Bezpieczeństwo w systemie łączności radiowej TETRA

mgr. inż. Quang Anh Tran
Instytut Telekomunikacji, PW

Plan wykładu

- Wprowadzenie
- Opis, architektura i parametry systemu TETRA
- Środki bezpieczeństwa w systemie TETRA
- Pytania i uwagi

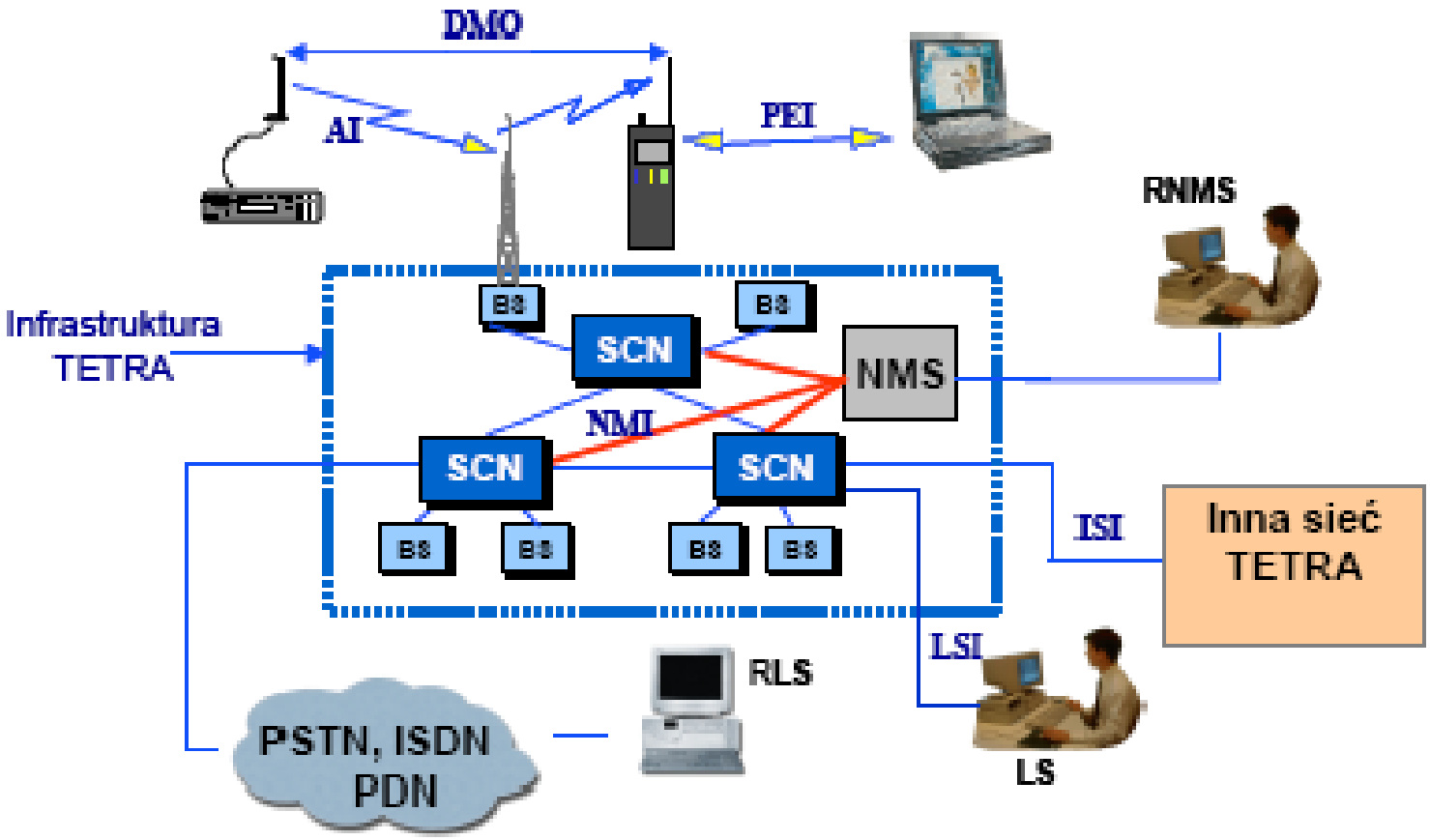
Czym jest TETRA?

- TETRA (*TErrestrial Trunked Radio*) - światowy standard cyfrowych mobilnych sieci trunkingowych opracowany przez ETSI w 1992 roku
- Szerokie zastosowanie w instytucjach, przedsiębiorstwach użyteczności publicznej, dla służb bezpieczeństwa publicznego itp.
- Kierunki rozwoju standardu wyznacza TETRA MoU (*TETRA Memorandum of Understanding*), które zrzesza ponad 100 organizacji i firm z całego świata
- Światowi liderzy w dostawie sprzętów: Motorola (280 kontraktów, 64 kraje), Nokia/EADS, Ericsson

- Opracowano dwa wydania standardu TETRA
  - TETRA 1 (najbardziej powszechny)
  - TETRA 2 (w 1999 r.)
- TETRA na świecie:
  - Finlandia – VIVRE (Nokia/EADS), 35 tys. użytkowników.
  - Dania – SINE (Motorola)
  - Niemcy – Nokia/EADS,
  - Szwecja – RAKEL (Nokia/EADS), 50 tys. użytkowników
  - Wielka Brytania – AIRWAVE (Motorola), 200 tys. użytkowników
- TETRA w Polsce:
  - niewielka ilość rozproszonych systemów np. Policja (Warszawa, Łódź, Kraków, Szczecin), MPK (Wrocław, Gdańsk), port morski w Gdańsku - Motorola

Elementy systemu TETRA

- węzły sterujące **SCN** (*Switching Control Node*),
- stacje bazowe **BS** (*Base Station*),
- zdalne stanowiska liniowe dyspozytorów **RLS** (*Remote Line Station*),
- stanowiska administratorów sieci **NMS** (*Network Management Station*),
- zewnętrzne stanowiska zarządzania siecią **ENMS** *(External Network Management Station*),
- terminale ruchome **MS** (*Mobile Station*),
- punkty styku (*Gateway*) z innymi sieciami



Rysunek 1. Architektura i interfejsy systemu TETRA
(*Z. Jóskiewicz.: TETRA – system łączności radiowej dla transportu publicznego, 2005*)

Podstawowe parametry systemu TETRA

- Zakresy częstotliwości (MHz):
  - służby publiczne: 380-400
  - zastosowanie komercyjne: 410-420, 420-430, 450-460, 460-470, 870-888, 915-933
- Szerokość kanału: 25 kHz
  - zwielokrotnienie czasowe TDMA, 4 kanały głosowe, 1 kanał danych
- Szybkość transmisji
  - głos: 36 kbit/s
  - dane zabezpieczone: 19,2 kbit/s
- Czas zestawiania połączenia: < 300 ms
- Czas przeniesienia połączenia: < 1 ms
- Moc wyjściowa terminalu: 1, 3, 10 W

Typy zagrożenia:

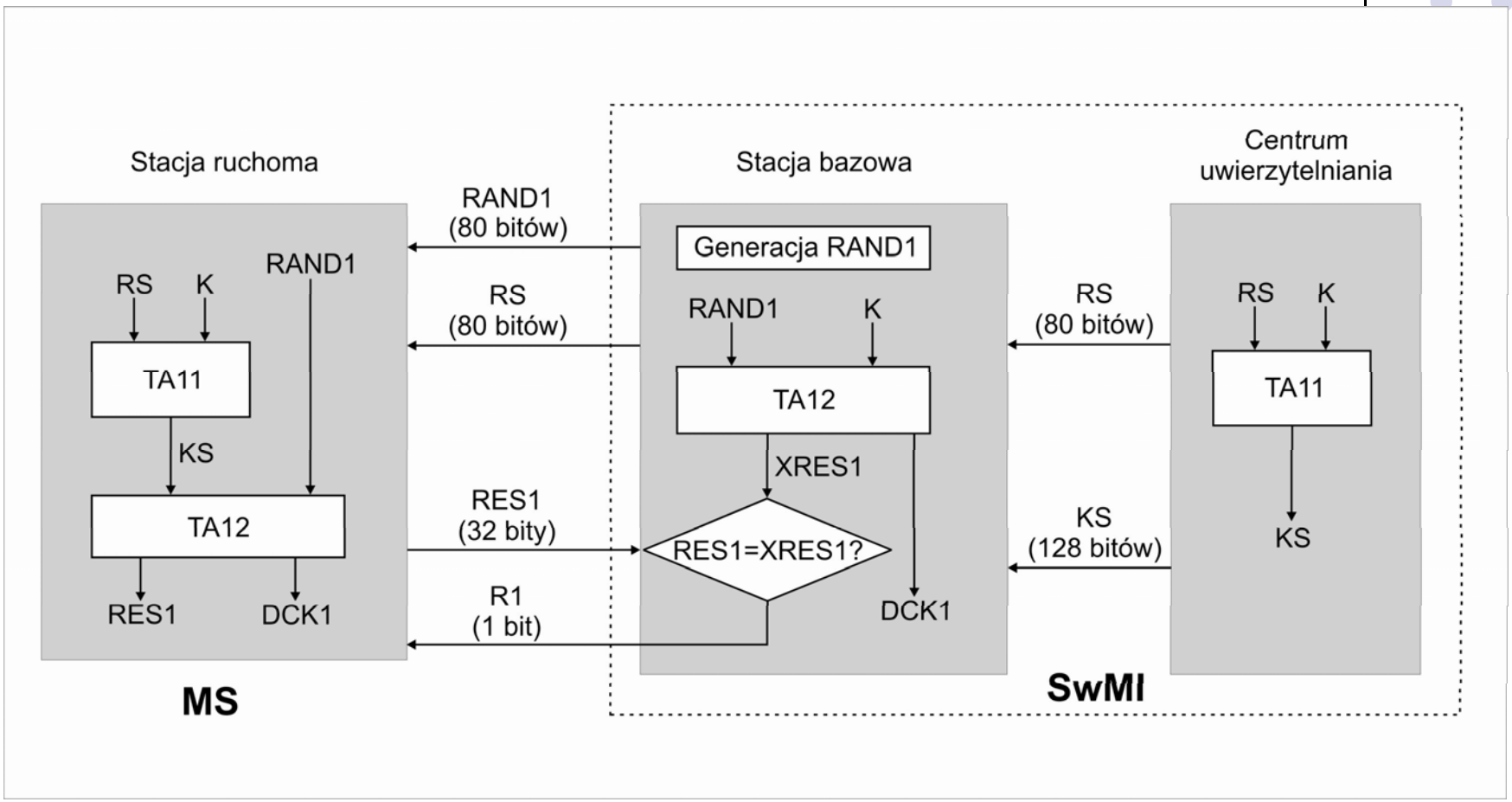
- zagrożenia dla przekazywanych informacji
  - przechwytywanie informacji, czyli podsłuch (*interception, eavesdropping*)
  - manipulacje informacją (*manipulation*)
  - kwestionowanie odbioru lub autorstwa informacji (*repudiation*)
- zagrożenia dla użytkowników systemu
  - analiza ruchu (*traffic analysis*)
  - obserwowalność użytkowników (*observability*)
- zagrożenia związane z działaniem samego systemu
  - blokowanie dostępu do usługi (*denial of service*)
  - nieuprawnionym korzystaniu z zasobów (*unauthorized use of resources*)

Środki bezpieczeństwa w standardzie TETRA

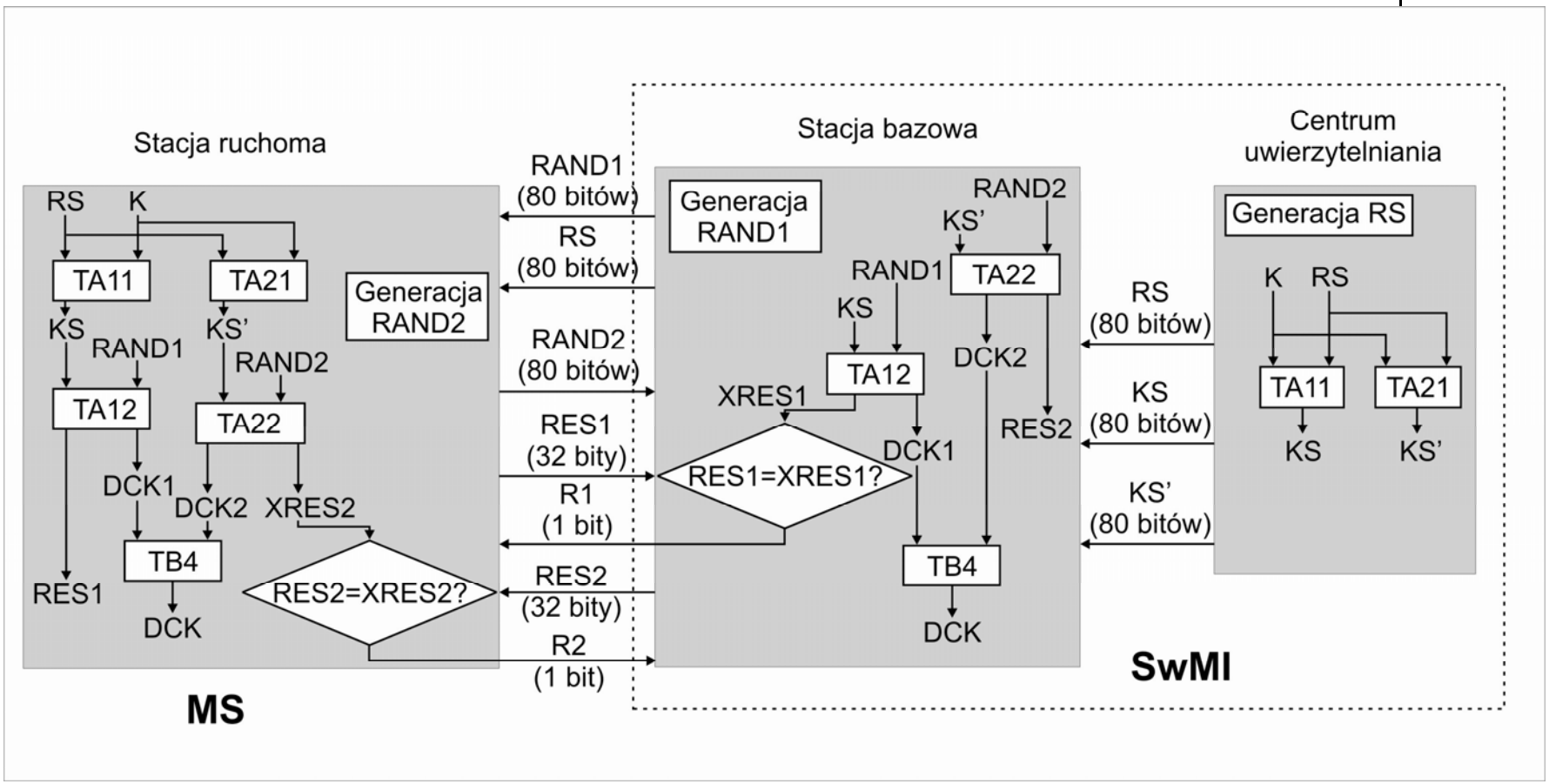
- uwierzytelnianie użytkownika i infrastruktury sieciowej,
- szyfrowanie informacji przekazywanych przez kanał radiowy,
- szyfrowanie informacji w relacji *„end-to-end”*,
- utajnianie tożsamości abonentów,
- zdalna blokada terminali.

Uwierzytelniania w systemie TETRA

- Uwierzytelnianie użytkownika (grupy użytkowników)
  - Zapobieganie podszywaniu się pod innego użytkownika w kanale radiowym
  - Zapobieganie nieautoryzowanego wykorzystania zasobów sieci
- Uwierzytelnianie infrastruktury sieciowej
  - Upewnianie użytkownika o autentyczności infrastruktury sieciowej TETRA
  - Zapobieganie podszywaniu się pod elementy infrastruktury sieciowej (np. „fałszywa stacja bazowa”)
- Uwierzytelnianie wzajemne obu podmiotów
  - W zastosowaniach wymagających najwyższego poziomu bezpieczeństwa



Rysunek 2. Uwierzytelnianie stacji ruchomej MS (*Mobile Station*) przez infrastrukturę sieciową SwMI (*Switching and Management Infastructure*)



Rysunek 3. Uwierzytelnianie wzajemne inicjowane przez SwMI

Zarządzanie kluczami kryptograficznymi

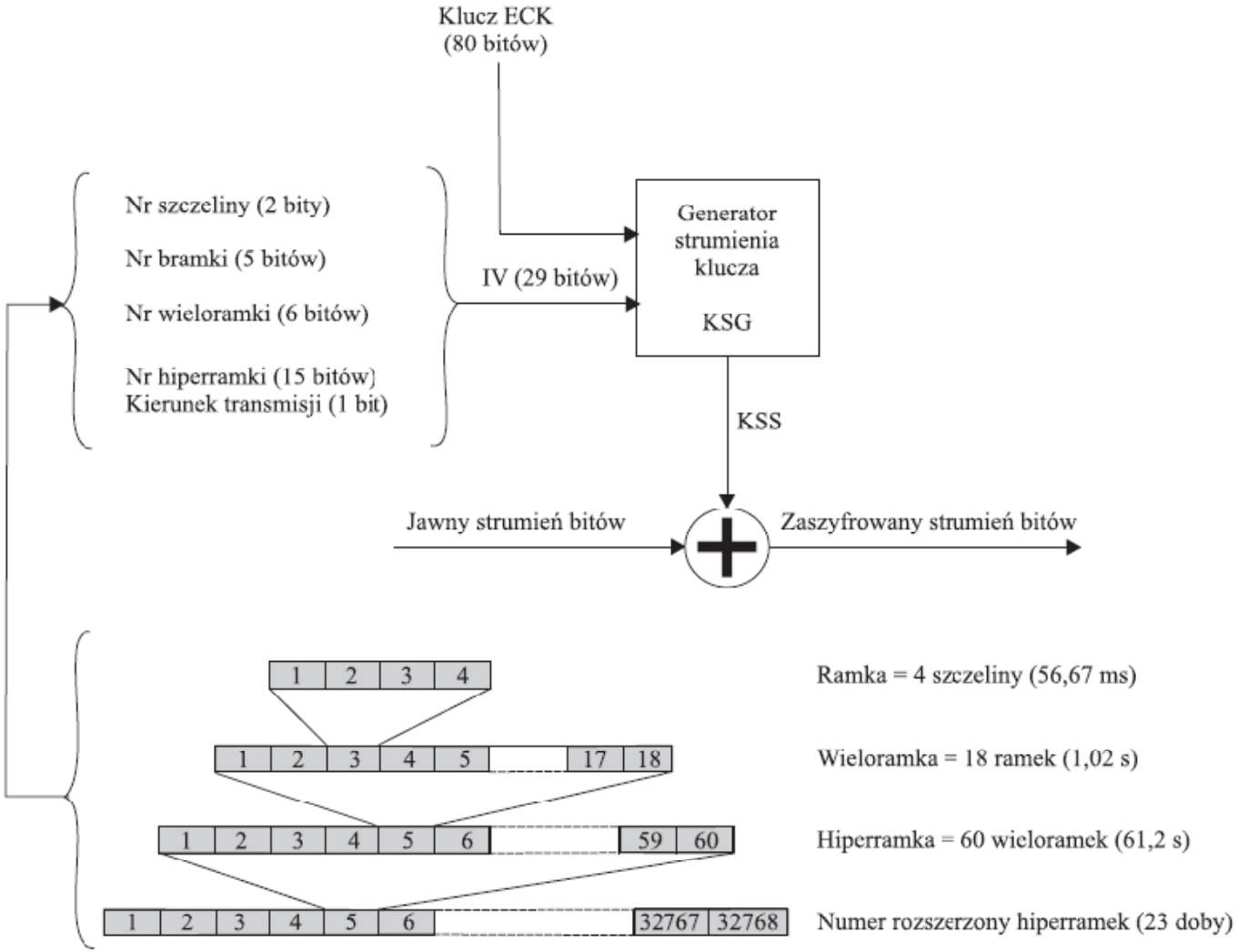
- Podstawowe klucze szyfrujące w standardzie TETRA:
  - Klucz pochodny DCK (*Derived Cipher Key*)
    - Indywidualny, dynamicznie przypisywany określonego terminalu,
    - Wytwarzany podczas realizacji procedury uwierzytelniania i nigdy nie przesyłany drogą radiową
  - Klucz wspólny CCK (*Common Cipher Key*)
    - Generowany przez SwMI i dostarczony do MS w formie zaszyfrowanej (DCK) drogą radiową
  - Klucz grupowy GCK (*Group Cipher Key*) / zmodyfikowany MGCK
    - Klucz przypisany do jednej zamkniętej grupy użytkowników
  - Klucz statyczny SCK (*Static Cipher Key*)
    - Generowany przez SwIMI w zestawach po 32 klucze

Klasy bezpieczeństwa

- Klasa 1 - najniższy poziom
  - brak szyfrowania informacji w interfejsie radiowym
- Klasa 2
  - szyfrowanie przesyłanych informacji przy użyciu SCK
  - może być stosowana procedura uwierzytelniania
- Klasa 3
  - szyfrowanie sygnałów głosowych i danych oraz informacji sygnalizacyjnych przy użyciu DCK
  - obowiązek stosowania uwierzytelniania
  - w przypadku połączeń grupowych – klucz MGCK w powiązaniu z kluczem wspólnym CCK

Szyfrowanie informacji w interfejsie radiowym

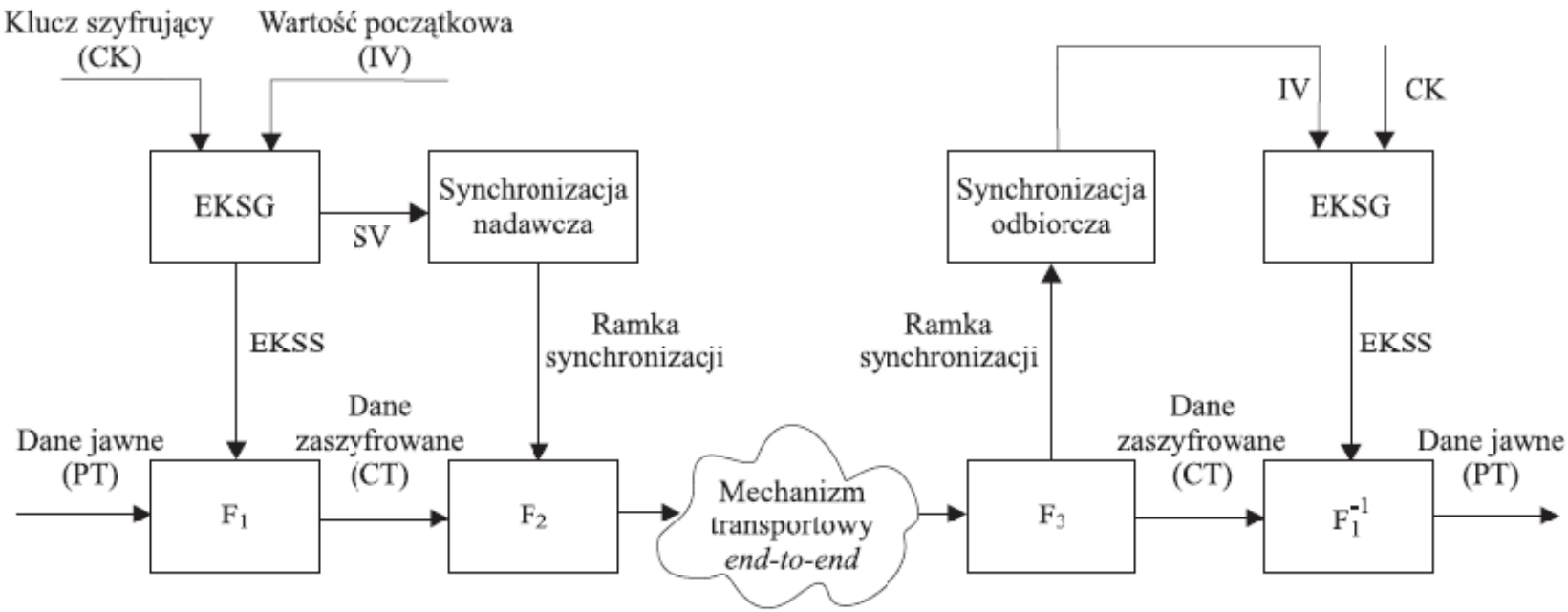
- Szyfrowanie informacji w interfejsie radiowym umożliwia dostosowanie bezpieczeństwa w sieciach radiowych do poziomu, jaki zapewniają sieci stacjonarne
- Funkcje realizujące procesu szyfrowania/deszyfrowania są ulokowane w górnej części podwarstwy MAC, wchodzącej w skład warstwy łącza danych stosu protokołów TETRA
- W procesie szyfrowania/deszyfrowania informacji są wykorzystywane algorytmy szyfrowania strumieniowego z kluczami symetrycznymi.



Rysunek 4. Mechanizm szyfrowania informacji w interfejsie radiowym
(*Telekomunikacja i techniki informacyjne 3-4/2005*)

Szyfrowanie informacji w relacji *end-to-end*

- Szyfrowanie *end-to-end* obejmuje zabezpieczenie danych transportowanych między terminami, bez angażowania infrastruktury sieciowej
- Wymagania dot. mechanizmu szyfrowania „*end-to-end*”
  - ten sam mechanizm szyfrowania w obu kierunkach transmisji
  - niezależność procesu synchronizacji dla każdego kierunku
  - procedura szyfrowania *end-to-end* powinna być umieszczona w płaszczyźnie użytkownika, powyżej procedury szyfrowania w interfejsie radiowym ulokowanej w podwarstwie MAC;
  - zależności czasowe i kolejność transmitowanych danych powinny być utrzymywane w obrębie par podszczelin



Rysunek 5. Schemat ogólny mechanizmu szyfrowania i deszyfrowania głosu w relacji „end-to-end” (*Telekomunikacja i techniki informacyjne 3-4/2005*)

Ochrona poufności tożsamości użytkowników

- W standardzie TETRA do zapewnienia poufności tożsamości abonenta wykorzystywany jest zastępczy numer abonenta ATSI (*Alias TETRA Subscriber Identity*)
- Standard TETRA definiuje mechanizm ESI *(Encrypted Short Identity)*, który dostarcza środki zabezpieczania informacji identyfikacyjnych transmitowanych w kanale radiowym
- Mechanizm ESI może być stosowany tylko w sieciach, w których informacja przekazywana przez kanał radiowy jest szyfrowana. Wykorzystuje klucze CCK lub SCK w zależności od klasy bezpieczeństwa.

Zdalne blokowanie terminali

- zablokowanie wyposażenia terminalu
  - opiera się na numerze TEI *(TETRA Equipment Identity)*
  - stacja ruchoma nie może być dłużej używana, nawet jeżeli zostanie wprowadzony inny numer ITSI
- blokada abonenta w sieci
  - wykorzystuje numer ITSI *(Individual TETRA Subscriber Identity)*
  - stacja ruchoma może być wykorzystywana z innym, aktywnym numerem ITSI
  - blokada czasowa z możliwością ponownego uaktywnienia lub trwała
- użycie obu tych funkcji jednocześnie

Standardowe algorytmy kryptograficzne

- W celu zapewnienia współpracy systemów opracowanych przez różnych producentów, eksperci SAGE (*Security Algorithm Group of Experts*) w ETSI opracowali dwie grupy algorytmow kryptograficznych o różnym stopniu dostępności:
  - TEA2 i TEA3 – głównie do stosowania przez organizacje bezpieczeństwa publicznego, objęte ograniczeniami eksportowymi;
  - TEA1 i TEA4 – łatwiej dostępne

Dziękuję bardzo za uwagę!

Pytania? Uwagi?