and equipment are separate. IMEI number is used in equipment identification. During any MS access MSC may verify IMEI.

After IMEI reception EIR examines 3 lists:

-Black list, equipment identities which have been stolen

-Grey list, should be tracked for evaluation

-White list, equipment approved by the operator

-Unknown equipment

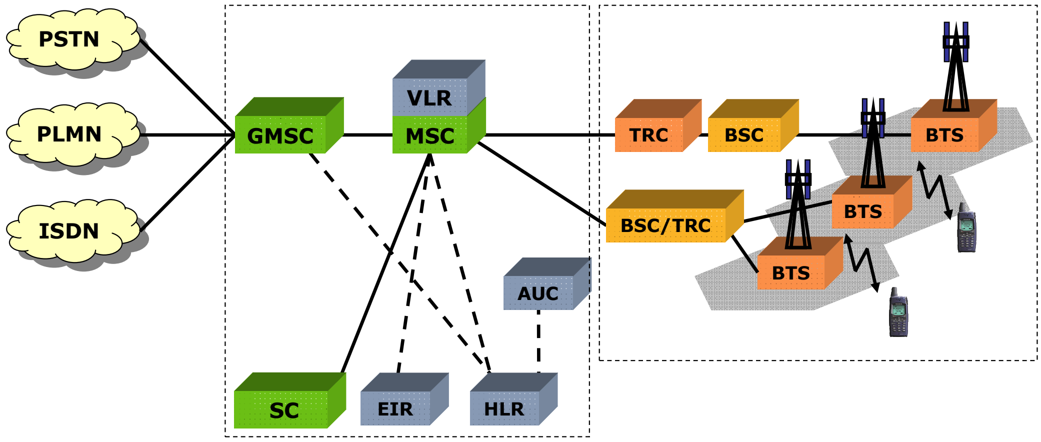
The network rejects equipment if is on black list or unknown.

It must be noted that equipment barring does not mean subscriber barring since these are separate.

Note:

CEIR = Central EIR (in Ireland) – many European operators use this database.

Short messages



SC – Service Centre

(SMS-C – Short Message Service Centre)

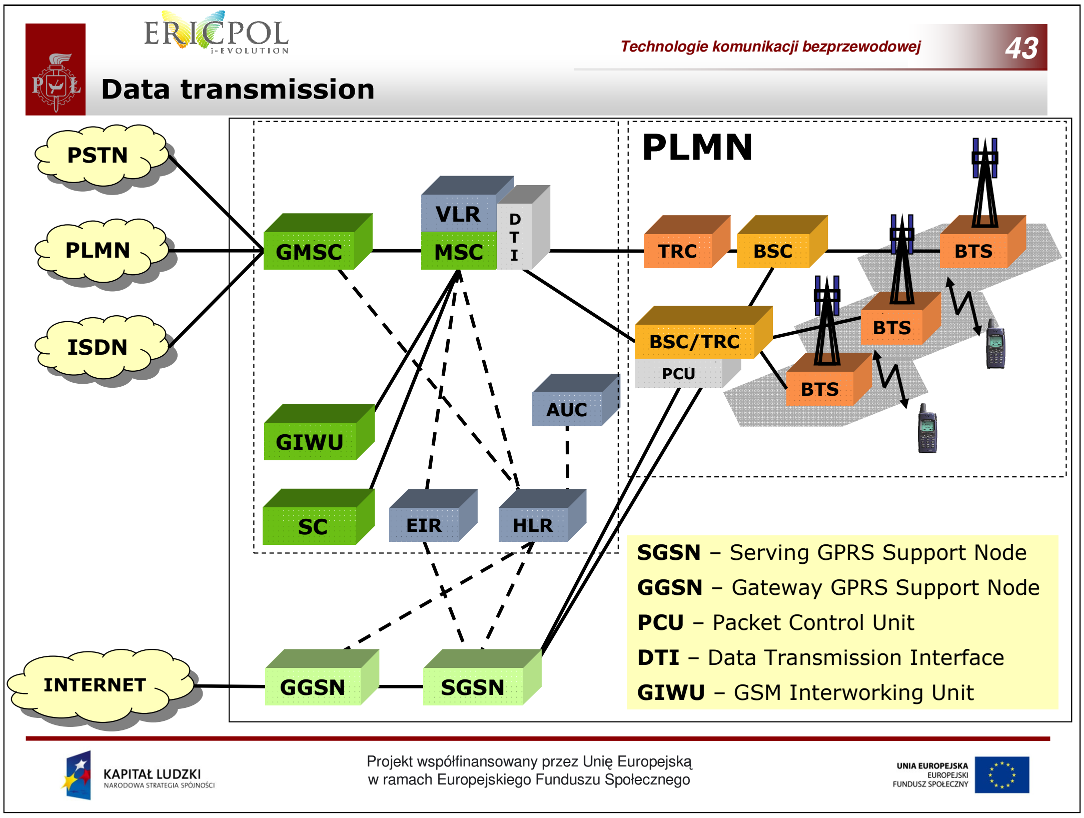
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Short Messages

GSM system allows users to send or receive text messages. These messages are called SMS messages. There is a device which is used to transmit SMS messages it is SMS-GMSC Short Message Service Gateway MSC.

Service Centre (SC): function responsible for the relaying and store-and-forwarding of a short message between an SME and an MS. The SC is not a part of the GSM/UMTS PLMN, however MSC and SC may be integrated.

There are two main scenarios: SM MO and SM MT. Plus additional problems like undelivered messages.



Data transmission

GSM allows its subscribers to transfer data for example faxes. The GIWU is the device which support data services in GSM. GIWU stands for GSM Interworking Unit.

Early data transmission was relatively slow. Basic data transfer speed was at rate of 9.6 kbps. It had to be changed. GSM Phase 2+ introduced GPRS service which allows subscribers data transfer at rate of 171.2 kbps. Transfer is sufficient for multimedia applications and comfy internet browsing.

GPRS stands for General Packet Radio Service and it is packet-switched service. Thus GPRS requires additional nodes in GSM structure. Packet Control Unit must be added to the BSC. Serving GPRS Support Node SGSN acts as an MSC in GSM circuit-switched connection. It forwards incoming and outgoing IP packets addressed to/from the MS. SGSN serves all subscribers which are physically located within geographical SGSN service area. SGSN also provides authentication and ciphering, mobility management, manages logical link to the MS.

Gateway GPRS Support Node GGSN is a device which is an interface towards the external IP packet networks.

BSC must have additional Packet Control Unit PCU to support GPRS connections.

Note:

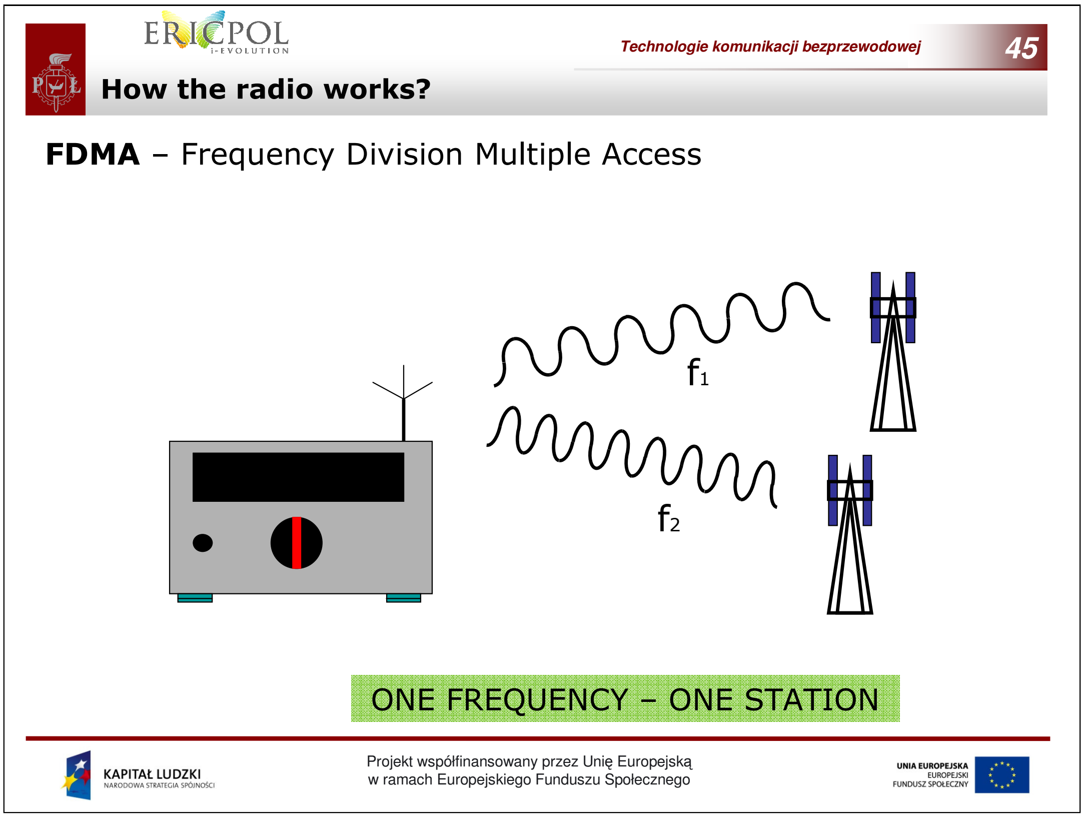
In previous versions of CME20/CMS 40 the functions of the DTI were implemented using a GSM Inter-Working Unit (GIWU), separate from the MSC/VLR.

SGSN contacts with HLR to authenticate the MS while transferring the packet data.

Radio Interface

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Radio interface



How the radio works

FDMA – Frequency Division Multiple Access

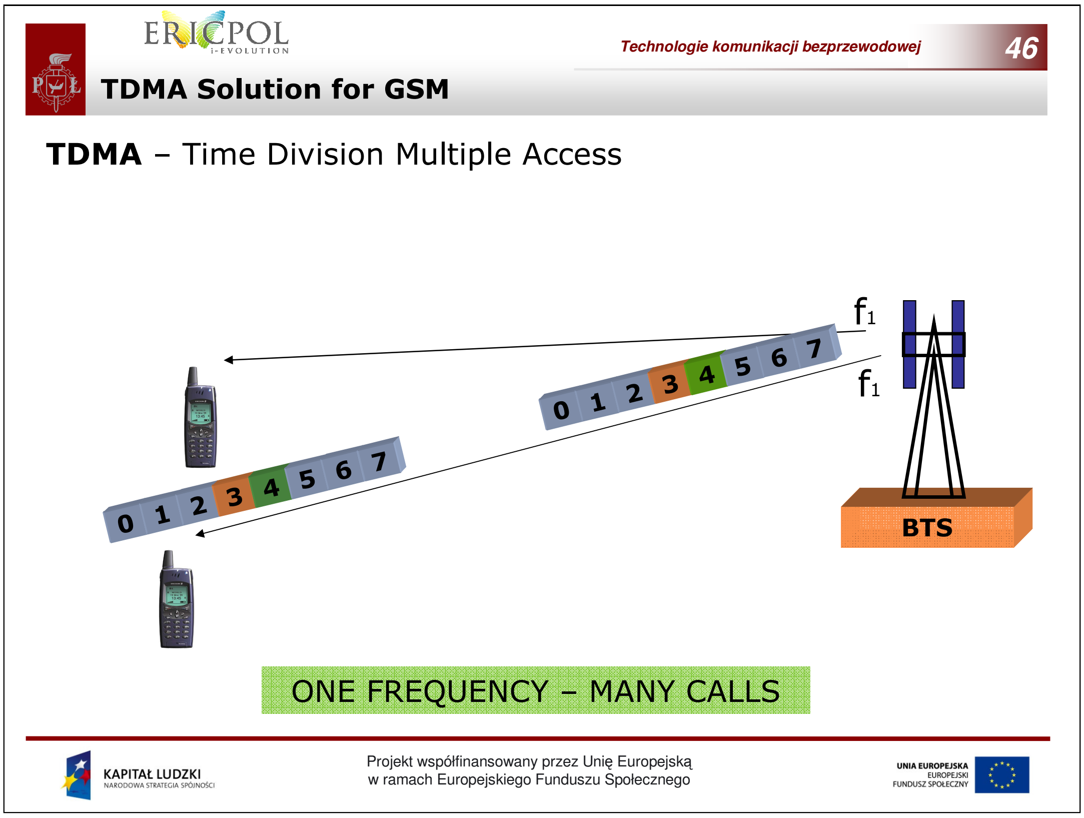
Each radio station has its own frequency. FDMA was used by early cellular systems like NMT or AMPS.

Note:

Full duplex: f1+f2,

Half duplex: f1 (for example walkie-talkie),

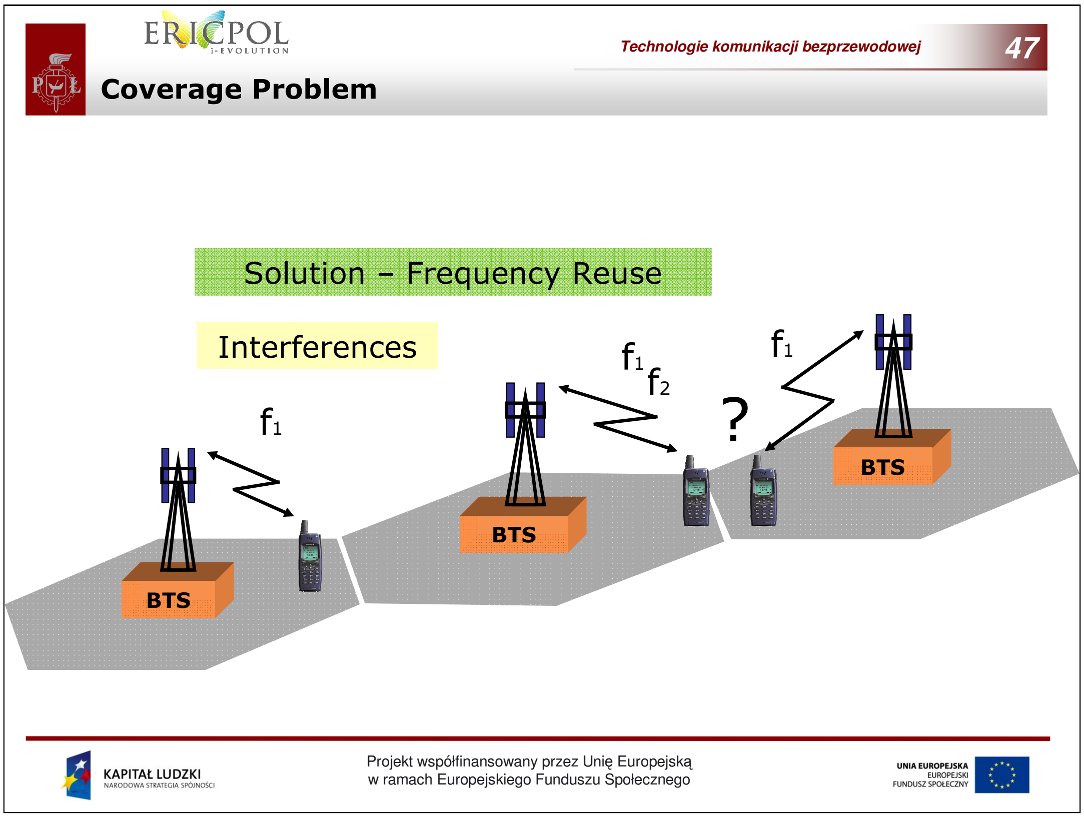
Simplex: f1 (for example radio)



TDMA Solution for GSM

TDMA – Time Division Multiple Access. TDMA is used by most of cellular systems. The idea of TDMA is that one carrier frequency is used by more than one call. Each call has its own period of time when sends or receives signals. This period of time is called time slot. MS has two frequencies assigned. One for transmitting the signal other for receiving the signal. Information sent during one time slot is called a burst.

Note: Clarifying problem of the synchronous and asynchronous TDMA



Coverage Problem

Each company with a license to operate a mobile network has allocated a limited number of frequencies. These are transmitted throughout the cells in their network. Depending on the traffic load and the availability of frequencies, a cell may have one or more frequencies allocated to it. It is important when allocating frequencies that interferences are avoided. Interference may be caused by variety of factors. A common factor is a use of similar frequencies close to each other.

The higher the interface the lower the call quality.

To cover an entire country frequencies must be reused many times at different geographical locations in order to provide a network with sufficient capacity. The same frequencies can not be reused in neighbouring cells as they would interfere with each other. So special patterns of frequency usage are determined during the planning of the network.

These frequency reuse patterns ensure that any frequencies being reused are located at a sufficient distance apart to ensure that there is little interference between them. The term frequency reuse distance is used to describe the distance between two identical frequencies in a reuse pattern.

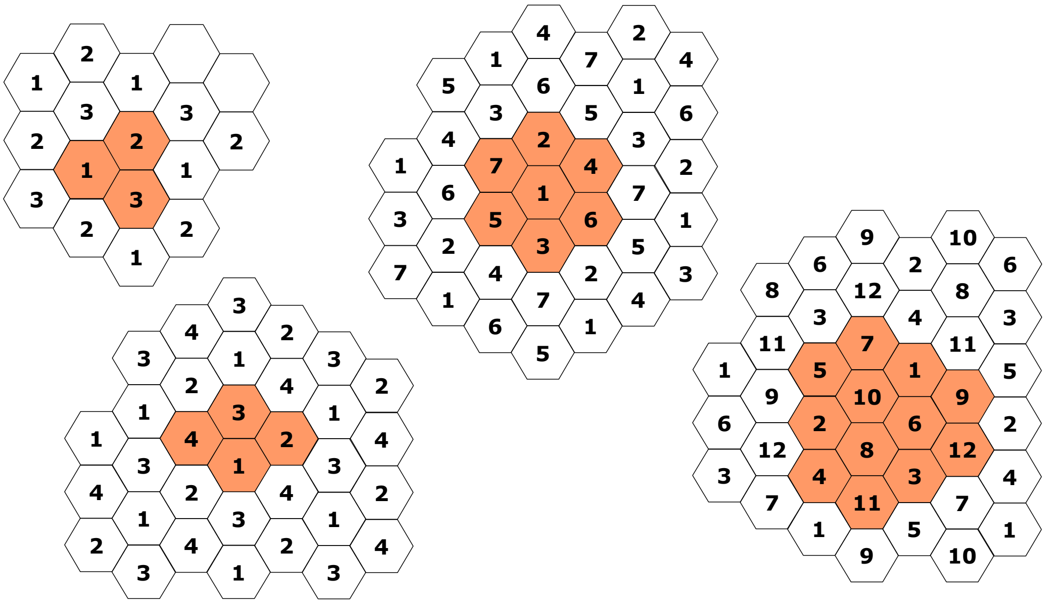
The lower the frequency reuse distance the more capacity available in the network.

Note:

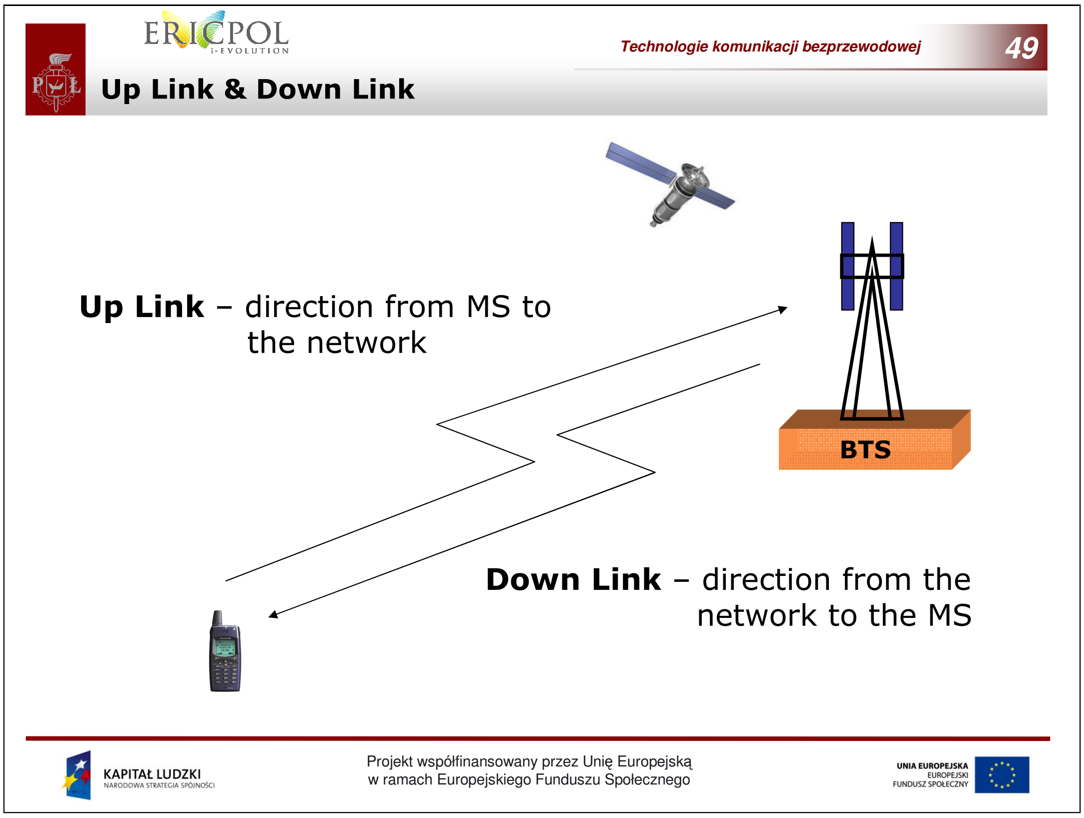
Why hexagonal shape?

It is easy to show drawing several circles which have common areas.

Frequency Reuse Factor



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Up Link & Down Link

Up Link is the direction from the MS to the BTS.

Down Link is the direction from the BTS to the MS.

Note:

Why? Because of the satellite systems and location of the geo stationary satellite transponders.

Channel Concept 1

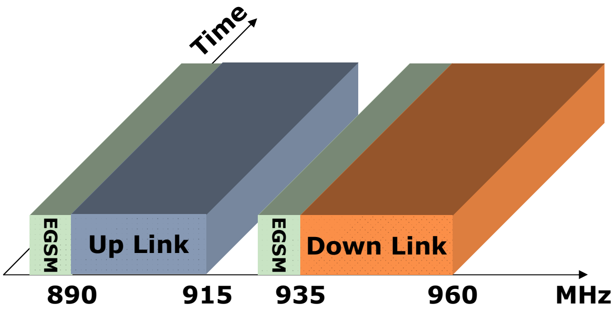
P-GSM 900:

Bandwidth – 25MHz

Duplex Distance – 45MHz

E-GSM 900:

Extra 10 MHz bandwidth



Channel Concept 1

Bandwidth

Is the term used to describe the amount of frequency range allocated to one application.

The direction from the MS to network is referred to as uplink. Direction to the MS is downlink.

Duplex Distance.

The use of full duplex requires that the downlink and uplink transmissions must be separated in frequency by a minimum distance. This is the duplex distance. Without it uplink and downlink transmissions would interfere with each other.

In PGSM900 (Primary GSM900)
Bandwidth 25MHz
Duplex Distance 45 MHz

In EGSM900 (Extended GSM900)
Bandwidth 35 MHz
Duplex Distance 45 MHz

We also have:
GSM1800 (formerly called DCS)
Uplink 1710-1785 MHz
Downlink 1805-1880 MHz
Bandwidth 75MHz
Duplex Distance 95MHz

GSM1900 (also called PCS)
Uplink 1850-1910 MHz
Downlink 1930-1990 MHz
Bandwidth 60MHz
Duplex Distance 80MHz

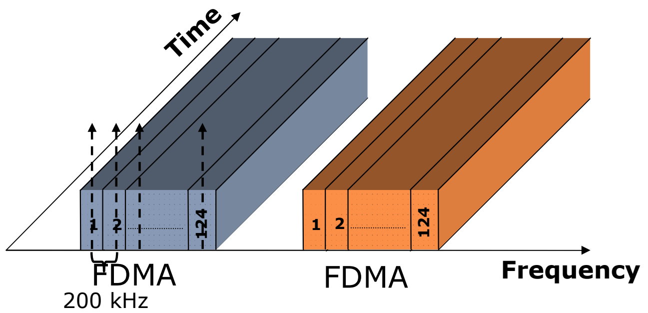
Note:
Why Uplink is 890? Because if the frequency is lower, than the emitted power can be smaller.

Channel Concept 2

ARFCN – Absolute Radio Frequency Channel Number

Carrier separation – 200kHz

P-GSM900 – Radio Channels – 124



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Channel Concept 2

Carrier separation is the distance on the frequency band between channels being transmitted in the same direction. This is required in order to avoid the overlapping of information in one channel into an adjacent channel. The length of separation between two channels is dependent on the amount of information which is to be transmitted within the channel. The greater the amount of information to transmit the greater the amount of separation required.

In PGSM900 there is 25MHz bandwidth divided by 200kHz carrier separation it gives 125 radio channels in each direction. Only 124 channels are used because there is one guard channel in each direction to avoid interferences.

In all GSM systems carrier separation is 200kHz.

What is used on similar frequencies?

•Radiolocation, amateur radio (915-930 MHz)

-Aeronautical radionavigation (960+ MHz)

-Flight safety, navigation (960+ MHz)

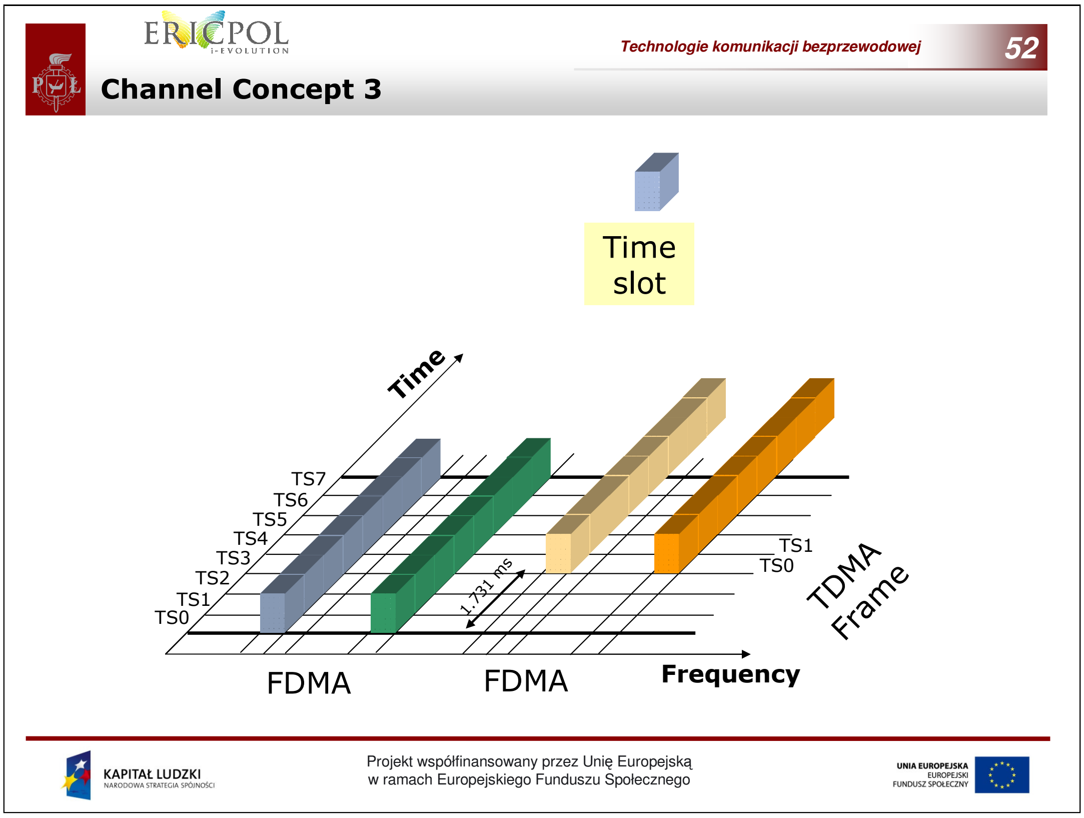
-Defence systems (915-921 MHz)

-UIC Railway systems (921-925 MHz)

-Information Distribution systems (980+ MHz)

http://upload.wikimedia.org/wikipedia/commons/4/45/United_States_Frequency_Allocations_Chart_2003_-_The_Radio_Spectrum.jpg

http://www.onlineconversion.com/downloads/european_frequency_allocations.pdf

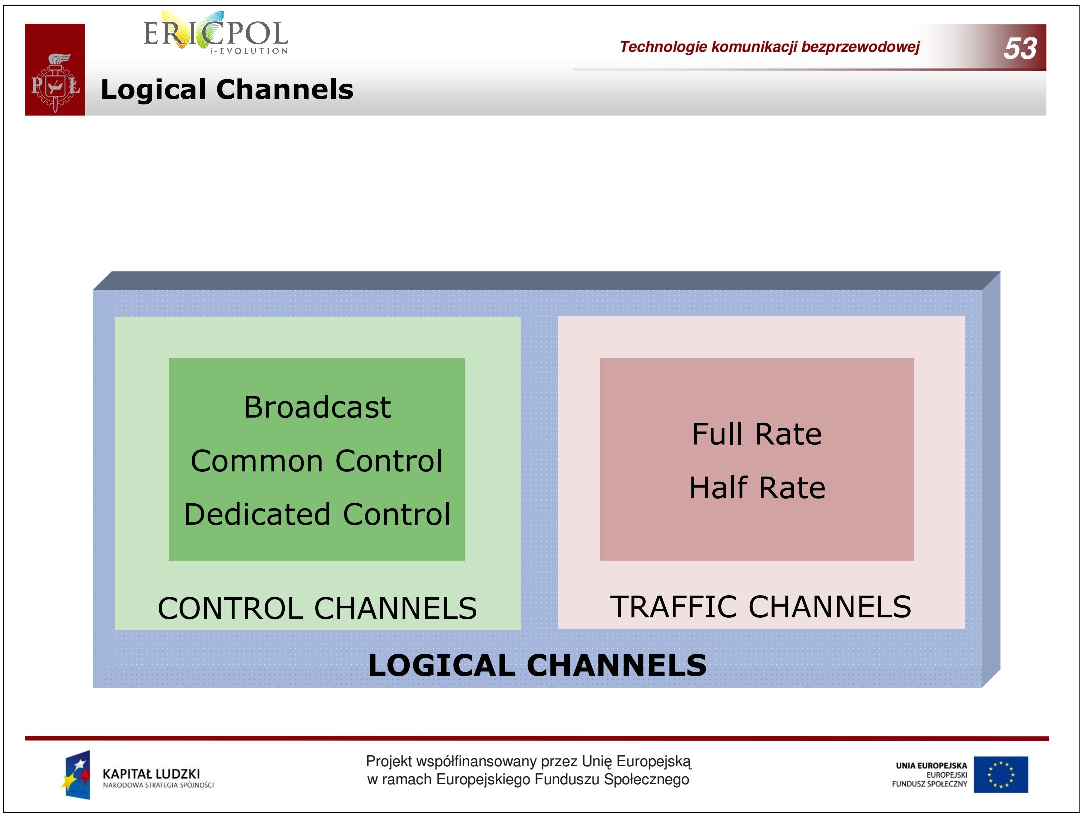


Channel Concept 3

TDMA frame consist of 8 time slot on each carrier (one frequency). The up link and down link time slots are separated in time by 3 time slots. Why? To allow the same TS to be used in uplink and downlink without requiring the MS to transmit in both ways simultaneously.

Note:

This solution appears as a problem when we are using GPRS. That's the reason why in GPRS we can find MS classes. Although in standard's documentation there is described MS which allows to transmit simultaneously in both direction, the most of MS in market can't do this (there are just only one or two models which can do this)



Physical channels can be used to transmit different types of info depending on the needs.

Logical Channels

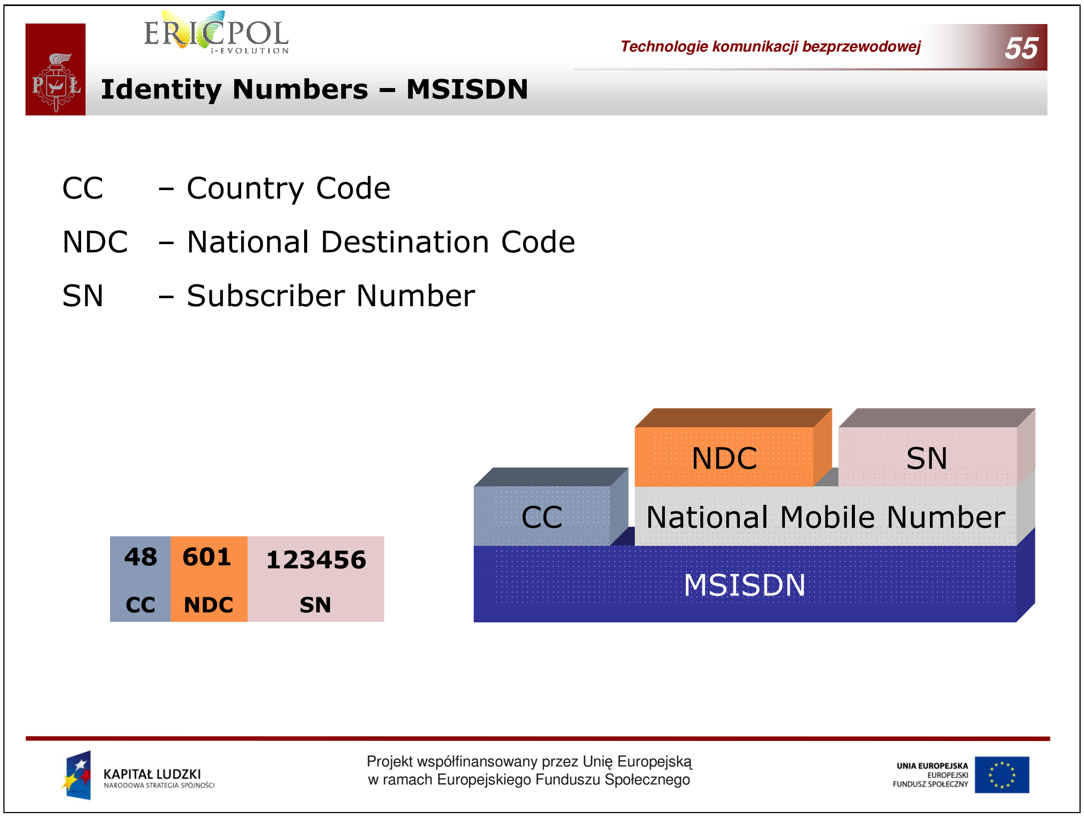
There are many types of logical channels. Each designed to carry different type of information to or from the MS. All information must be formatted correctly so that the receiving device can understand the meaning of different bits in the message. In the burst used to carry traffic some bits represent the speech or traffic while others are used as a training sequence.

Logical Channels may be divided into Control Channels and Traffic Channels. Control Channels are used for transmitting control messages, such as network information. Traffic Channels are used for transferring speech or data.

ID – Numbers

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

ID-Numbers



Mobile Station ISDN Number

MSISDN uniquely identifies a mobile telephone subscription in the PSTN numbering plan. This is the number dialled when calling a mobile subscriber. As the MSISDN is an actual telephone number of mobile subscriber it is the only the network identity that subscribers are aware of. All other network identities are for internal network use and subscribers do not need to be aware of them.

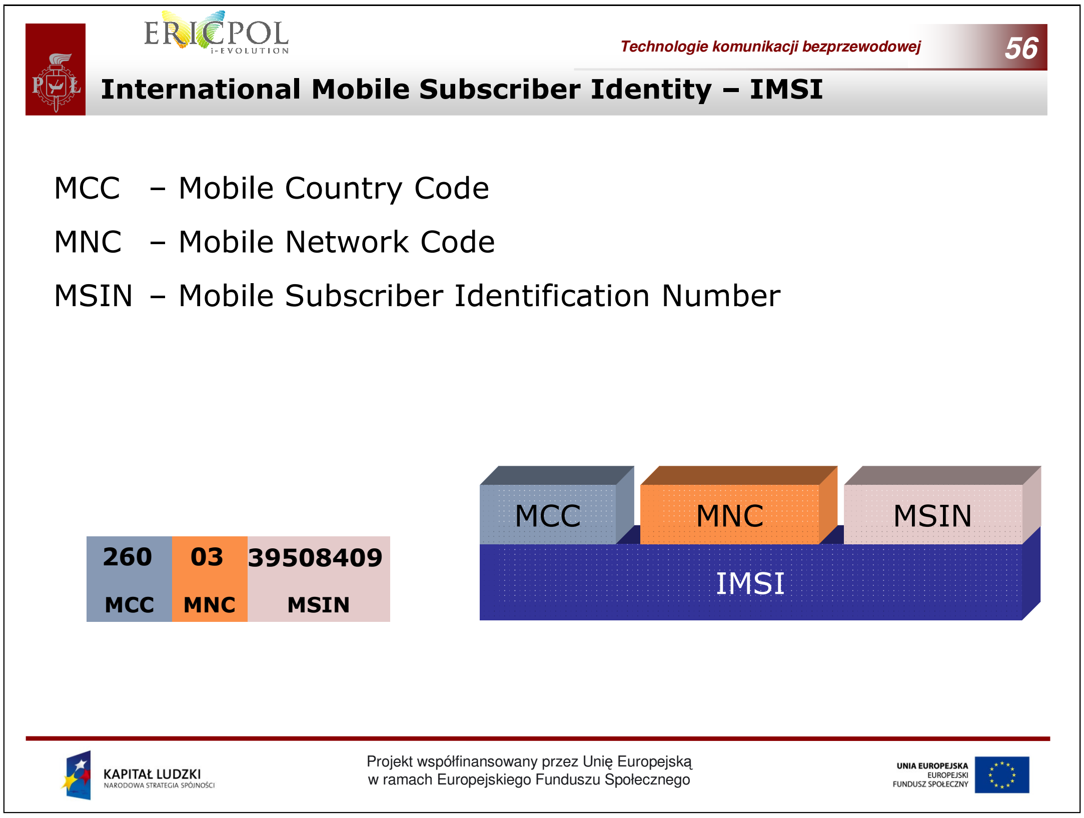
MSISDN consist of Country Code CC, National Destination Code NDC and Subscriber Number SN. An NDC is allocated to each PLMN. In some countries more than one NDC may be required for each PLMN. MSISDN may be variable length. The maximum length is 15 digits, prefixes not included.

Example:

CC 48 polish country code

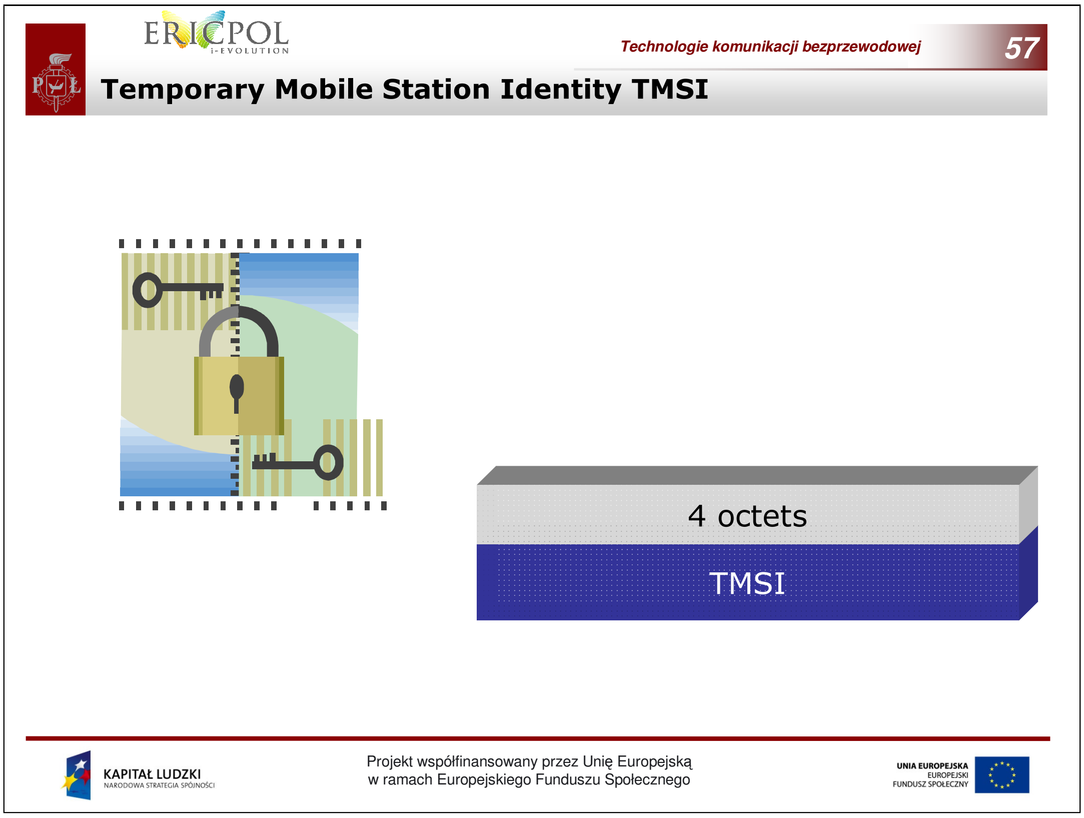
NDC 602 one of polish mobile operators

SN 395084 one of operator's subscriber number



IMSI International Mobile Subscriber Identity

The IMSI is a unique identity allocated to each subscriber which facilitates correct subscriber identification over the radio path and through the network. It is used in signaling in the PLMN. All network related subscriber information is connected to an IMSI. IMSI is stored in SIM card, HLR and serving VLR. IMSI has maximum length of 15 digits.



Temporary Mobile Subscriber Identity TMSI

TMSI is a temporary IMSI number made known to an MS at registration. It is used to protect the subscriber's identity on the air interface. The TMSI has local significance only (within MSC/VLR area). TMSI is changed at time intervals or when certain events occur such as location updating. The TMSI structure can be determined by an operator but should be no longer than 8 digits.

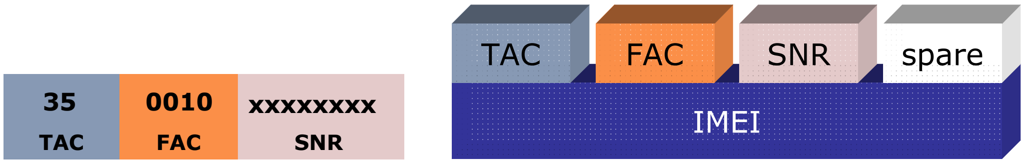
International Mobile Equipment Identity IMEI

TAC – Type Approval Code

FAC – Final Assembly Code

SNR – Serial Number

*#06#



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

IMEI International Mobile Equipment Identity

IMEI is used to uniquely identify MS equipment to the network. The IMEI is used for security procedures such as identifying stolen equipment and unauthorized access to the network. According to GSM specification IMEI has total length of 15 digits.

ERICPOL i-EVOLUTION

Technologie komunikacji bezprzewodowej 59

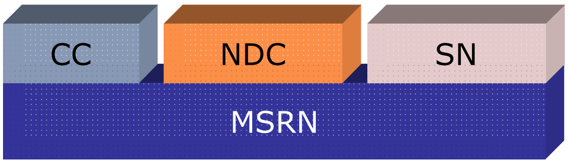
Mobile Station Roaming Number MSRN

CC – Country Code

NDC – National Destination Code

SN – Servicing Number

48	663	426592
CC	NDC	SN



KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego

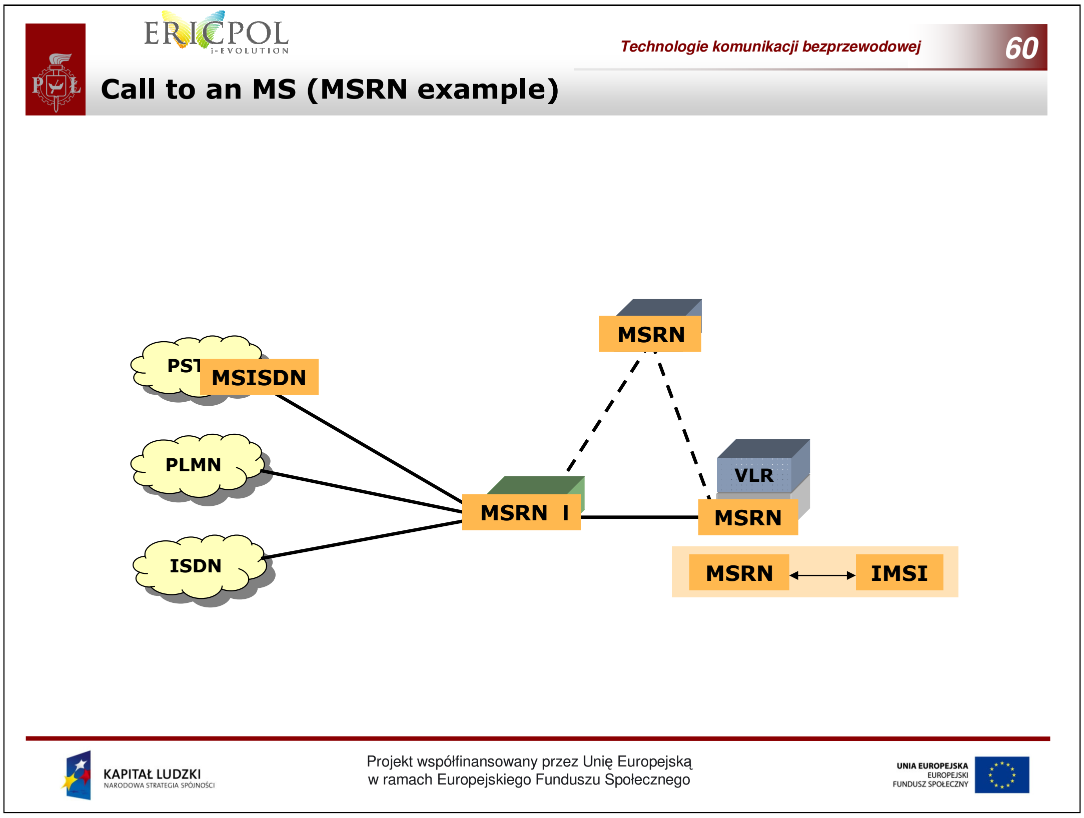
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

MSRN Mobile Station Roaming Number

MSRN is a temporary network identity which is assigned during the establishment of a call to a roaming subscriber.

Is similar to MSISDN number. For Visiting MSC the number is:

VCC+VNDC+SN



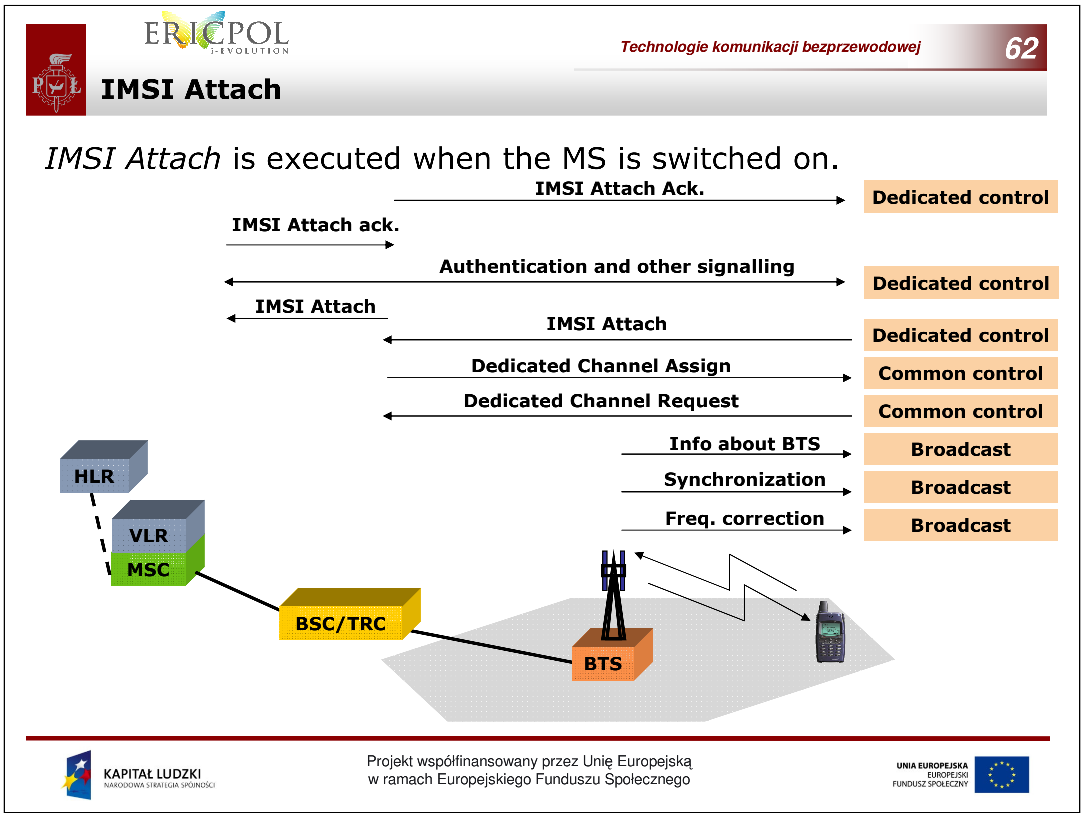
Call to an MS

1. PSTN subscriber dials MSISDN number. MSISDN is analyzed in the PSTN which identifies a call as to a mobile subscriber. A connection is established to subscriber's home GMSC.
2. The GMSC analyzes MSISDN to find out which HLR the MS is registered in. The GMSC queries the HLR for information about how to route the call to the serving MSC/VLR.
3. The HLR translates MSISDN to IMSI and determines which MSC/VLR currently is serving the MS.
4. The HLR requests an MSRN from serving MSC/VLR.
5. The MSC/VLR returns MSRN to GMSC via HLR.
6. The GMSC analyzes the MSRN and routes the call to serving MSC/VLR.
7. The MS is paged using IMSI or TMSI.

Traffic Cases

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

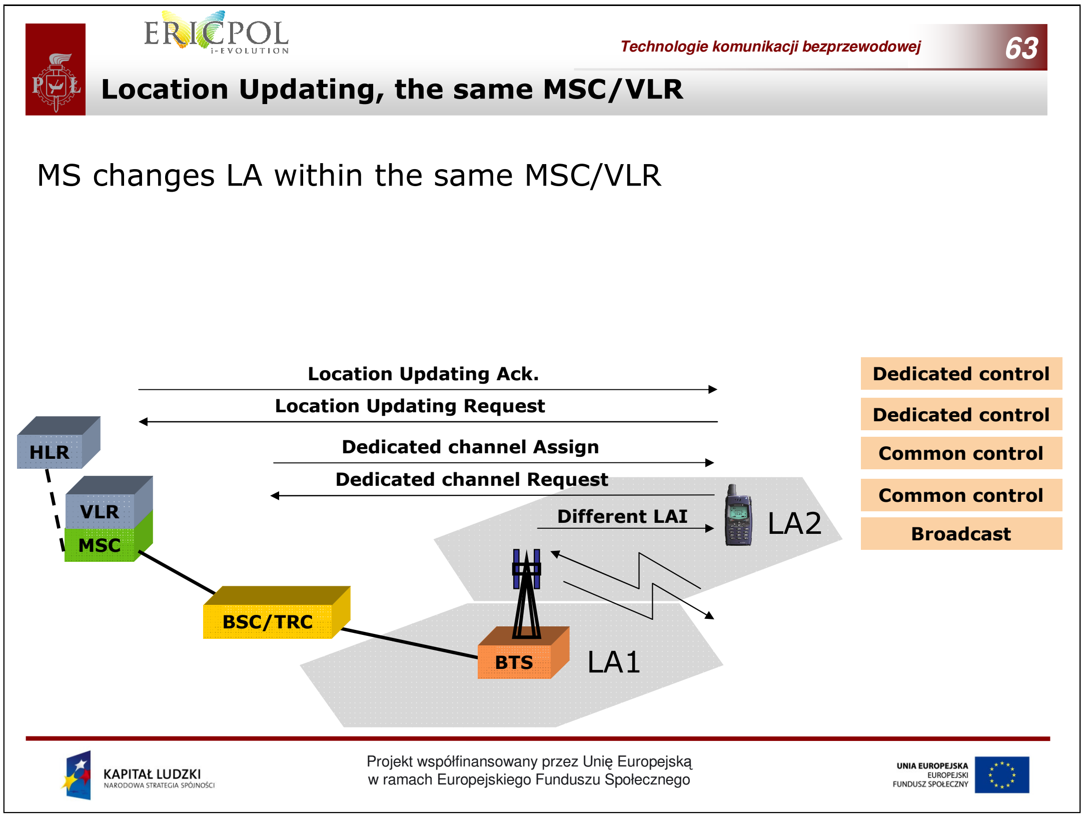
Examples of most typical traffic cases



IMSI Attach

IMSI Attach procedure is performed when MS is switched on. Procedure consists of following:

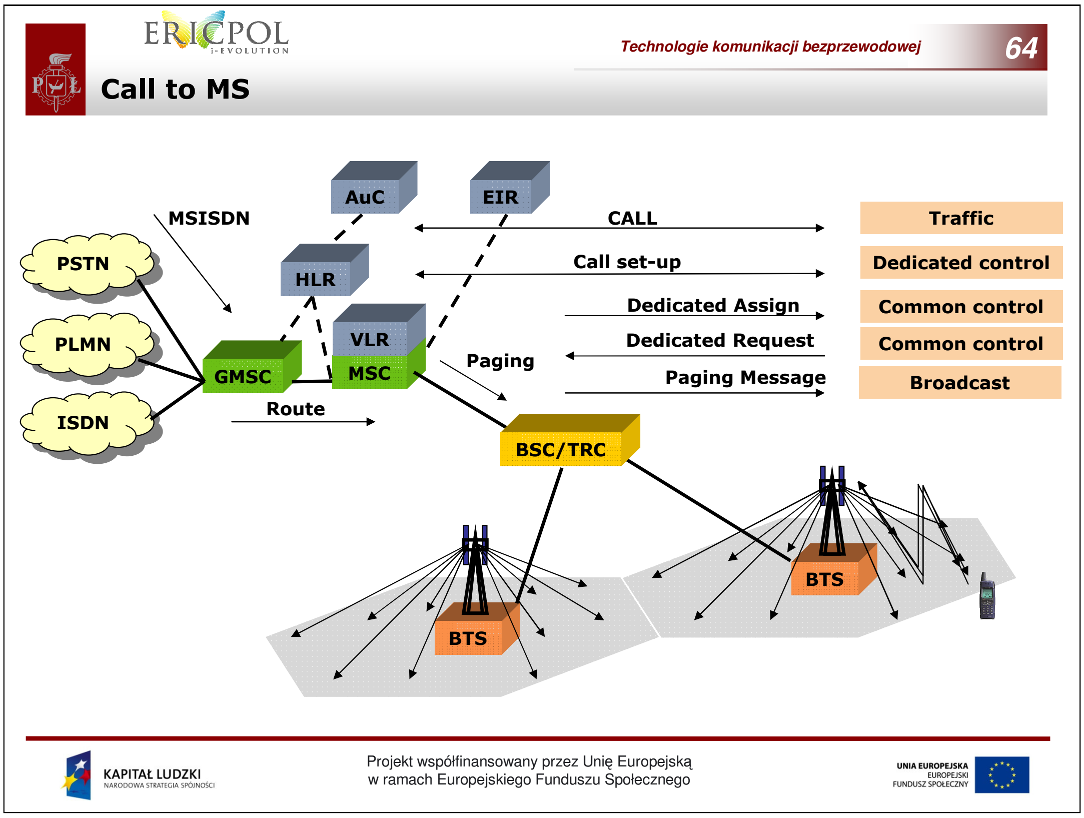
1. MS sends request for signalling channel via common control channel.
2. MS gets signalling channel assignment via common control channel.
3. MS transmits an IMSI attach message to the network via dedicated control channel.
4. VLR determines if it has records of MS subscription. If not VLR receives subscription information from HLR.
5. VLR updates MS status to IDLE.
6. MS get acknowledgment message via dedicated control channel.



Location Updating, same MSC/VLR

Location Updating within the same MSC/VLR involves following steps:

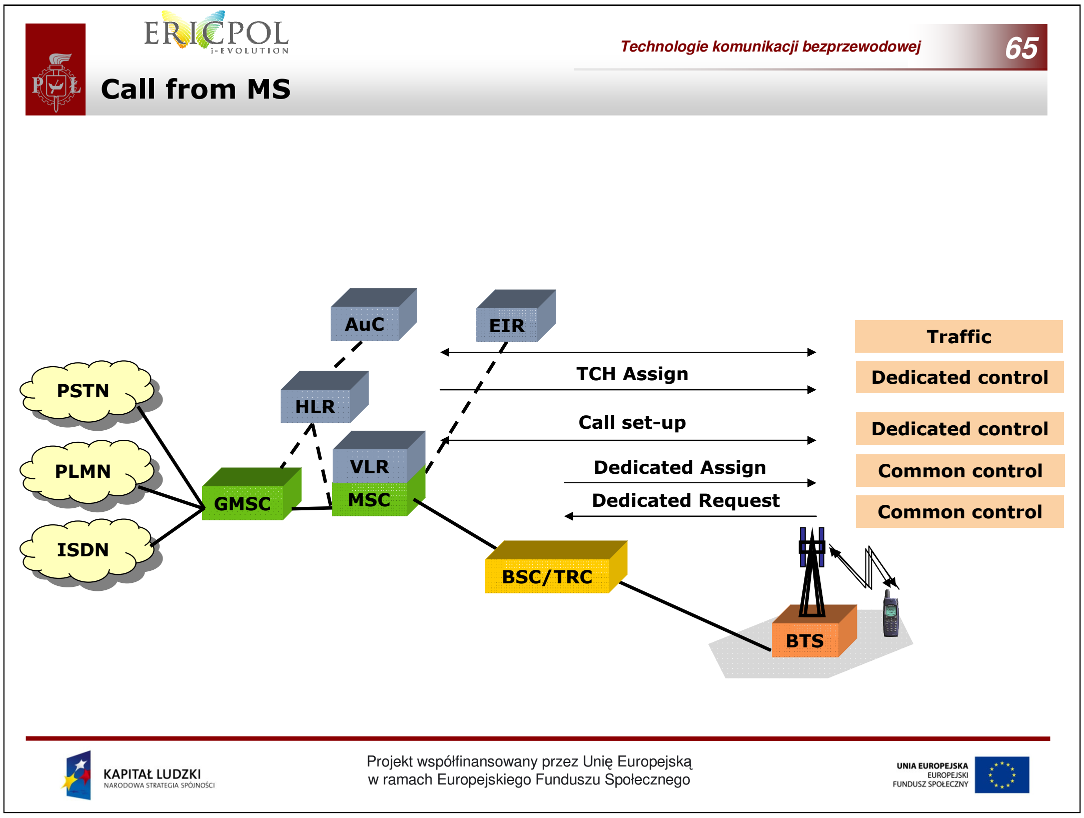
1. MS listens on broadcast channels of new cell to determine LAI. If new LAI differs from old one Location Updating is necessary.
2. MS sends signalling channel request message on common control channel. It gets the channel on other common control channel.
3. MS connects to network via dedicated control channel. Authentication is performed.
4. MS sends Location Updating Request via dedicated control channel if authentication is successful. MSC/VLR determines that the MS is already registered.
5. System acknowledges Location Updating via dedicated control channel and requests BTS to release dedicated control channel.



Call to a MS

MS terminated call from PSTN has following process:

1. PSTN subscriber enters MSISDN number. Number is analyzed in PSTN which identifies that the call is to mobile network subscriber. A connection to MS's home GMSC is established.
2. The GMSC analyzes the MSISDN to find out which HLR the MS is registered in. GMSC queries HLR for information about how to route the call to the serving MSC/VLR.
3. The HLR translates MSISDN into IMSI and determines which MSC/VLR is currently serving the MS. The HLR also checks the service „Call forwarding to C-number". If the service is activated, the call is rerouted by the GMSC to that number.
4. The HLR requests an MSRN from serving MSC/VLR.
5. The MSC/VLR returns an MSRN via HLR to the GMSC.
6. The GMSC analyzes the MSRN and routes the call to the MSC/VLR.
7. The MSC/VLR knows which LA the MS is located in. A paging message is sent to the BSCs controlling LA.
8. BSCs distribute the paging message to BTSs in the desired LA. BTSs transmit paging message over the air interface using PCH (Paging Channel) . IMSI or TMSI is used to page the MS but numbers are only valid within current MSC/VLR service area.
9. When MS detects paging message it sends request for a dedicated control channel via common control channel.
10. The BSC provides dedicated control channel using common control channel.
11. Dedicated control channel is using in call set-up procedures. When traffic is allocated dedicated control channel is released.
12. MS rings. When subscriber answers connection is established.



Call from a MS

MS originated call has following steps:

1. The MS uses common control channel to ask for signalling channel.
2. The BSC allocates dedicated control channel and informs MS about it via common control channel.
3. The MS sends a call set-up request via dedicated control channel to the MSC/VLR. All signalling preceding a call takes place over dedicated control channel.
    1. MS is marked ACTIVE in the VLR.
    2. The authentication procedure takes place.
    3. Ciphering equipment identification starts.
    4. B-subscriber number is sent to the network.
    5. Checking if the subscriber has the service „Barring of outgoing calls" activated.
4. The MSC/VLR instructs the BSC to allocate an idle traffic channel. The BTS and MS tune to the traffic channel.
5. The MSC/VLR forwards the B-number to the exchange in the PSTN which establishes a connection to the subscriber.
6. When B-subscriber answers connection is established.

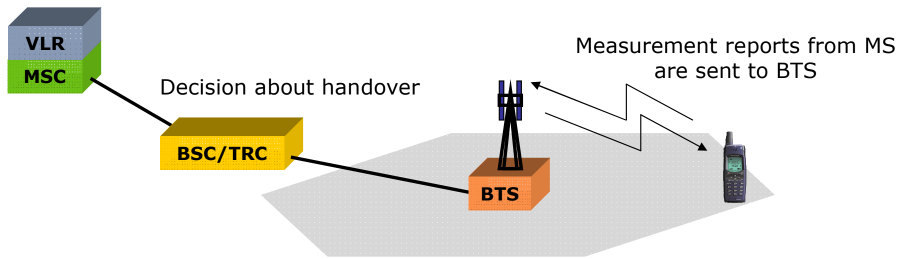
Measurements

BTS measures:

- Signal strength
- Transmission quality on TCH up link

MS measures:

- Signal strength
- Transmission quality on TCH down link



Measurement reports from MS and BTS

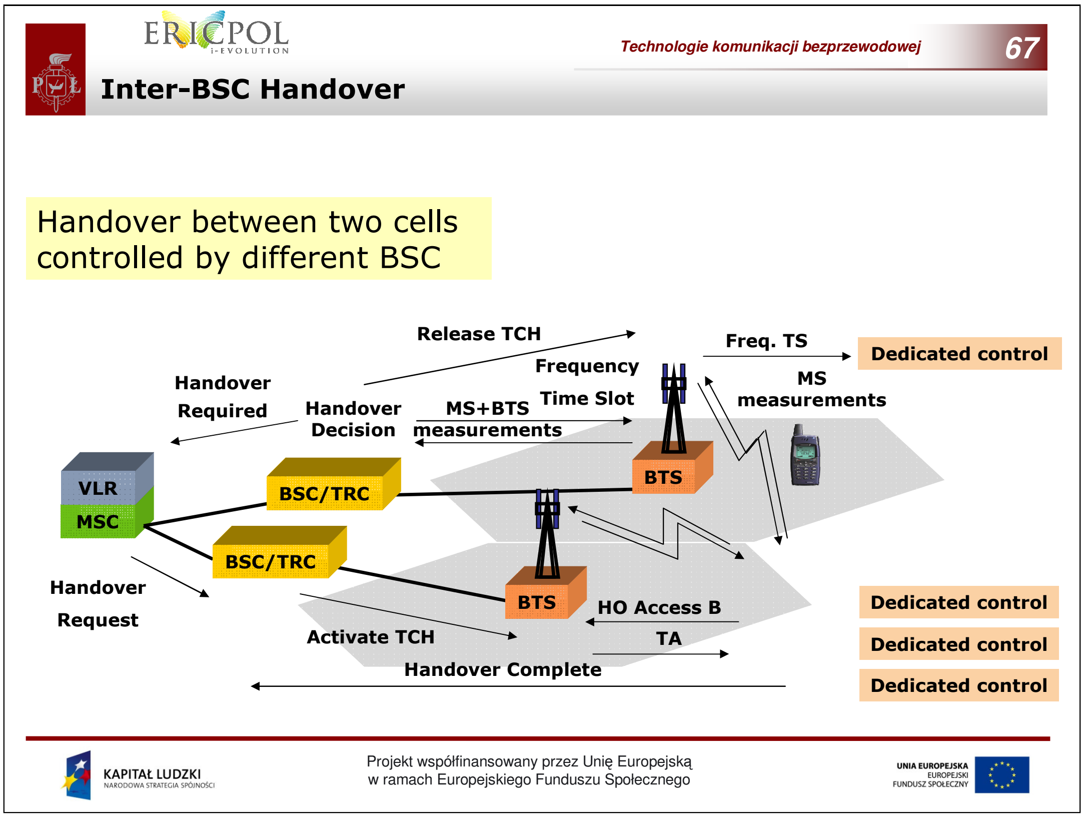
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Locating

Handover – a process of changing cells **DURING THE CALL**.

To choose the best target cell measurements are performed by the MS and the BTS. Handover is often called MAHO Mobile Associated Handover.

Note: Decision about Handover can be taken on the basics of the too high Time Advance of the MS (Signal power and signal quality can be good enough).



Inter-BSC Handover

If the MS moves to an area covered by a cell belonging to another BSC and a handover is required, an inter-BSC handover takes place. within the same MSC.

1. The old BSC has taken the decision, based on the measurement reports, that a call should be handed over to the cell belonging to the new BSC. The serving (old) BSC sends a handover-required message to the MSC, with the identity of the new cell.

2. The MSC knows which BSC controls the BTS and sends a handover request to this BSC.

3. The new BSC now orders the BTS to activate a traffic channel, if there is one that is idle.

4. When the BTS has activated the traffic channel, the new BSC sends information about the time slot, frequency, and output power to the MSC.

5. The MSC passes this information on to the old BSC.

6. The MS is told to change to the new traffic channel via dedicated control channel.

7. The MS sends a handover burst on the new dedicated control channel.

8. As soon as the BTS detects the handover bursts, it sends physical information which contains timing advance and output power to the MS via dedicated control channel.

9. The new BSC confirms that the BTS has received the handover bursts.

10. This information is passed on to the MSC by the BSC, which changes the path in the Group Switch (GS).

11. The MSC informs the old BSC that the old traffic channel is no longer required.

12. The old traffic channel is deactivated in the BTS.

If the cell belongs to a new LAI (Location Area Identity), the MS must perform a normal location update after the call is released.

Sum-up

- GSM History and services
- GSM Structure
- Radio Interface
- ID - Numbers
- Traffic Cases

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Any questions?

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Thank you for your attention.

Aleksandra Chećko, BDTR
Ericpol Telecom Sp. z o.o.
Aleksandra.Checko@ericpol.pl
Tel.: +48 42 664 2434

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

„Technologie komunikacji bezprzewodowej"
„Technologia GSM"

Prezentacja jest współfinansowana przez
Unię Europejską w ramach
Europejskiego Funduszu Społecznego w projekcie pt.

„Innowacyjna dydaktyka bez ograniczeń - zintegrowany rozwój Politechniki Łódzkiej - zarządzanie Uczelnią, nowoczesna oferta edukacyjna i wzmacniania zdolności do zatrudniania osób niepełnosprawnych"

Prezentacja dystrybuowana jest bezpłatnie

Politechnika Łódzka

Politechnika Łódzka, ul. Żeromskiego 116, 90-924 Łódź, tel. (042) 631 28 83
www.kapitalludzki.p.lodz.pl