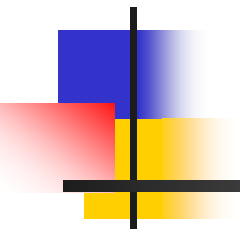
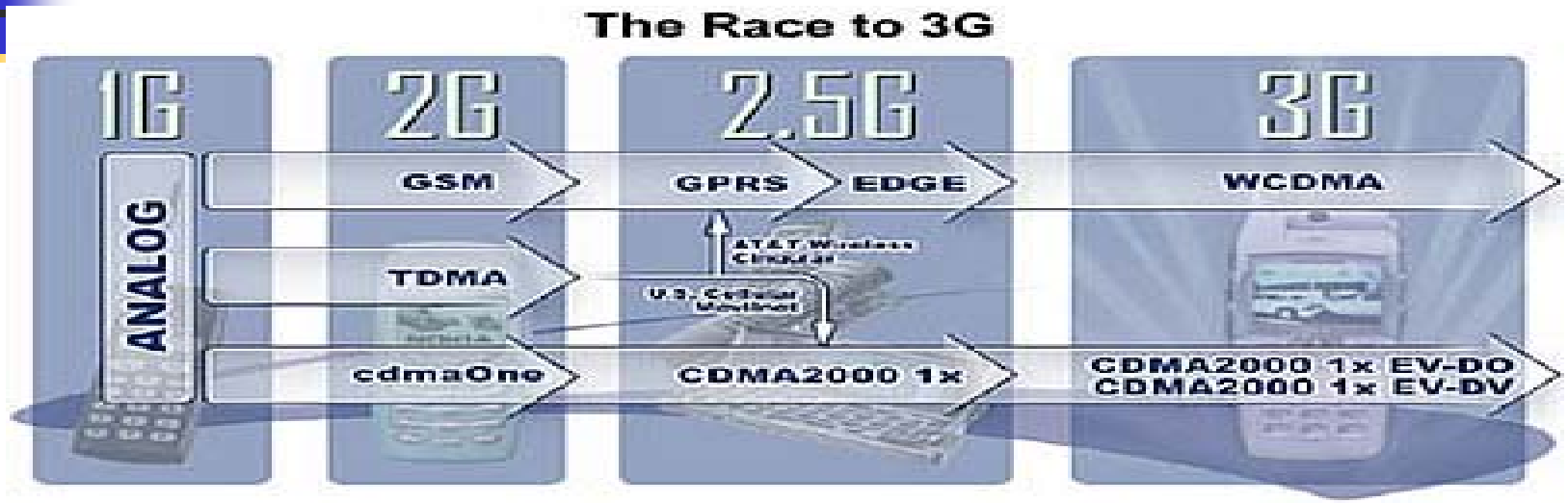


UMTSC

IMT-2000

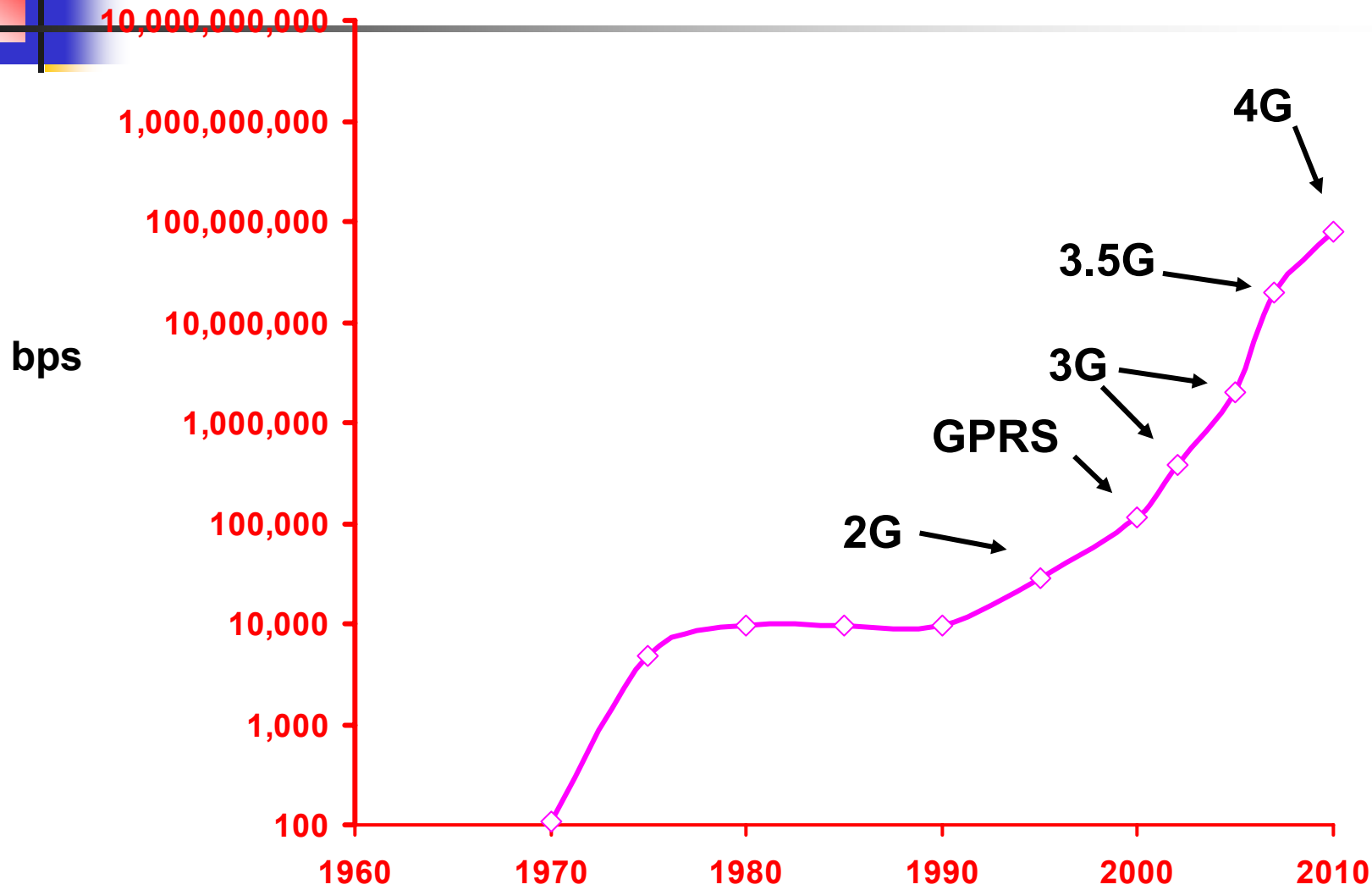
- **The International Telecommunications Union-Radio communications** (ITU-R) opracowało specyfikacje systemu 3G, mające na celu ułatwienie stworzenia globalnej bezprzewodowej infrastruktury obejmującej naziemne i sateliterne systemy zapewniającej trwały mobilny dostęp do sieci publicznych i prywatnych
- IMT-2000 jest ogólną nazwą dla wszystkich systemów 3G
- Włącza on nowe możliwości oraz zapewnia ewolucyjne przejście z istniejących bezprzewodowych systemów 2G

Droga do 3G



- 1G: analogowa
- 2G : 1-sza cyfrowa mobilna telefonia
- 2.5G: przejście od 2G do 3G
- 3G standard: IMT-2000

3G & Przyszłe Systemy Bezprzewodowe



IMT-2000

- Kluczowe własności
- Alokacja międzynarodowego spektrum
- Radiowe interfejsy
- Harmonizowane systemy 3G
- UMTS
- UTRAN, USRAN
- Kanały w UTRAN

3G: oczekiwania

- Ulepszona cyfrowa komunikacja głosowa
- Większe spektrum – wieksza prędkość transmisji danych
- Szybkie usługi oparte na transmisji pakietów, takie e-mail, SMS i szerokopasmowy dostęp do Internetu
- Sądzi się też, że abonenci będą oczekiwać:
  - Usług lokalizacyjnych
  - Interaktywnych gier
  - Video na żądanie
  - Monitorowanie mieszkań i domów
  - Oraz prawdopodobnie wielu innych rzeczy

Kluczowe własności

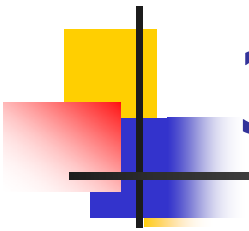
- Wysoki stopień podobieństwa rozwiązań konstrukcyjnych na całym świecie
- Kompatybilność usług w IMT-2000 oraz w stałych sieciach
- Wysoka jakość
- Mały terminal do używania na całym świecie, bez względu na to czy są to komórki pico, micro, macro, czy satelitarne
- Możliwości roamingu na całym świecie
- Możliwości aplikacji multimedialnych oraz szeroki zakres usług i terminali

3G: oferowane usługi

- Jakość głosu porównywalna do jakości oferowanej prze publiczną sieć telefoniczną
- 144 Kbits - użytkownicy szybkiego ruchu samochodowego
- 384 Kbits - piesi lub wolno poruszający się na małych obszarach
- Aż do 2 Mbits- stałe zastosowania, jak np. w biurze
- Symetryczna/asymetryczna transmisja danych
- Realizacja serwisów opartych zarówno na transmisji danych jak i komutacji pakietów jak też komutacji obwodów, takich jak ruch sieciowy oparty na Internet Protocol (IP) czy wideo w czasie rzeczywistym

Technologie (standardy)

- 3G ma znaczną przewagę nad innymi cyfrowymi standardami, takimi jak:
  - GSM (Global System for Mobile)
  - czy IS-136 TDMA używanym przede wszystkim w Ameryce Północnej
- Technologie 3G:-
  - WCDMA or UMTS-FDD (Universal Mobile Telecommunications System - Frequency Division Duplex)---Direct Spread
  - cdma2000 - 1x-EvDO/EvDV---Multi carrier
  - UMTS – TDD (Time Division Duplex) or TD-SCDMA (Time Division - Synchronous Code Division Multiple Access) ---Time Code
- Technologie 4G:
  - Digital Audio Broadcast (DAB) and Digital Video Broadcast (DVB) for wide area broadcasting
  - Local Multipoint Distribution System (LMDS)
  - Microwave Multipoint Distribution System (MMDS)



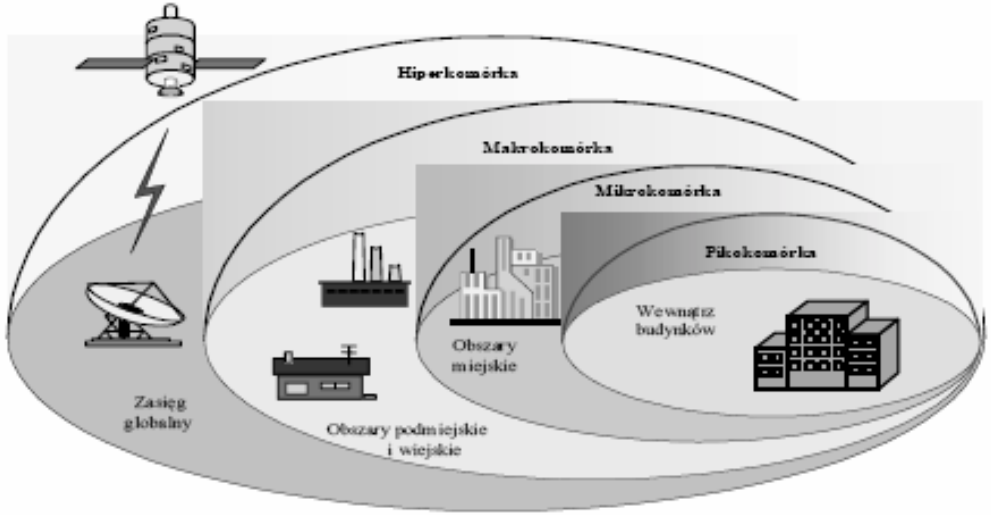
3G: standardy

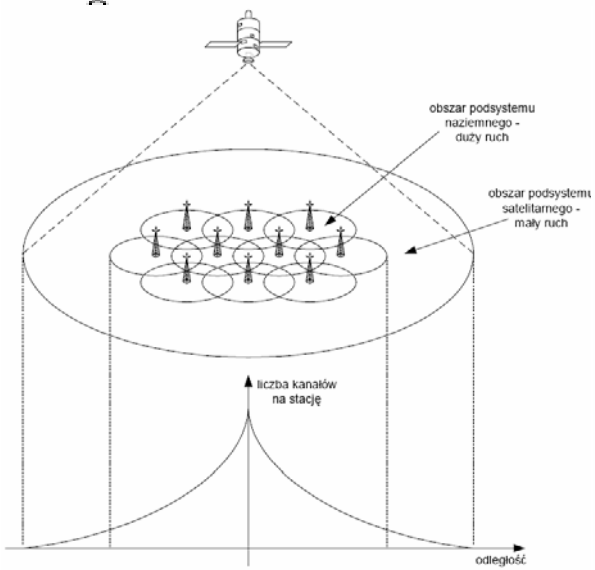
- Standardy
  - Europa: UMTS (Universal Mobile Telecommunications System) (W-CDMA)
  - Japonia: W-CDMA
  - USA: cdma2000

Środowisko pracy systemu UMTS

Koncepcja obsługi użytkowników w róż nych klasach komórek o zróżnicowanych zasięgach:

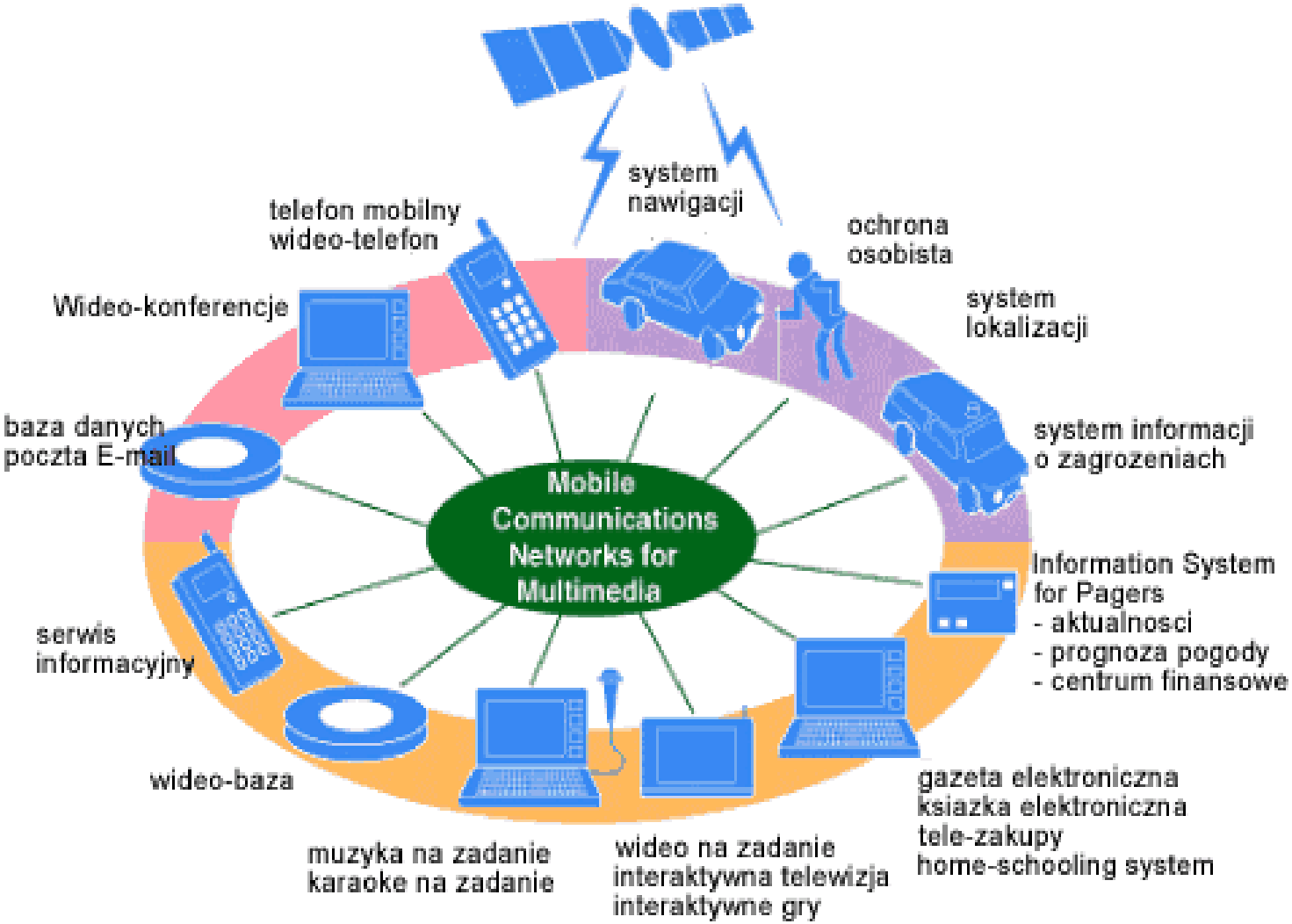
- **segment naziemny** - wnętrza budynków, obszary miejskie, podmiejskie i wiejskie.
- **segment satelitarny** - morza, oceany, pustynie, góry oraz tych, obszary bez lub słabo rozwiniętaną telekomunikacyjną



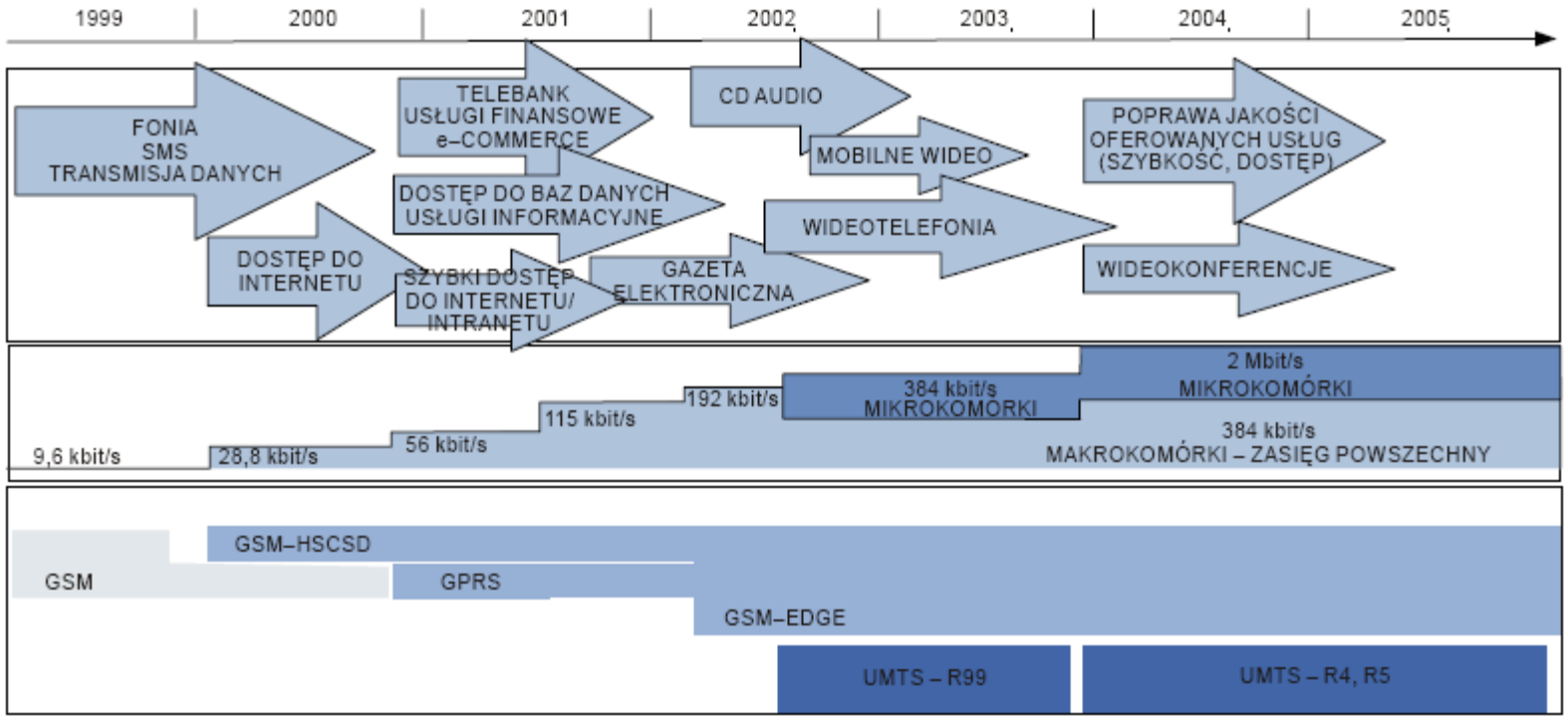


Klasa komórki	Promień komórki	Prędkość stacji ruchomej	Szybkość transmisji	Dostępność usług
Pikokomórka (wnętrza obiektów biurowych, obiekty handlowe)	< 100 m	< 10 km/h	< 2 Mb/s	Wszystkie
Mikrokomórka (tereny miejskie z dużymi skupiskami ludności)	< 1 km	120 km/h	< 512 kb/s	Liczny podzbiór
Makrokomórka (tereny wiejskie i miejskie z niewielkimi skupiskami ludności)	< 10 km	< 500 km/h	< 384 kb/s	Usługi podstawowe
Hiperkomórka (obszary mórz, oceanów oraz lądy, w tym również obszary górzyste i pustynie)	300 – 800 km (satelity LEO, MEO) 4000 – 5000 km (satelity GEO)	< 1000 km/h (samoloty)	< 144 kb/s	Usługi podstawowe

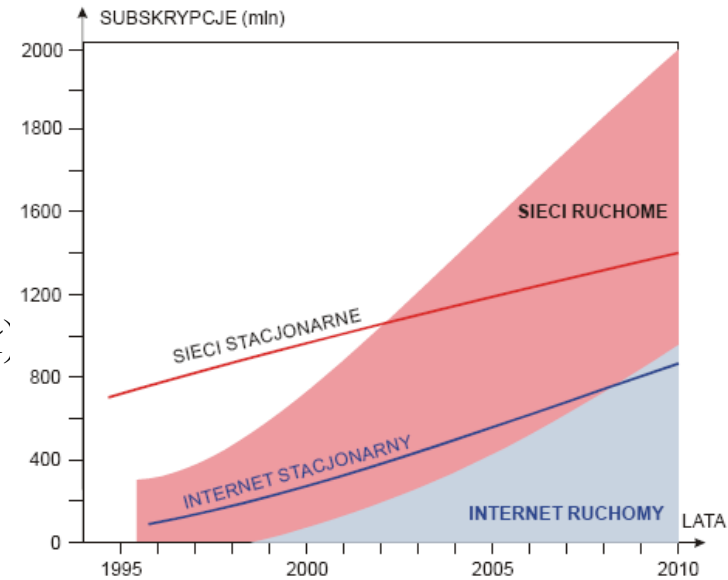
3G: integracja dotychczasowych systemów komunikacji mobilnej



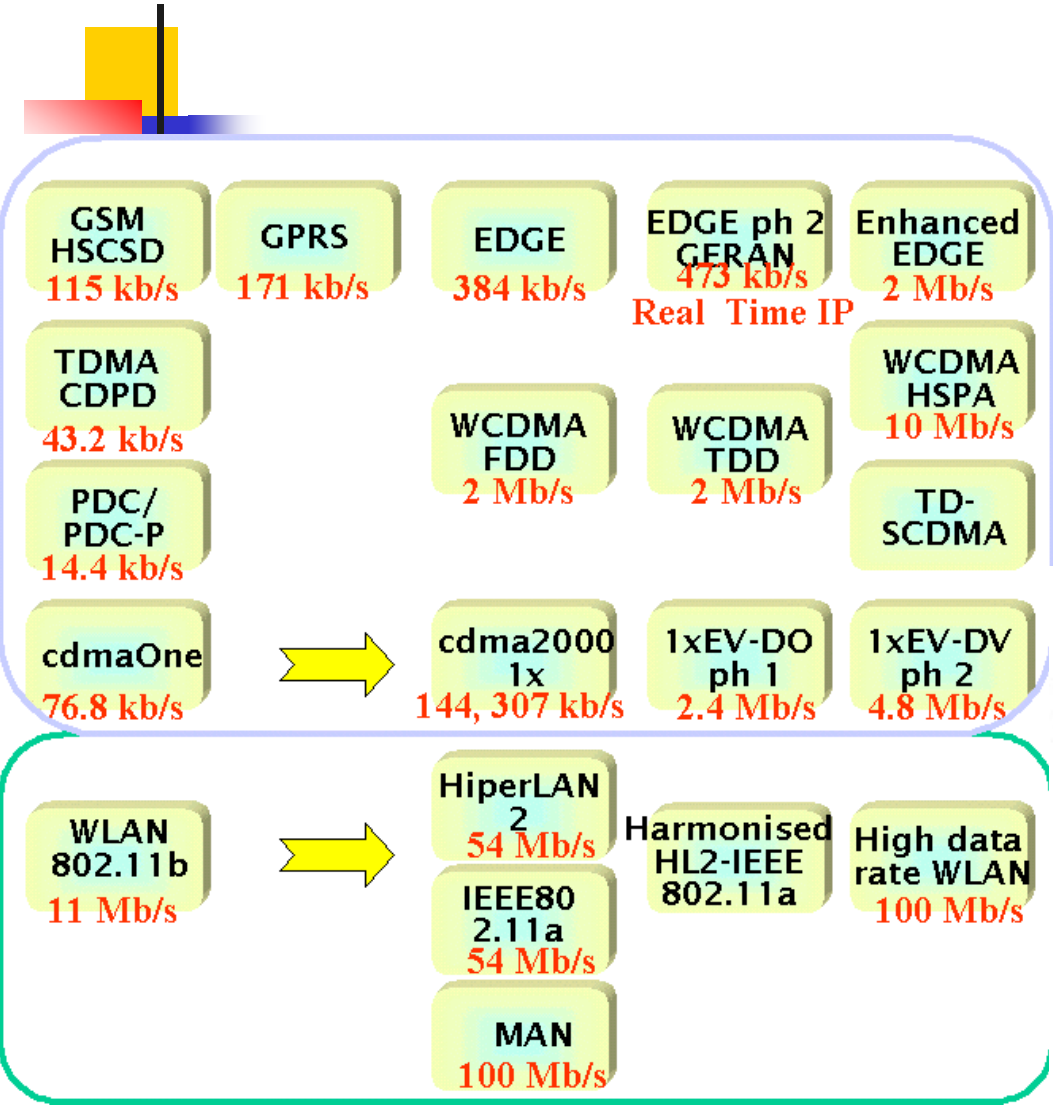
Rozwój nowych usług



- informacja i rozrywka dla danego terenu
- mobilne biuro (e-maile, wideo-konferencje, sprzedaż)
- bezprzewodowy dom (obsługa i monitoring)
- samochód w łączności ze światem (aktualne inf. na drodze)
- usługi lokalizacyjne (GPS, sprawniejsza nawigacja)
- dynamiczna selekcja i definiowanie profilu usług,
- zdalne zamawianie produktów i usług (reklamy, szyb.przesył)
- m-banking (płatności poprzez terminale)
- „mikropłatności” (połączenia interaktywne, bezpieczeństwo, personalizacja)

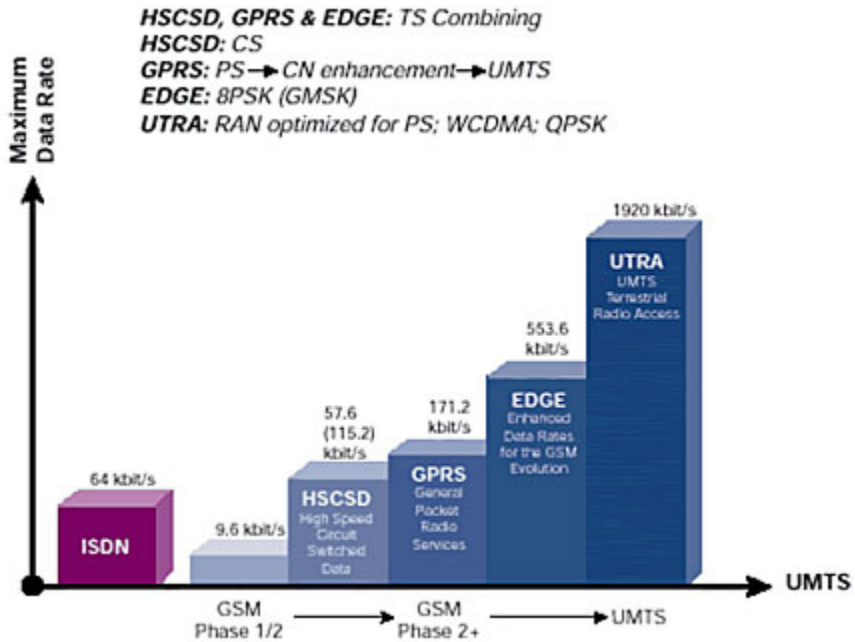


Szybkości transmisji w 2.5G i 3G



Szybka transmisja Danych
(3G Internet)

W technikach szerokopasmowe (WCDMA) CDMA (Code Division Multiple Access) i TDMA (Time Division Multiple Access) Taki typ interfejsu radiowego umożliwia przyznanie całego dostępnego pasma każdej z komórek sieci, bez konieczność rozdziału częstotliwości między komórki (i ograniczenia detalicznego transferu). Każdy użytkownik otrzymuje indyw.kod (kodowy ciąg rozpraszający)



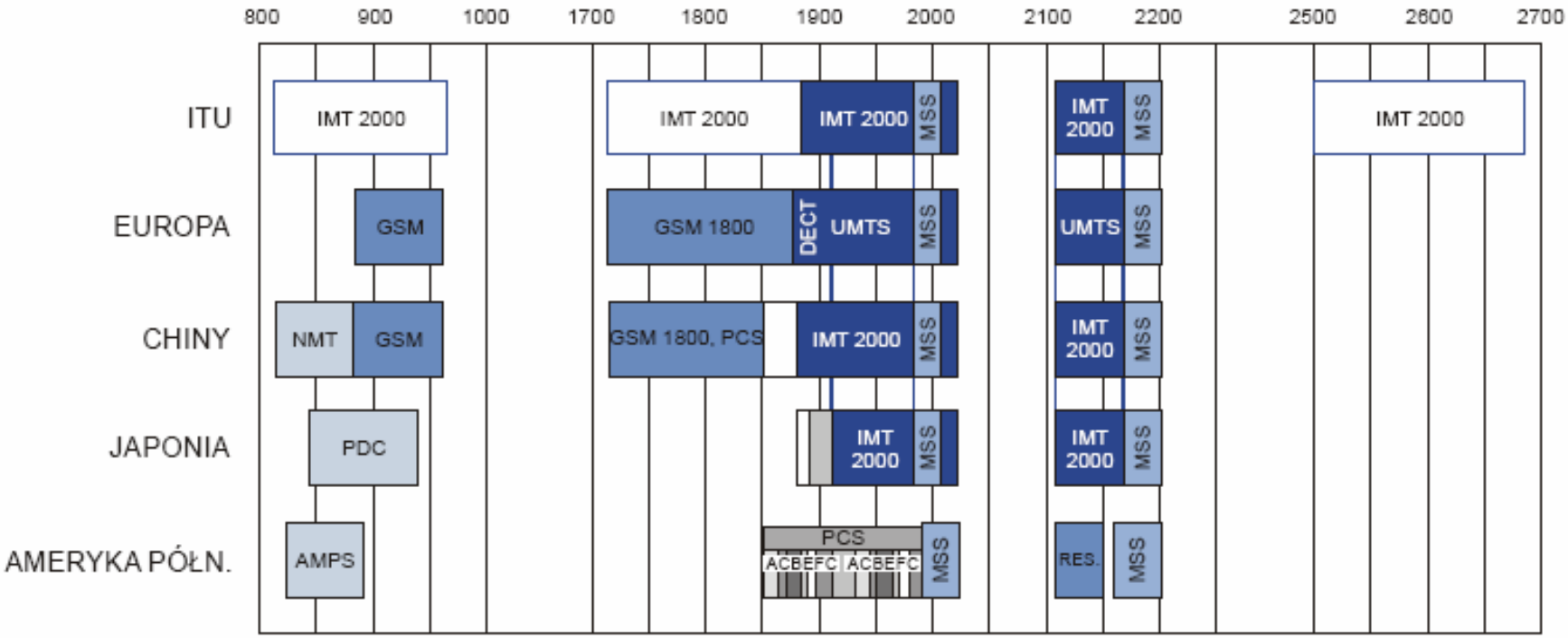
Alokacja międzynarodowego spektrum (ITU-R)

- Zakresy podstawowe:
  - 1885 – 2025 MHz i 2110 – 2200 MHz (1992 r)
  - 1920 – 1980 MHz i 2110 – 2170 MHz w trybie FDD
  - 1885 – 1920 MHz i 2010 – 2025 MHz w trybie TDD
- Rozszerzenia zakresów (2000 r)
  - Te, które ustalono w 1992 r
  - Używane zakresy 2 G (w tym GSM 900, 1800, i 1900) oraz 698-806 MHz, 2500-2690 i 2700-2900 od 2005 r

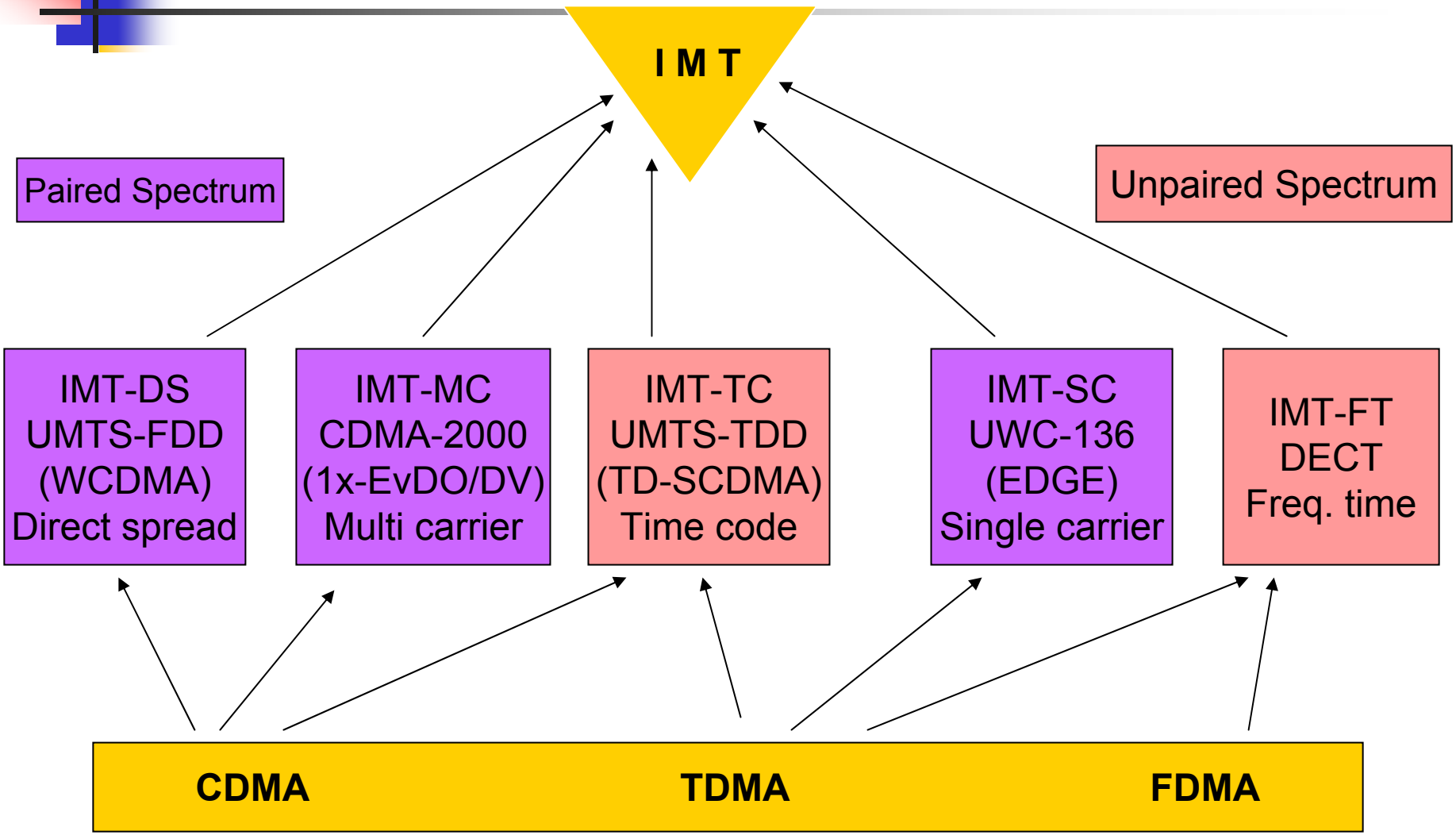
Alokacja międzynarodowego spektrum

- Obecnie nie ma jednego ustalonego, powszechnie dostępnego spektrum dla 3G; jest to kwestią negocjacji
- Raczej kilka zakresów niż jeden
- Ze względów praktycznych < 3GHz (2000 r); 5, 7 GHz (2003 r)
- Proponowane zakresy:
  - USA: 698-960 MHZ, 1710-1885 MHz, 2500-2690 MHz
  - Kraje Azji i Pacyfiku – podobnie jak USA
  - Ameryka Centralna i Południowa: 2,5 GHz, 1.7 GHz
  - Kanada: 1.7 GHz
- Europa: rozpatruje mozliwość zwrotu szeregu używanych zakresów

Alokacja międzynarodowego spektrum



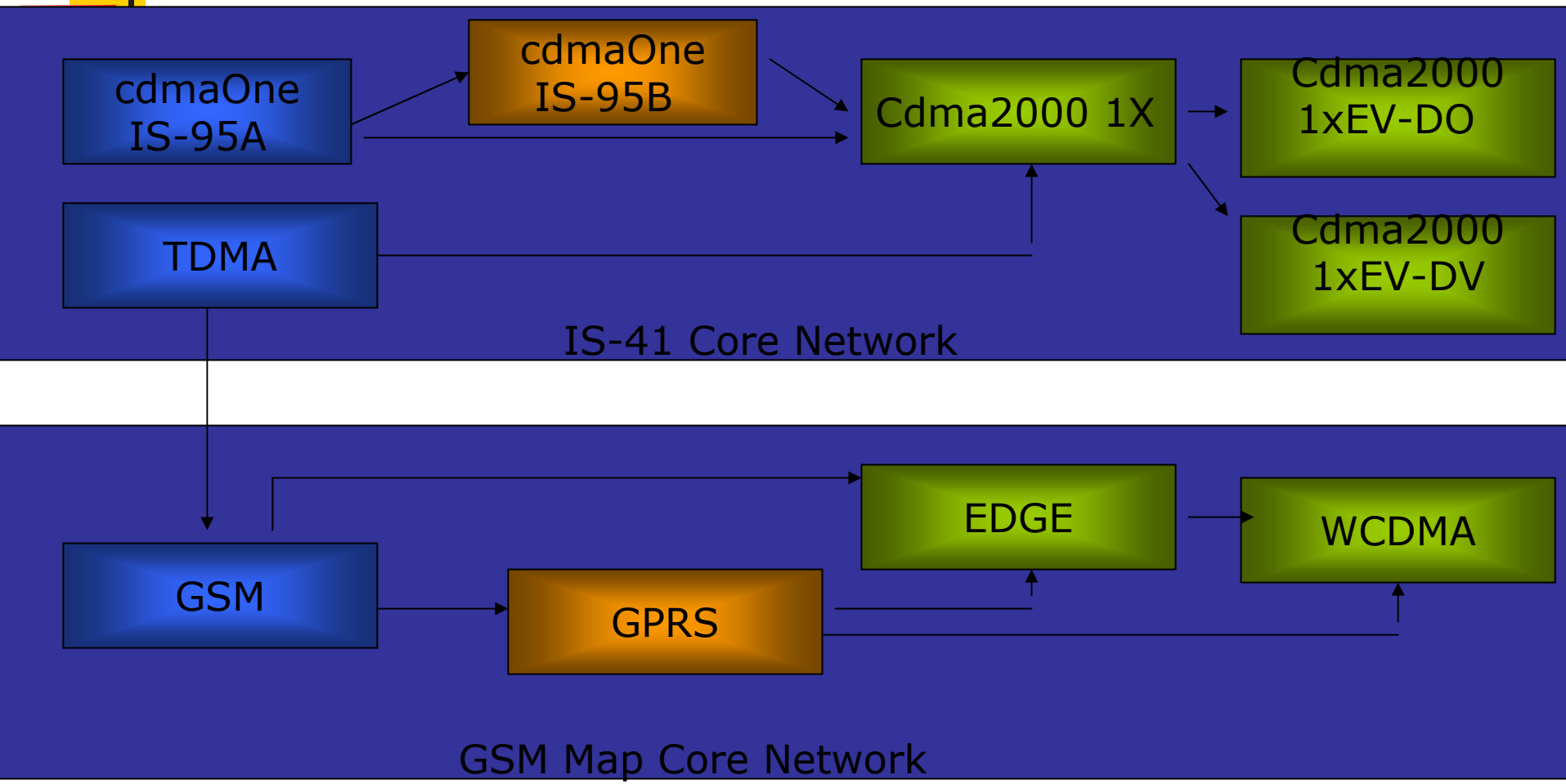
IMT-2000: interfejsy radiowe

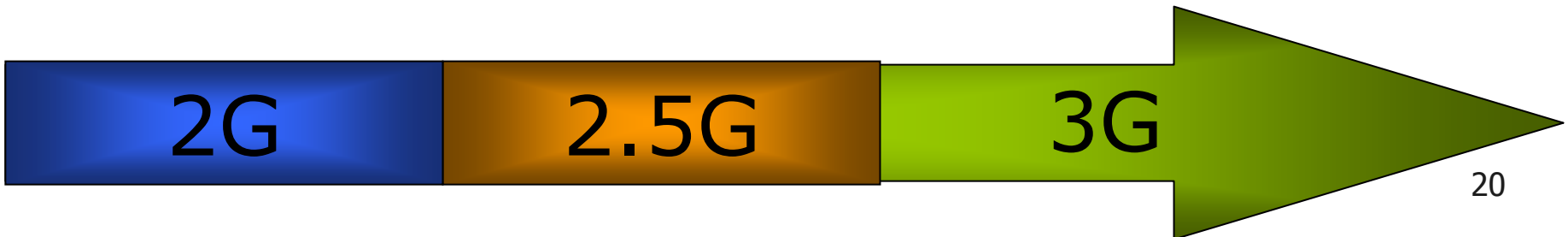


Harmonizowane systemy 3G

- Usługi bazujace na wysokiej prędkości danych, włączając w to aplikacje internetowe i intranetowe
- Zastosowania głosowe i niegłosowe
- Globalny roaming
- Ewolucja na bazie systemów 2G
- ANSI-41 oraz GSM-MAP jako sieci rdzeniowe

Drogi ewolucji





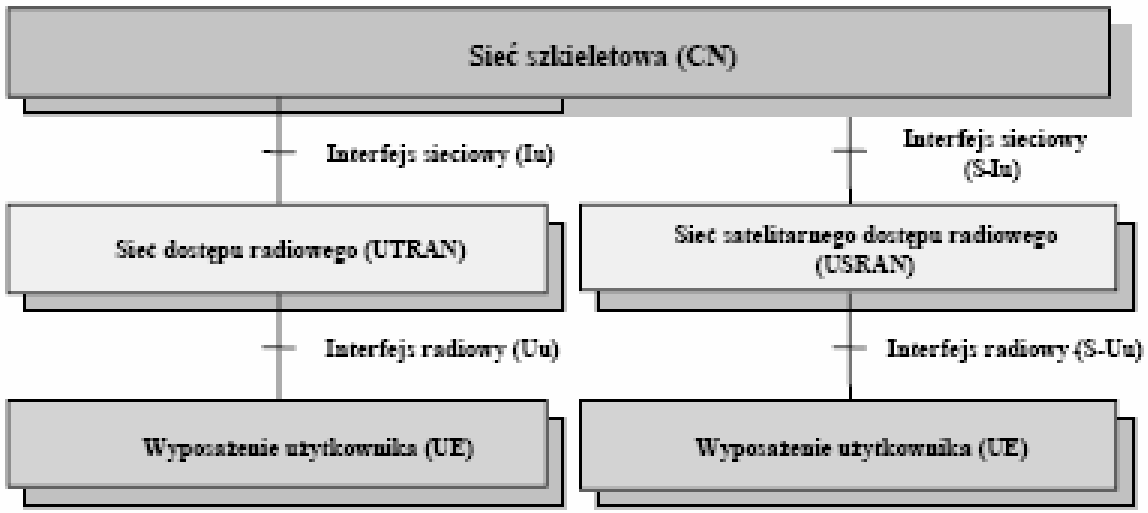
MMS (Multimedia Messaging Service)

- Otwarta przemysłowa specyfikacja utworzona przez WAP forum
- Oparta na architekturze store & forward
- Istotne wzmocnienie obecnej usługi SMS: tekst, kolor, ikony, loga, klipy dźwiękowe, fotografie, animowana fotografia, video klipy
- Działa dzięki szerokopasmowym kanałom w systemach 2.5G i 3G
- Może być dostarczony jako email

Architektura systemu UMTS

Podstawowe elementy architektury systemu:

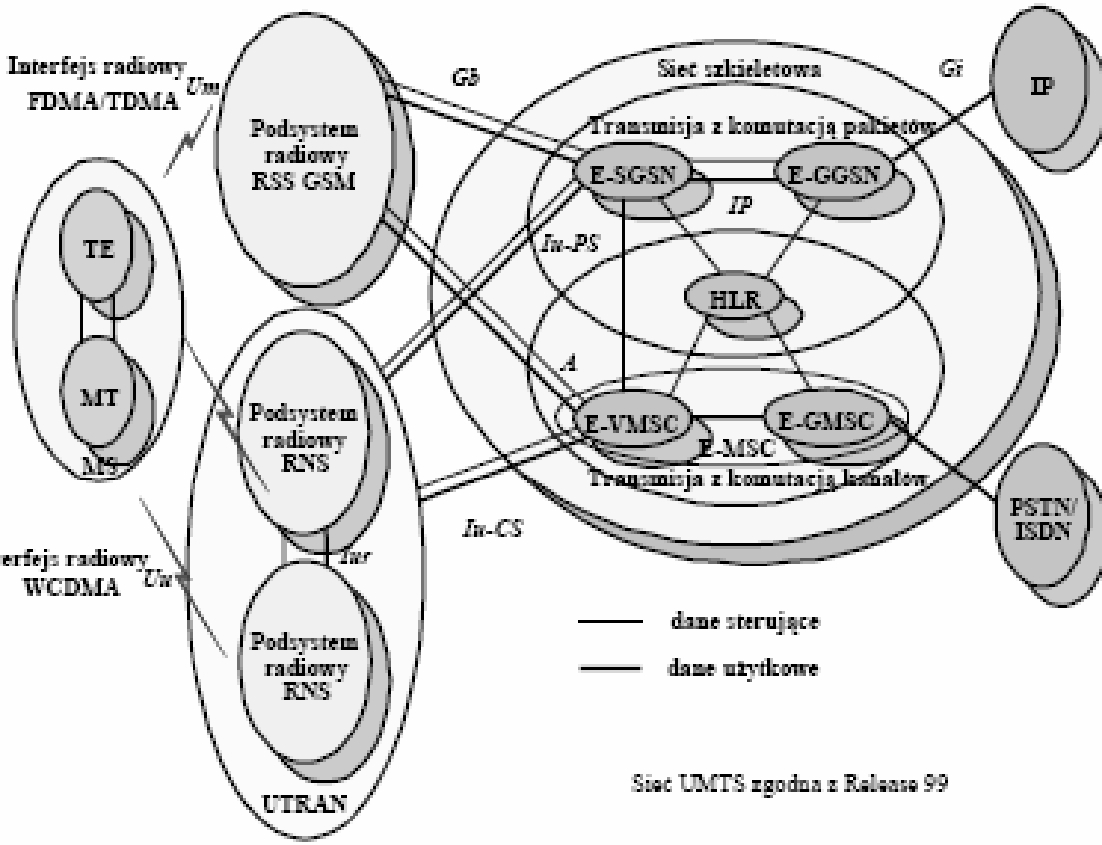
- sieć szkieletowa CN (Core Network),
- naziemna sieć dostępu radiowego UTRAN (UMTS Terrestial Radio Access Network),
- satelitarna sieć dostępu radiowego USRAN (UMTS Satellite Radio Access Network),
- wyposażenie użytkownika UE (User Equipment)



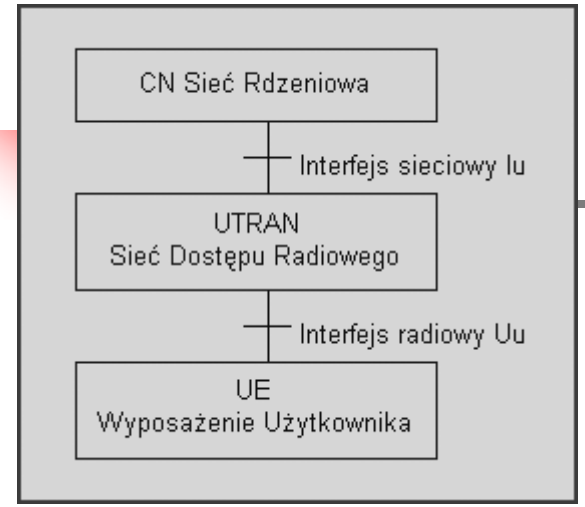
Sieć szkieletowa (*Core Network)*

Funkcje sieci szkieletowej:

- zarządzanie siecią dostępową UTRAN i innymi podsystemami radiowymi (np. GSM)
- zarządzanie transmisją danych w sieci,
- transmisja danych do sieci zewnętrznych (np. PSTN, ISDN, Internet).



Ogólna architektura systemu UMTS



•Sieć rdzeniową CN (Core Network)
•Sieć dostępu radiowego UTRAN
(UMTS Terrestial Radio Access Network)
•Wyposażenie użytkownika UE (User Equipment)
+ Interfejsy: sieciowy Iu i radiowy Uu

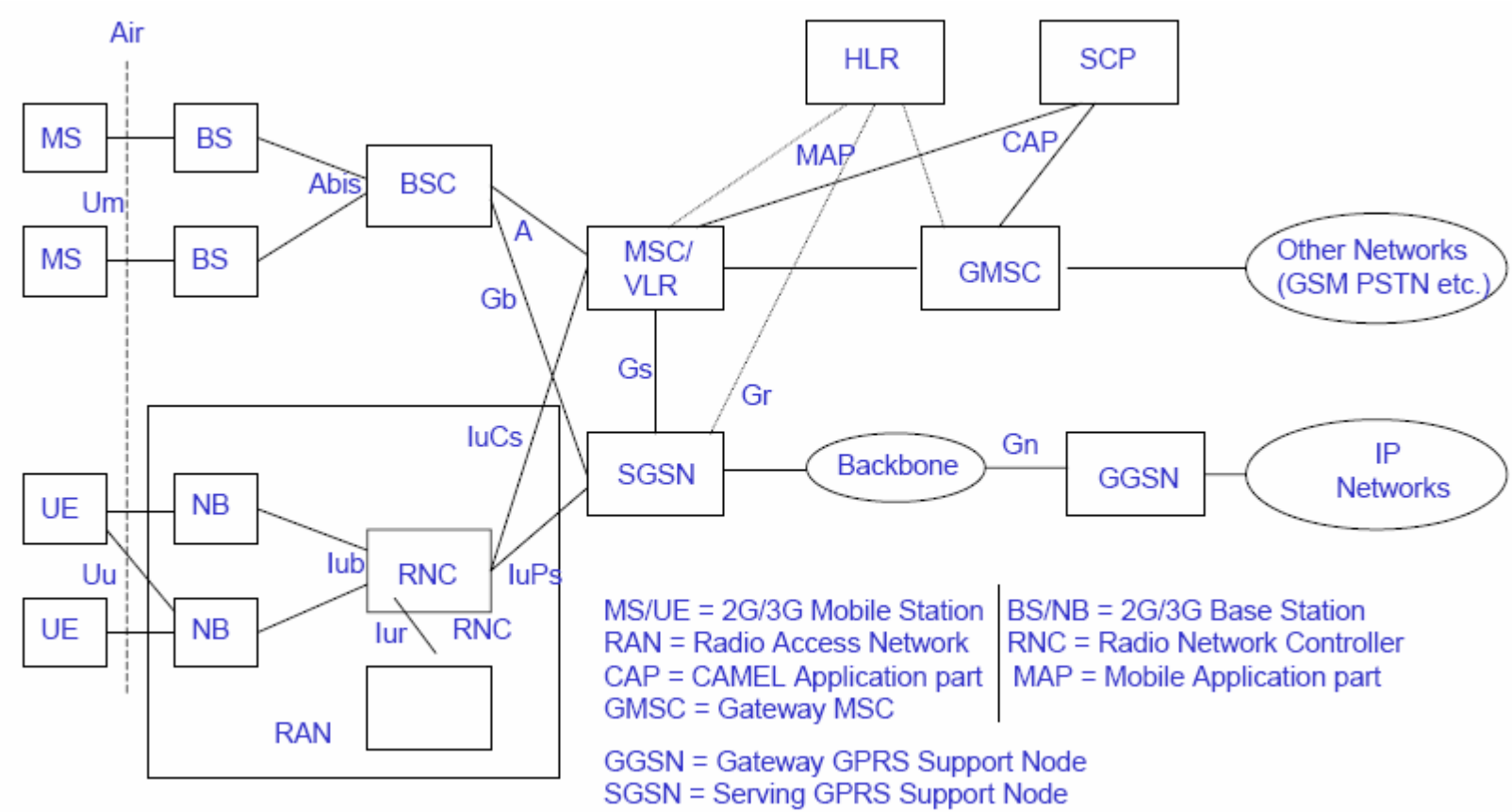
UTRAN jest odpowiedzialna za realizację bezpośrednich połącz. do terminali ruchomych użytkowników końcowych. System dba o efektywne wykorzystanie zasobów radiowych oraz o kontrolę mobilności abonentów. Natomiast sieć rdzeniowa CN realizuje funkcje połączeniowe zachodzące zarówno w jej obrębie i na zew

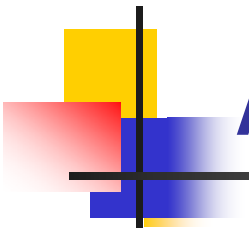
Architekturę systemu UMTS można rozpatrywać **z punktu widzenia fizycznego lub funkcjonaln**

- W pierwszym przypadku system ten jest opisany przy użyciu koncepcji domen, przy tym pod pojęciem domeny rozumie się zbiór powiązanych ze sobą fizycznych elementów sieci.
- W drugim zaś przy użyciu warstw (stratum) - warstwy rozumie się jako zbiór funkcji służących do realizacji przekazu informacji pomiędzy domenami.

Z achitektury komórkowej wynikają ponadto pewne zalety:
- stacje ruchome o dużym stopniu mobilności obsługiwane w makrokomórkach, co powoduje redukcję częstości przenoszenia połączenia pomiędzy komórkami, a zatem zmniejszenie obciążenia sieci sygnałami sterującymi,
- makrokomórki pokrywają miejsca trudne do pokrycia komórkami niższego rzędu,
- makrokomórki dodają pewną nadmiarowość powodując wzrost jego niezawodności.

Architektura UMTS

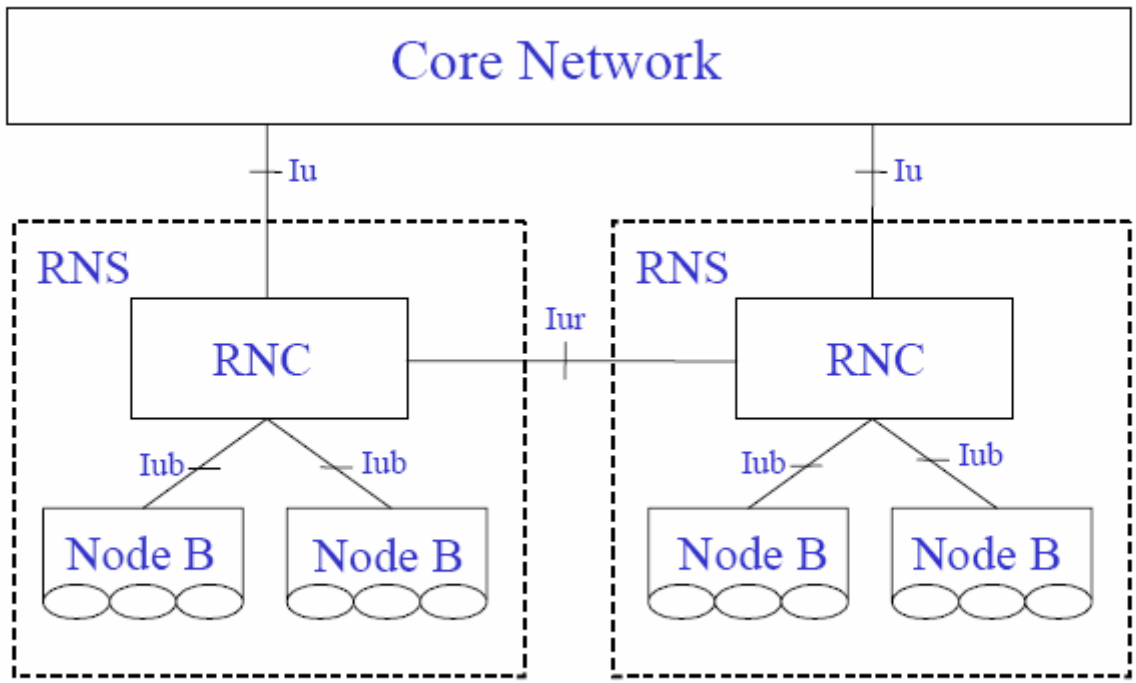




Architektura UMTS

- Nowy węzeł SGSN: nowy pakietowy węzeł transmisji pakietów zamiast transmisji poprzez komutację obwodów
- Najważniejsze zmiany są w sieciowym dostępie radiowym: RAN (UTRAN)

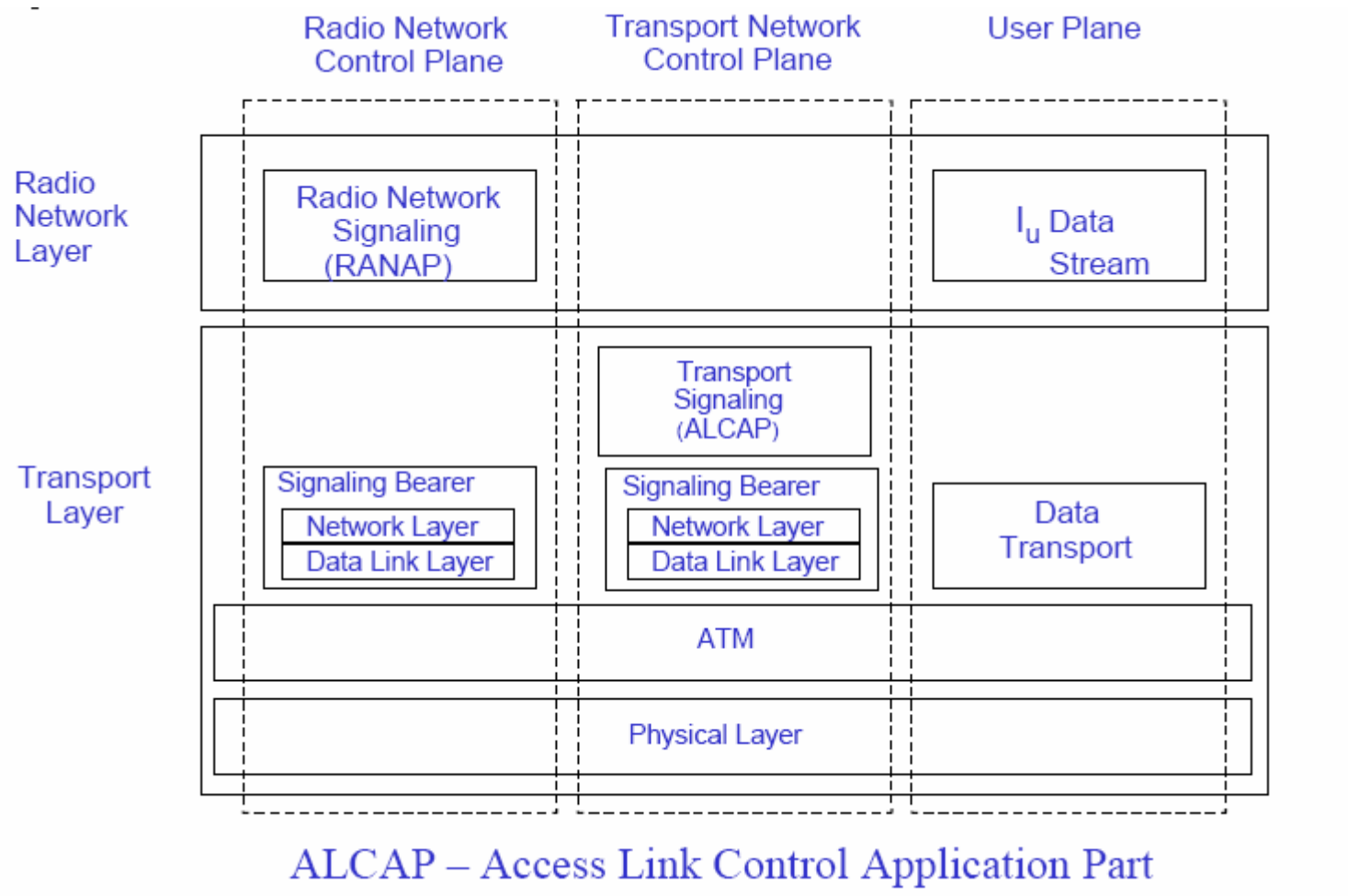
Architektura UTRAN



Architektura UTRAN

- Jest zbiorem podsystemów RNS (radio network subsystems)
- RNS ma dwa główne elementy: węzeł B oraz RNC
- RNS jest odpowiedzialny za zasoby radiowe oraz transmisję/odbiór w zbiorze komórek
- RNC jest odpowiedzialny za używanie i przydział zasobów radiowych RNS, między innymi
  - Przeniesienie połączenia
  - Makrodywersyfikacja strumieni I_{ub}
  - Synchronizacja ramek

UTRAN: ogólna struktura protokołowa



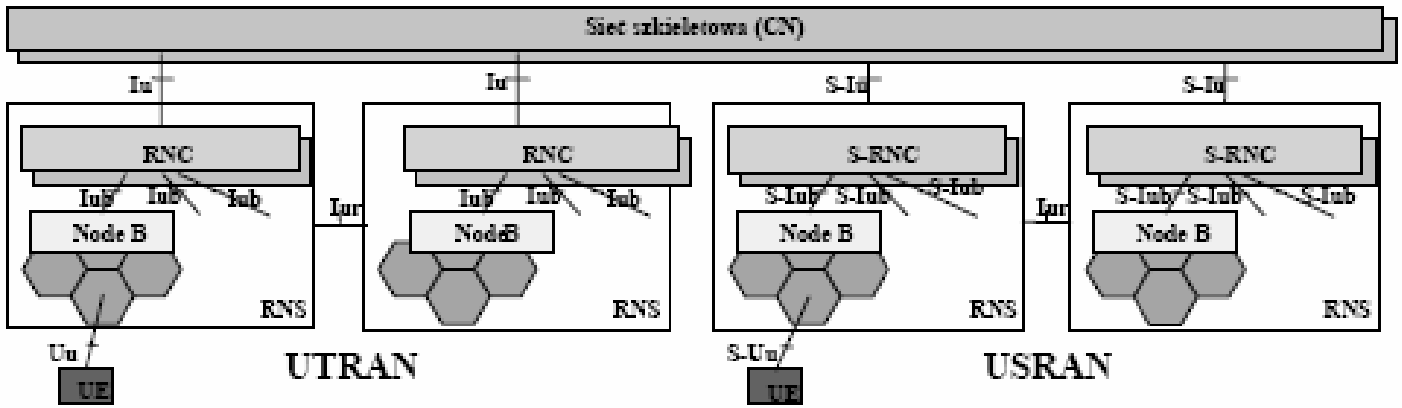
UTRAN: ogólna struktura protokołowa

- Zawiera dwa warstwy: warstwa sieci radiowej (RNL) oraz warstwa sieciowego transportu (TNL)
  - RNL: funkcje związane z UTRAN
  - TNL: realizuje technologię transportu
- Kanały: transportowe (jak informacja jest transmitowana przez interfejs radiowy), logiczne (są opisywane przez typ informacji, którą przenoszą), fizyczne (definiowane w zależności czy FDD czy TDD)

Sieć dostępu radiowego UTRAN i USRAN

Do podstawowych zadań UTRAN i USRAN należą:

- kontrola i zarządzanie zasobami radiowymi,
- szyfrowanie i deszyfrowanie informacji w kanale radiowym,
- obsługa użytkowników ruchomych,
- kontrola dostępu do systemu, w tym:
  - autoryzacja użytkownika,
  - zarządzanie dostępem do kanału radiowego,
  - analiza stanu łącza radiowego,
  - przesyłanie informacji w trybie rozsiewczym,
  - synchronizacja systemową.



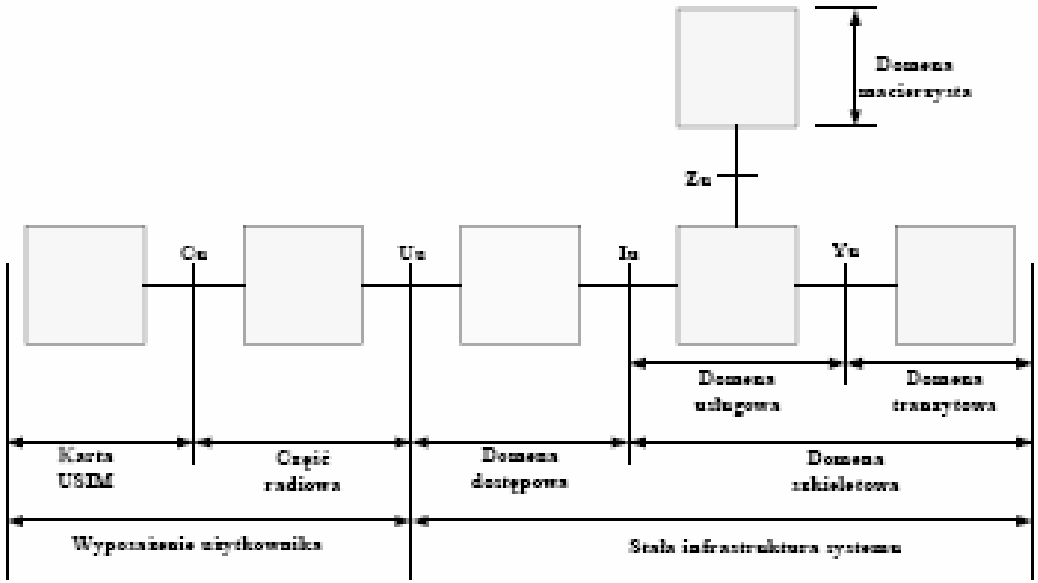
Struktura domenowa systemu UMTS

Architektura systemu UMTS opisywana jest poprzez:

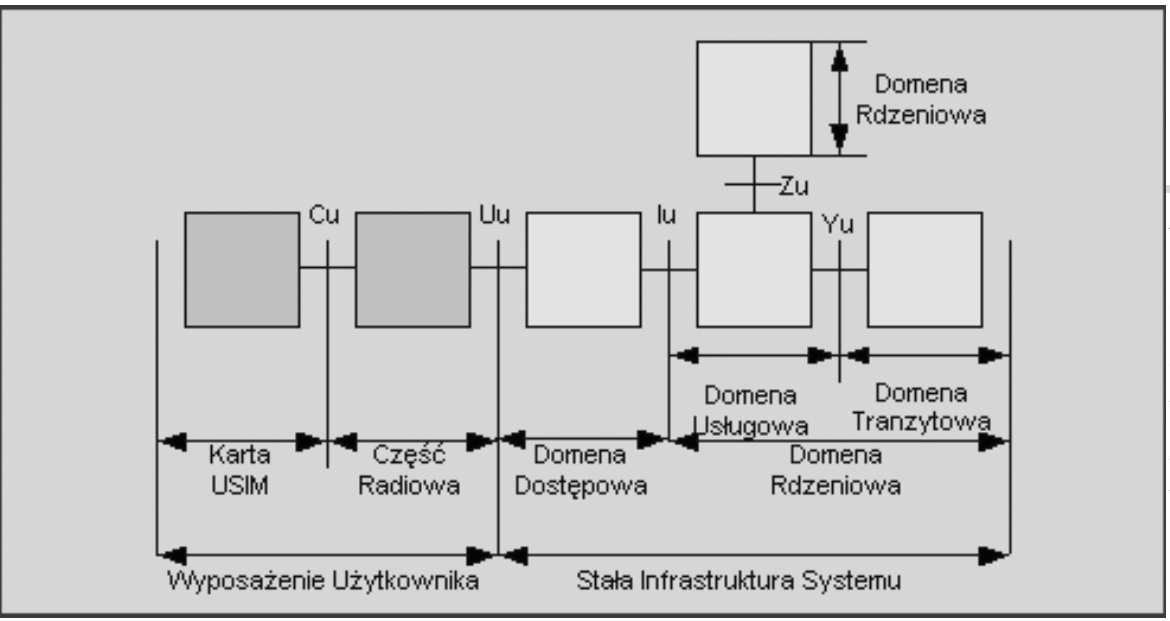
- fizyczne powiązania elementów sieci – strukturę domenową (domain)
- funkcjonalne powiązania elementów sieci - strukturę warstwową (*stratum*).

Strukturę domenową systemu UMTS tworzą:

- domena wyposażenia użytkownika (User Equipment Domain)
- domena infrastruktury systemu (Infrastructure Domain):



Struktura domenowa systemu UMTS

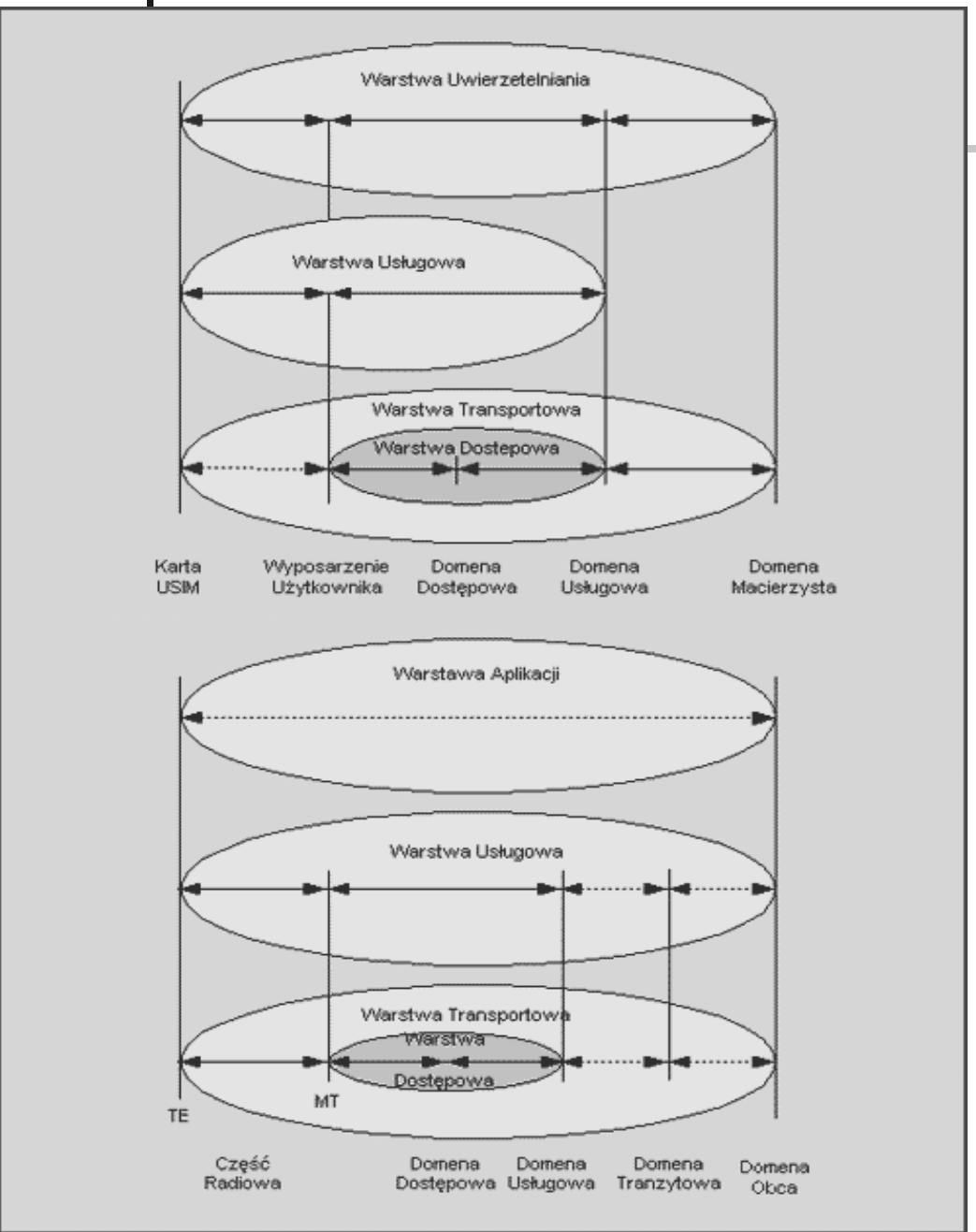


•wyposażenia użytkownika (User Equipment Damain)
•stałej infrastruktury systemu (Infrastructure Damain).
Wyposażenie użytkownika zawiera część **radiową (Mobile Equip.Damai** do realizacji transmisji radiowej i **kart** **USIM (User Services Identity Modul**
Infrastruktura to:
•domenę dostępową (AccessNetwork
•domenę rdzeniową (Core Network I

Do funkcji domeny rdzeniowej należy spełnienie następujących **zadań**:
•lokalizowanie użytkowników, *realizowanie funkcji sygnalizacyjnych i sterujących,
•kontrolowanie transferu strumienia danych, *generowanie informacji o stanie systemu.
W świetle powyższych zadań domena rdzeniowa **dzieli się na**:
•domenę **usługową (Serving Network Domain**), która jest odpowiedzialna za kierowanie wywoła do użytkownika oraz za przesyłanie informacji systemowych i danych, ze źródła do miejsca przezn
•domenę **tranzytową (Transit Nefwork Domain),** która w trakcie wywołania pośredniczy pomięd użytkownikiem i domeną usługową, w sytuacji gdy użytkownik znajduje się poza domeną rdzenio
•domenę **macierzystą (Home Nefwork Domain),** współpracującą bezpośrednio z kartą USIM, w której są przechowywane dane o użytkowniku i jego aktualna pozycja.
Współpraca pomiędzy poszczególnymi domenami będzie odbywać się za pomocą odpowiednich standaryzowanych interfejsów radiowych lub sieciowych nazwanymi Cu, Uu, lu, Zu oraz Yu.

Struktura warstwowa systemu UMTS

przepływ informacji:



•aplikacji (Application Stratum),

•uwierzytelnienia (Home Stratum),

•usługowej (Serving Stratum),

•transportowej (Transport Stratum),

•dostępowej (Access Stratum), która wchodz
w skład warstwy transportowej.

Warstwa aplikacji zawiera protok.end-to-en
(każda funkcja przechodzi proces autoryzacji

W **warstwie uwierzytelnienia** są gromadzon
dane o dostępnych w sieci usługach i o użytk
a także dokonuje się jego autoryzacji.
(zawiera protokoły koordynują wymianę inf.
o użytk.pomiędzy kartąUSIM i dom.macierz

Warstwa usługowa zawiera protokoły komu
i funkcje opisu zasady doboru tras (raute fun
do transmisji danych lub inf. sterujących.

Zadania warstwy transportowej:

•korekcji błędów i ewentualnych retransmisj

•szyfracji w łączu radiowym oraz pomiędzy
poszczególnymi warstwami (opcjonalnie),

•adaptacji szybkości strumienia danych (opcj

•transkodowania (opcjonalnie).

Karta USIM

- Karta USIM zawiera pięć typów danych:
  - **Dane administracyjne**: na stałe przydzielone przez producenta USIM i przez operatora/dostawcę usług (np. klucze i algorytmy bezpieczeństwa, numer IMSI, informacje o klasie dostępu);
  - **tymczasowe dane sieciowe**: informacje zarządzania mobilnością (np. aktualny obszar przywołań ID, tymczasowy numer abonenta ruchomego TMSI lub wartości obliczanego klucza szyfrującego);
  - **Dane o usługach:** informacje o dostępnych i dozwolonych usługach oraz ich danych wewnętrznych (np. lokalną książkę telefoniczną użytkownika, numer użytkownika ruchomego w sieci ISDN, stałe numery wywołania, numery wybierania usług, zastrzeżone numery wybierania, informacje o wywołaniach przychodzących i wychodzących, raporty o statusie i parametrach usługowych dla krótkiej wiadomości, zawiadomienie o stanie naładowania baterii, kontrolę wybierania interfejsów radiowych PLMN przez użytkownika i operatora, listę sieci współpracujących itd.);
  - **Aplikacje**: niezbędne dla realizacji określonych usług, które są pobierane i przechowywane przez USIM dla późniejszego wykonania wewnątrz UE;
  - **Dane osobiste**: obejmują dane przechowywane przez użytkownika w karcie USIM; dla przykładu są to krótkie wiadomości SMS lub wybieranie skrócone.

Informacje na karcie USIM

Uniwersalna karta zintegrowana UICC przechowuje między innymi następujące informacje:

- Informacje związane z UICC:
  - Identyfikacja karty IC, unikalny numer identyfikacyjny UICC wydawcy karty,
  - Katalog aplikacji.
- Informacje związane z kartą USIM:
  - Międzynarodowy numer abonenta ruchomego IMSI (ang. International Mobile Subscriber Identity),
  - Znaki językowe,
  - Klucz szyfrujący (Kc) i algorytmy dla procedur kryptograficznych,
  - Klucz szyfrujący dla GPRS,
  - Kody dla połączeń alarmowych,
  - Możliwości i konfiguracja parametrów,

Karta USIM sprawdza i przechowuje informacje potrzebne dla zabezpieczenia dostępu:

- Kod dostępu PIN,
- Wskaźnik włączenia/wyłączenia PIN,
- Licznik błędów PIN,
- Odblokowanie PIN - PUK,
- Licznik błędów odblokowania PIN,
- Klucze poprawności danych,
- Kody identyfikacji abonenta.

Zabezpieczenia w UMTS

W UMTS zastosowano zabezpieczenia stosowane w sieciach 2G:

- Identyfikację i uwierzytelnienie użytkownika/abonenta,
- Szyfrowanie informacji w interfejsie radiowym,
- wykorzystanie identyfikatorów tymczasowych.

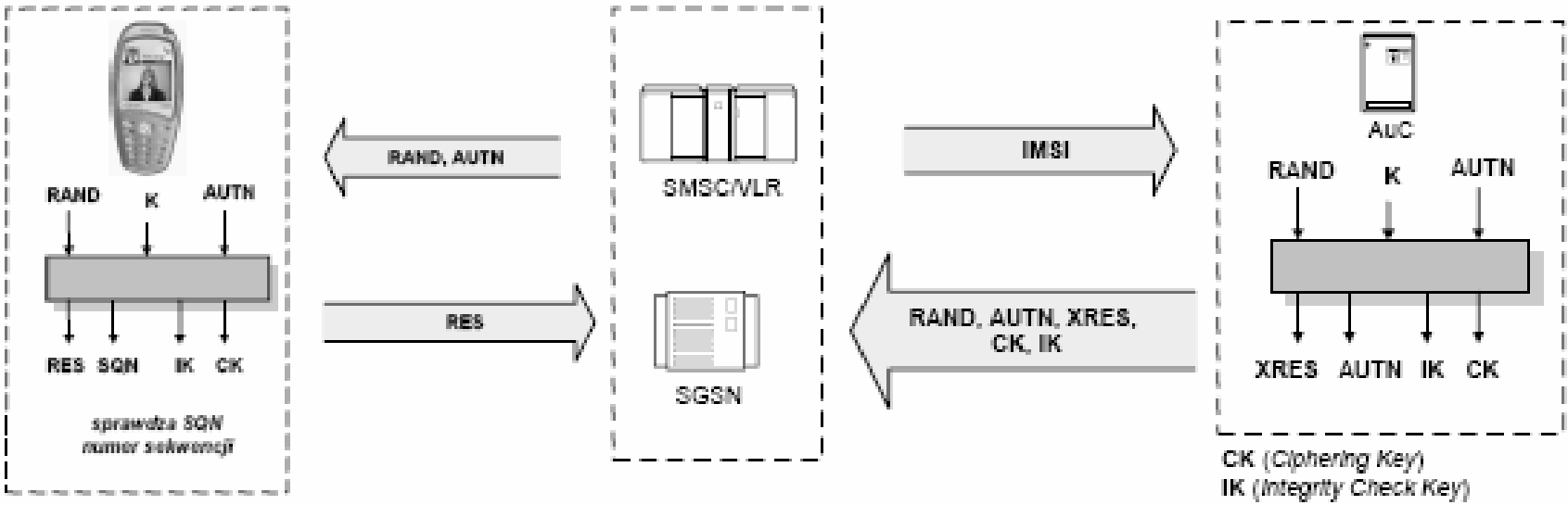
oraz wynikające z doświadczeń zdobytych podczas eksploatacji systemów 2G :

- obustronną identyfikację i uwierzytelnienie zarówno użytkownika/abonenta, jak i sieci - przeciwdziałające przeprowadzaniu tzw. aktywnych ataków przez osoby dysponujące sprzętem pozwalającym naśladować wybrany element sieci bądź terminal,
- szyfrowanie w obszarze działania podsystemu,
- protekcję spójności sygnalizacji w obszarze podsystemu.

- Algorytmy kryptograficzne stosowane do szyfrowania i ochrony spójności sygnalizacji muszą być ogólnie/publicznie dostępne (Zgodnie ze specyfikacją)
- Algorytmy wykorzystywane w autoryzacji obustronnej pozostają w gestii operatorów.

Obustronna identyfikacja i uwierzytelnienie

- W autoryzacji obustronnej biorą udział trzy elementy: sieć "macierzysta", sieć obsługująca, terminal z kartą **USIM** (*Universal Subscriber Identity Module*).
- Sieć obsługująca sprawdza „autentyczność" abonenta (podobnie jak w GSM), wykorzystując tzw. procedurę „wyzwanie-odpowiedź" (***challenge-response***).
- Terminal sprawdza czy sieć obsługująca została uprawniona do uwierzytelnienia terminala przez sieć macierzystą.
- Istnieje możliwość sprawdzenia czy terminal podłączony został do „legalnej" sieci.



Szyfrowanie

- Identyfikacja abonenta/użytkownika (IMSI) poprzez identyfikatory tymczasowe:
  - TIMSI w obszarze działania domeny komutacji kanałów CS sieci szkieletowej
  - P-TIMSI w obszarze działania domeny pakietowej PS sieci szkieletowej

- Szyfrowanie
  - Szyfrowanie strumienia danych poprzez wyznaczenie maski
  - Algorytm F8 z nową metodą szyfrownia blokowego KASUMI, który przekształca 64 bitowe wejście w 64 bitowe wyjście z wykorzystaniem 128 bitowego klucza szyfrującego CK.
  - Obecnie nie ma efektywnych algorytmów znajdujących stan wyjściowy przekształcenia na podstawie danych wejściowych i odwrotnie.
  - Istnieją dwie metody złamania algorytmu: przetestowanie wszystkich możliwych kombinacji 128 bitowego klucza lub sprawdzenie wszystkich kombinacji par wejście/wyjście

Kontrola spójności wiadomości sygnalizacyjnych

- Zastosowanie klucza kontroli spójności IK przekazywanego do RNC wspólnie z kluczem szyfrującym CK w wiadomości „określenie trybu bezpieczeństwa".
- Mechanizm badania spójności oparty jest na metodzie weryfikacji tzw. kodzie uwierzytelnienia wiadomości (message authentication code) generowanym przez jednokierunkową, nieodwracalną funkcję F9 (zmodyfikowana metoda szyfrowania blokowego KASUMI).
- Funkcja w zależności od klucza spójności generuje pseudolosowy 32-bitowy ciąg, który dodawany jest do wiadomości sygnalizacyjnej.
- Po drugiej stronie połączenia przeprowadzana jest analogiczna operacja. Otrzymane wiadomości są porównywane, identyczność ich potwierdza autentyczność wiadomości..
- Istnieją informacje, w przypadku których weryfikacja spójności jest niemożliwa, (sygnalizacja wymieniana w pierwszych fazach komunikacji zanim wygenerowany zostanie klucz IK).

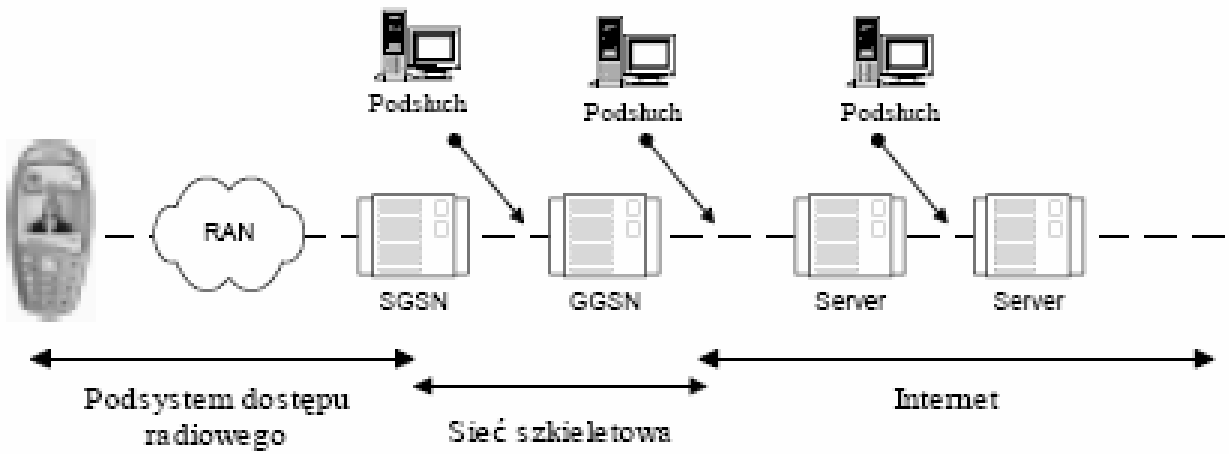
Scenariusze typowych ataków

- Inżynieria socjologiczna (Social Engineering)– czyli ataki na „czynniki ludzkie”,

  przejmowanie istotnych informacji bezpośrednio od użytkowników sieci (np. PIN) bądź innych „czynników ludzkich” zaangażowanych w zarządzanie/nadzór nad siecią (pomoc techniczna, BOK etc)

- Podsłuch elektroniczny (Sniffing),

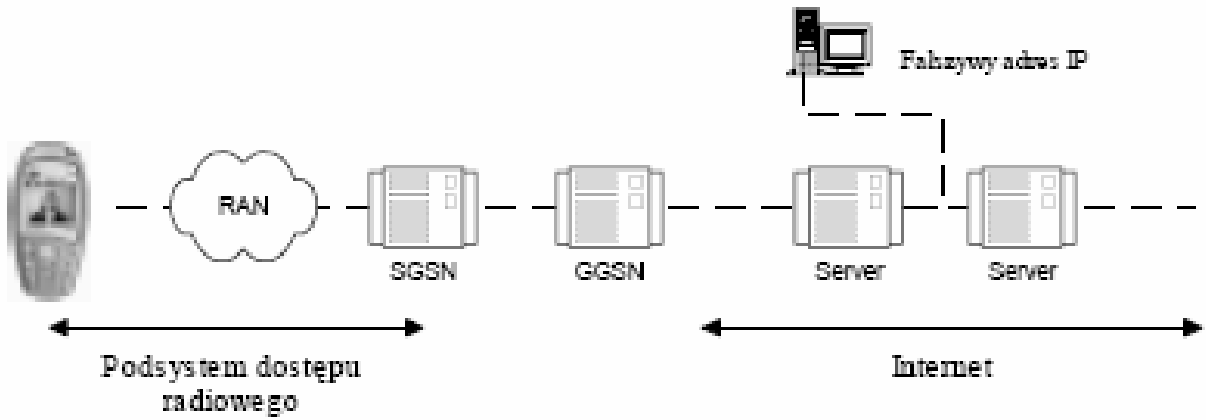
  przechwytywanie wybranych informacji (identyfikatorów użytkownika i haseł) z sieci za pomocą dostępnych programów, narzędzi i urządzeń w celu przejęcia istotnych uprawnień i użytkowników i administratorów systemu.



Scenariusze typowych ataków – c.d.

- Wtrącanie (Spoofing)

  Przejęcie identyfikatorów lub adresów użytkownika (np. adresu IP) i udawanie właściwego odbiorcy w celu przejęcia informacji/pakietów, które są do niego skierowane (telepraca i problem poufności informacji korporacyjnych)



- Przejmowanie sesji komunikacyjnych

  Wtrącenie fałszywego elementu w strukturę systemu w celu przejęcia aktualnych połączeń/sesji.

  Ataki tego typu są bardzo niebezpieczne i trudne do wykrycia oraz „odporne" na zabezpieczenia stosowane w systemie.

DoS (*Denial of Service*) – odmowa świadczenia usług

Ataki nie mają na celu przejęcia informacji lecz utrudnienie dostępu dla innych użytkowników i platform usługowych.

W typowym wariancie ataku DoS haker generuje ruch (np. żądania obsługi wymagające rezerwacji zasobów), który ma na celu zakłócenie/unieruchomienie serwera/elementu będącego ofiarą ataku.

Atak może polegać na wypełnieniu całej kolejki żądań obsługi atakowanego systemu i ignorowaniu potwierdzeń rezerwacji zasobów przez system.

Zarezerwowane zasoby są uwalniane po pewnym czasie, jednak gdy przy ciągłych żądaniach system odmawia współpracy na skutek braku zasobów.

Ataki typu DoS są trudne do odparcia i w większości przypadkow powodują znaczne konsekwencje ekonomiczne.