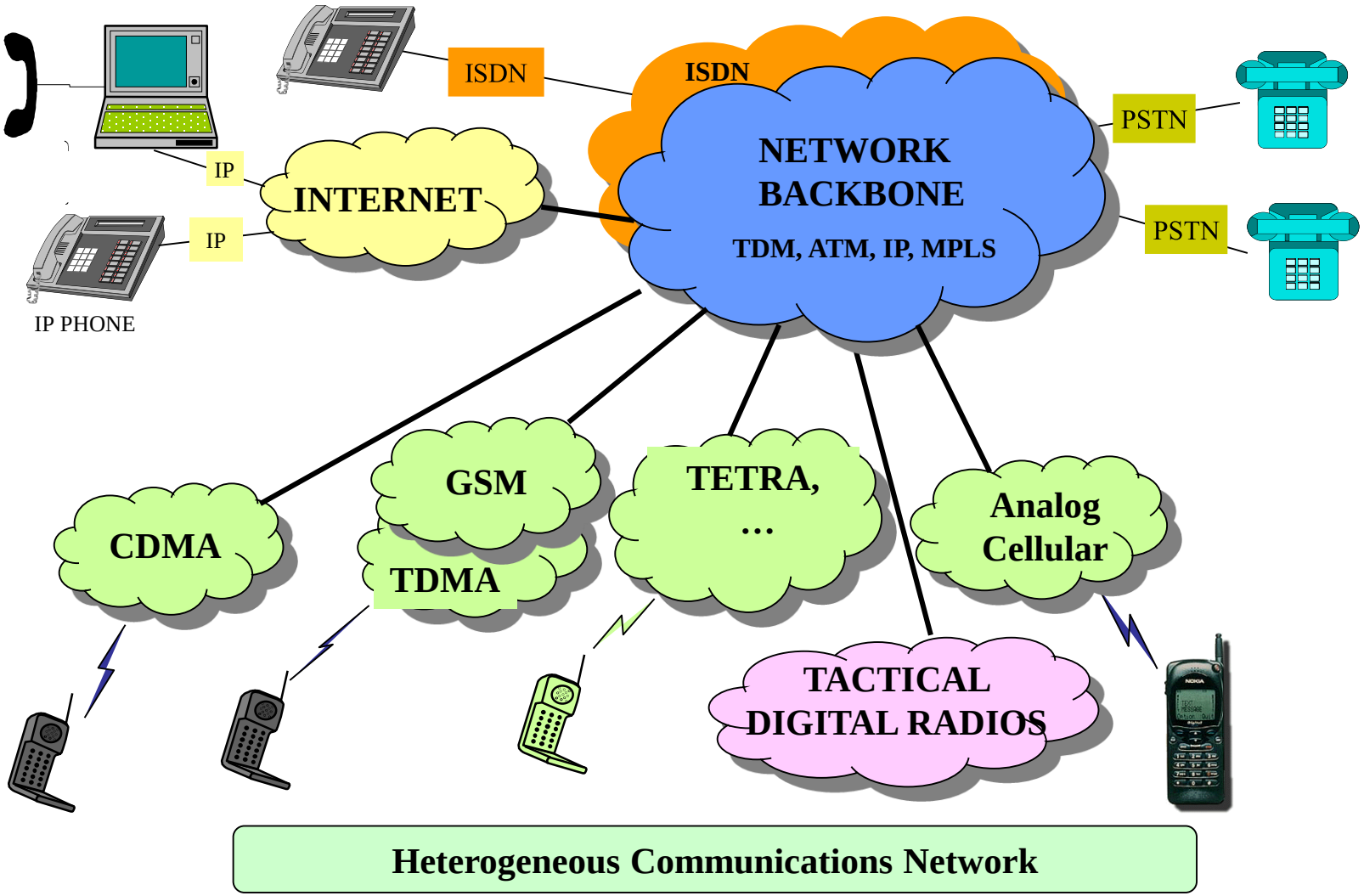
Sekcja Telekomunikacji Komitetu Elektroniki i Telekomunikacji PAN

Protokół SCIP
dla bezpiecznej komunikacji przez sieci publiczne

dr hab. inż. Grzegorz Różański

Posiedzenie Sekcji Telekomunikacji
Komitetu Elektroniki i Telekomunikacji PAN
Warszawa, 14.05.2014

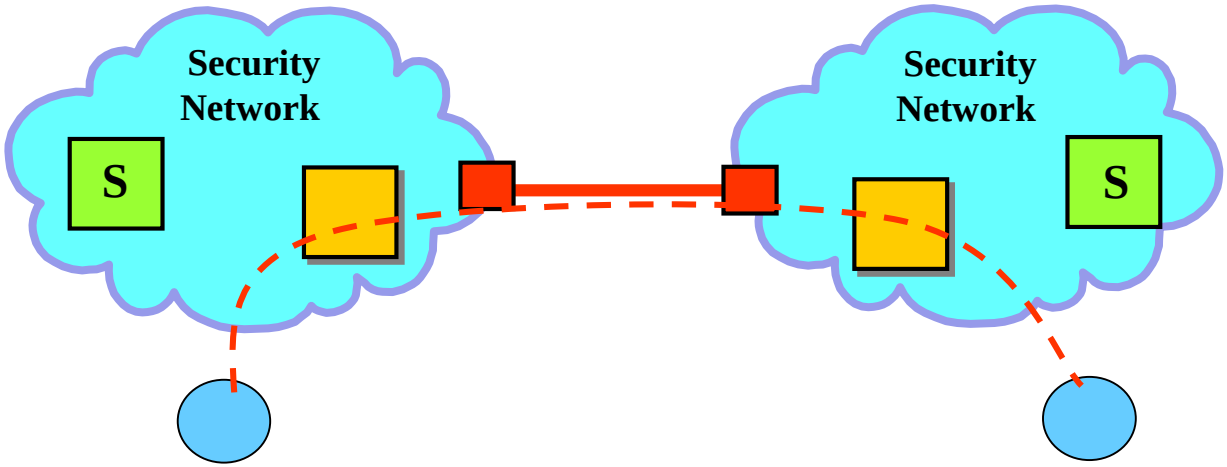
Heterogeniczność sieci telekomunikacyjnych



Bezpieczna łączność (Communications security)

Podstawowe funkcjonalności bezpiecznej komunikacji w sieciach wojskowych państw NATO:

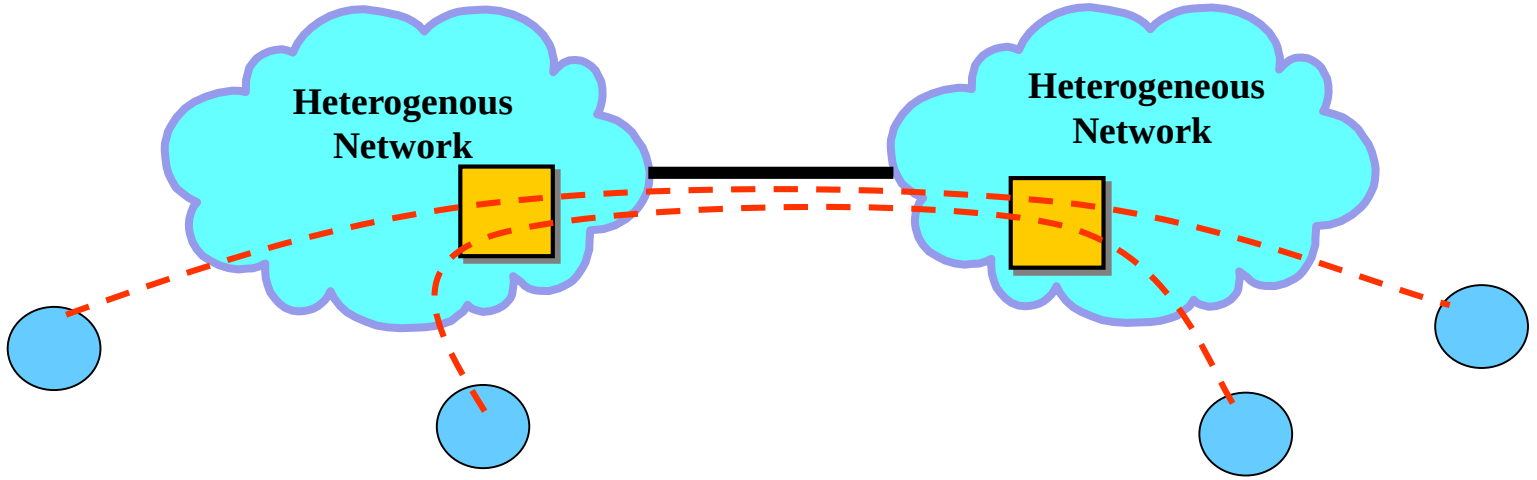
- **szyfrowanie/uwierzytelnianie ⇒ funkcje gwarantowane przez sieć**
- **szyfrowanie ⇒ realizowane za pośrednictwem łączy utajnianych**
- **uwierzytelnianie ⇒ realizowane z wykorzystaniem serwerów S (abonent i serwer należą do tego samego segmentu/domeny sieci),**
- **różne poziomy utajniania (Top Secret, Secret, Confidential, Restricted),**
- **usługi zapewnianie przez sieć ⇒ Voice, Data**



Bezpieczna łączność (End-to-end security)

Podstawowe założenia dla bezpiecznej komunikacji (wraz szyfrowaniem i uwierzytelnianiem informacji) pomiędzy dowolnymi punktami końcowymi /urządzeniami końcowymi sieci (źródłami/ujściami informacji):

- **uwierzytelnianie, szyfrowanie i deszyfrowanie w pełni implementowane w urządzeniach końcowych (bezpośrednia interakcja pomiędzy terminalami abonenckimi),**
- **funkcje sieci ⇒ tylko transport i komutacja danych,**
- **bez deszyfrowania/szyfrowania danych w węzłach sieci**



Strategia NATO

- **Stosowane obecnie rozwiązania bezpiecznej komunikacji fonicznej w sieciach wykorzystujących protokół IP bazują na architekturze VoIP (Voice over IP).**

- **W sieciach wojskowych państw NATO proponuje się dwie strategie:**

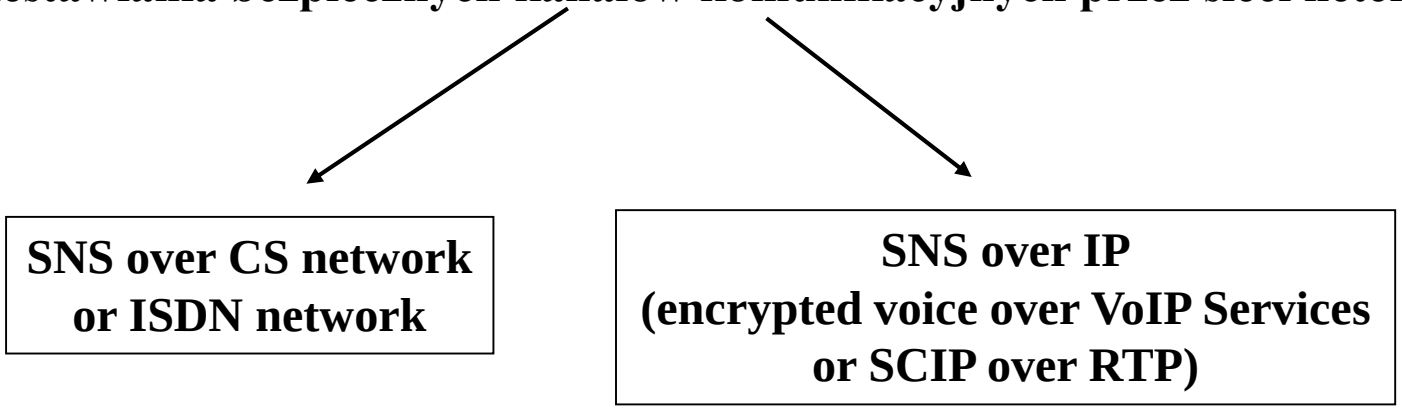
  - VoSIP (Voice over Secure IP),
  gdzie istotna rolę odgrywają różnorodne mechanizmy bezpieczeństwa implementowane w sieci głównie z wykorzystaniem protokołu IPSec,

  - SVoIP (Secure Voice over IP),
  gdzie istotną rolę odgrywa implementacja w sieci protokołu SCIP wraz z oferowanymi mechanizmami bezpiecznej komunikacji „End-to-End”.

SNS - Secure Network Independent Speech Communication

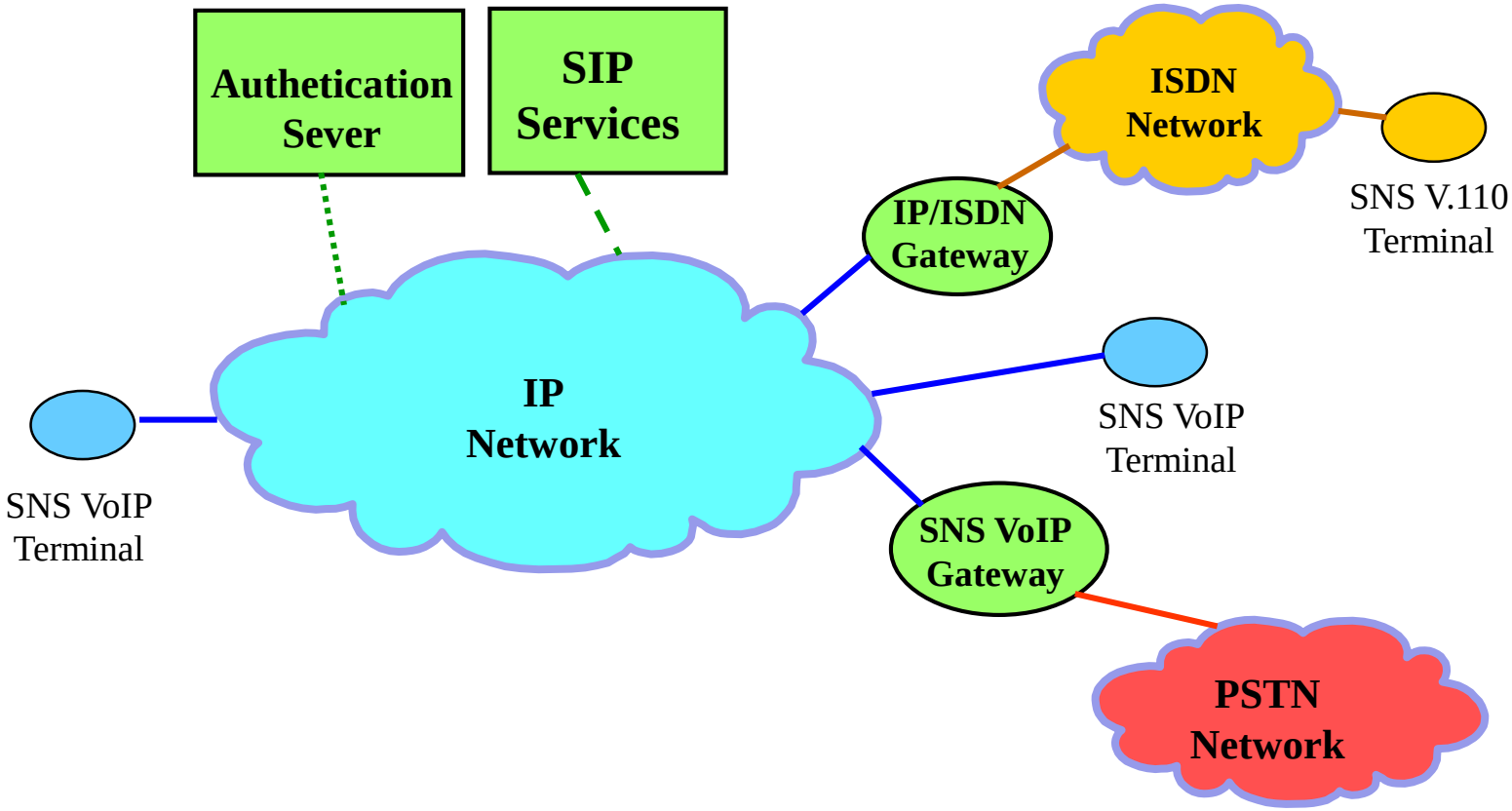
SNS wykorzystuje podstawowe mechanizmy oraz modułową architekturę SCIP do:

- **zestawiania bezpiecznych kanałów komunikacyjnych przez sieci heterogeniczne**

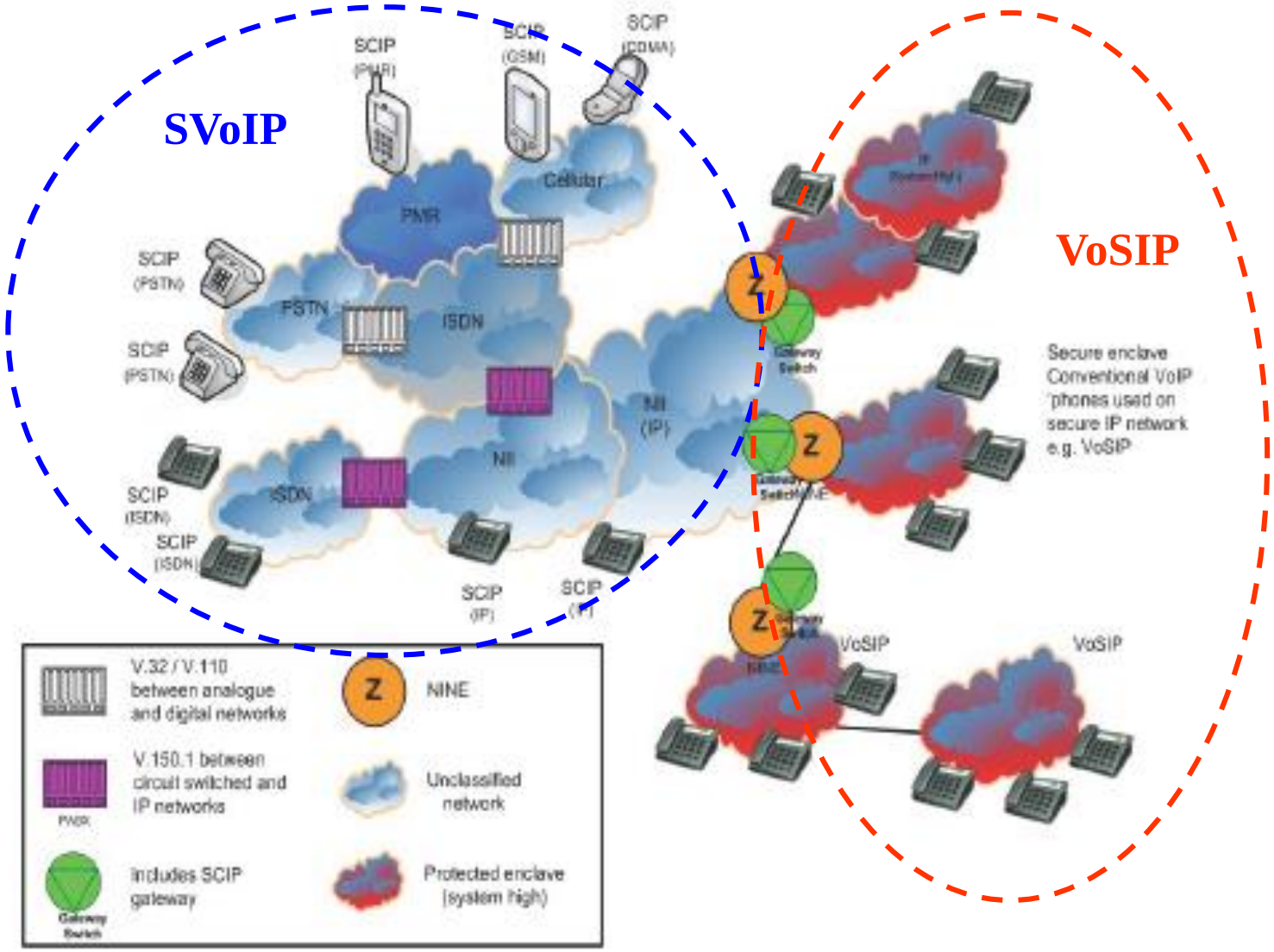


- **stosowania narodowych programów (algorytmów) kryptograficznych**
- **szyfrowania połączeń głosowych (także danych SMS) w układzie PtP i PtMP**

SNS over IP Network



SVoIP and VoSIP systems in NATO (Source: NCIA, conference proceedings)



(G. Elzingi, NATO)

Technologia proponowane przez NATO IICWG
(International Interoperability Communications Working Group)

Od 1998:
Future NarrowBand Digital Terminal (propozycja NSA dla bezpiecznej wąskopasmowej łączności E2E w sieciach wojskowych i służb państwowych

Od 2004:
Secure Communications Interoperability Protocol (protokół zaproponowany do stosowanie przez państwa NATO dla bezpiecznej łączności E2E w sieciach wojskowych i służb państwowych)

SCIP

Multi-Community/Multi-Level/Multi-Network Security Protocol

„BI-SC SECURE C2 DATA STRATEGY” (SDS) – NATO, 2010

Dokument przedstawia strategię bezpiecznej komunikacji dla systemów C2 wspieranych przez NEC (Network Enabled Capabilities) w przyszłych operacjach i misjach Sojuszu.

SDS omawia różnorodne działania ukierunkowane na wsparcie:

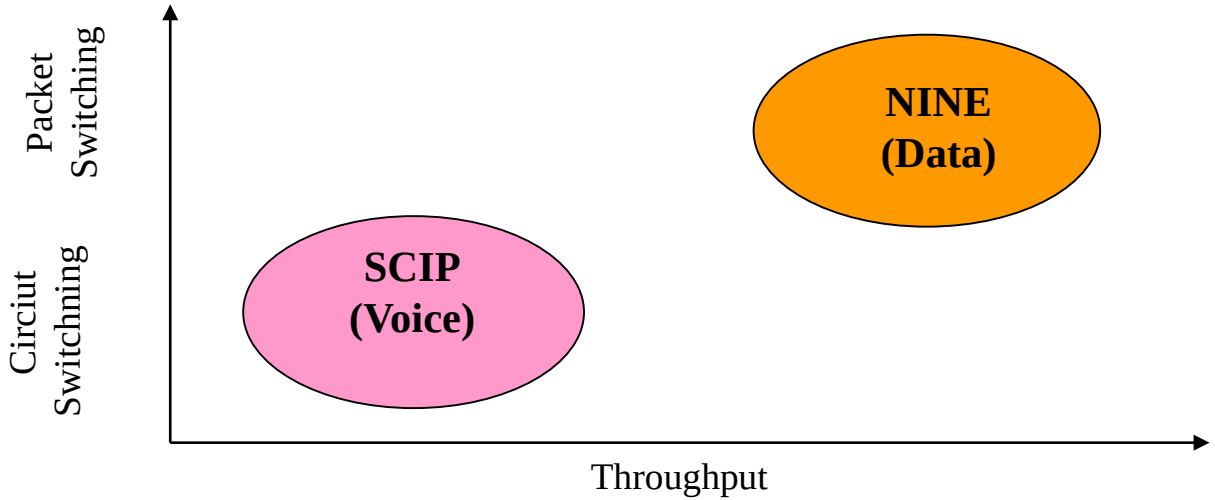
- **Protected Core Networking,**
- **Coherent Security Management,**
- **Coherent Cyber Defence,**
- **Trusted Automated Data Management,**
- **Trusted Data Exchange.**

proponując zastosowanie dwóch rozwiązań:

- **NINE – NATO IP Network Encryption**
- **SCIP - Secure Communications Interoperability Protocol**

dla zapewnienia bezpiecznej komunikacji typu „End-to-End” w sieciach heterogenicznych dla wsparcia usług „Voice, Video, Data” z wykorzystaniem protokołu IP (IPSec).

Secure Communications Interoperability Protocol (SCIP) - ?



- **NINE - odnosi się głównie do transmisji danych z uwzględnieniem aspektów kryptograficznych i bezpieczeństwa łączności z wykorzystaniem protokołu IPsec,**
- **SCIP - określa całe spektrum zagadnień związanych z urządzeniami końcowymi, normalizując sposób cyfryzacji sygnałów mowy, transmisji i utajniania. Normalizowane są także procedury sygnalizacyjne, a dane mogą być transmitowane przez dowolne medium, zależne od typu terminala (np. radiostacja osobista, radiostacja KF, telefon GSM, telefon VoIP, itp.). Konsekwencją stosowanie SCIP jest także możliwość ujednolicenia architektur wyżej wymienionych terminali, w tym radiostacji.**

Dlaczego SCIP?

Główne funkcjonalności protokołu SCIP dotyczą bezpiecznej komunikacji przez heterogeniczne sieci telekomunikacyjne za pośrednictwem protokołu IP (IPv4, IPv6):

- **wymaga niewielkich przepustowości dzięki kodekowi (MELPe) o szybkości 2,4 Kbps, co zapewnia łączność poprzez wąskopasmowe środki radiowe KF/UKF, a w przypadku dostępnych większych zasobów pasma (środki radiowe szerokopasmowe) stosowany jest kodek G.729D (7,2 Kbps);**
- **jest projektowany do pracy simpleksowej oraz komunikacji PtP lub PtMP, co dobrze odpowiada specyfice systemów mobilnych;**
- **integralną częścią protokołu jest komponent kryptograficzny (kryptografia koalicyjna, misyjna lub narodowa);**
- **w przypadku dostępnych większych przepustowości umożliwia transmisję danych multimedialnych w układzie typu „End to End" z szybkością do 10 Mbps.**

Podstawowe dokumenty normalizacyjne dla SCIP

SCIP zawiera cztery podstawowe komponenty:

1. **Voice Compression (kodeki foniczne)**
   – wykorzystanie kodeka MELP (2,4Kbit/s) lub G.729D (7,2 Kbps);

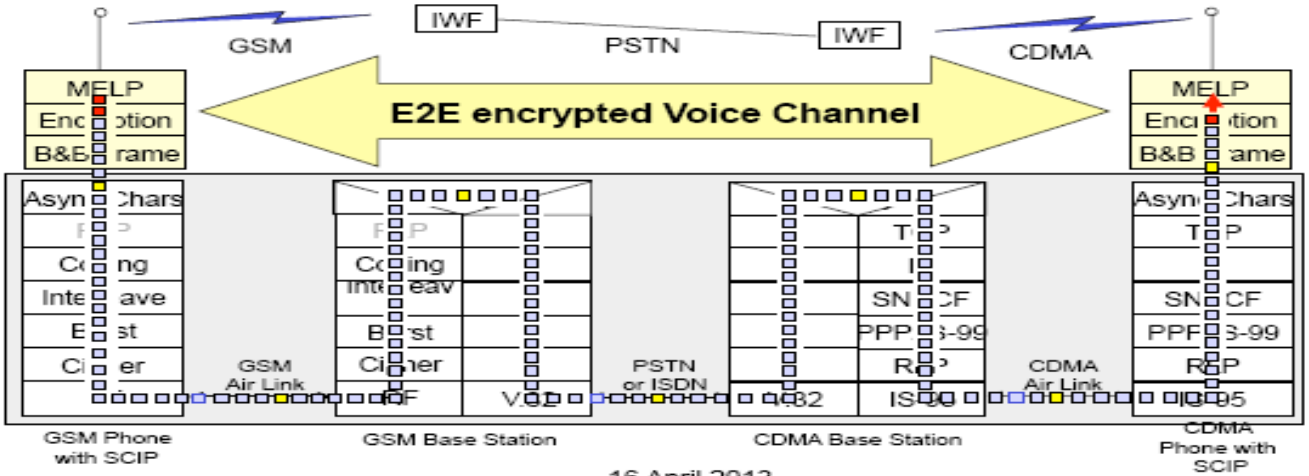
2. **Encryption (dokument SCIP 231)**
   – w urządzeniach SCIP stosowane jest szyfrowanie danych dla każdego połączenia;

2. **Key Management Infrastructure (dokument SCIP 120)**
   – zestawienie bezpiecznego połączenia realizowane jest w oparciu o klucz publiczny (klucze TEK)

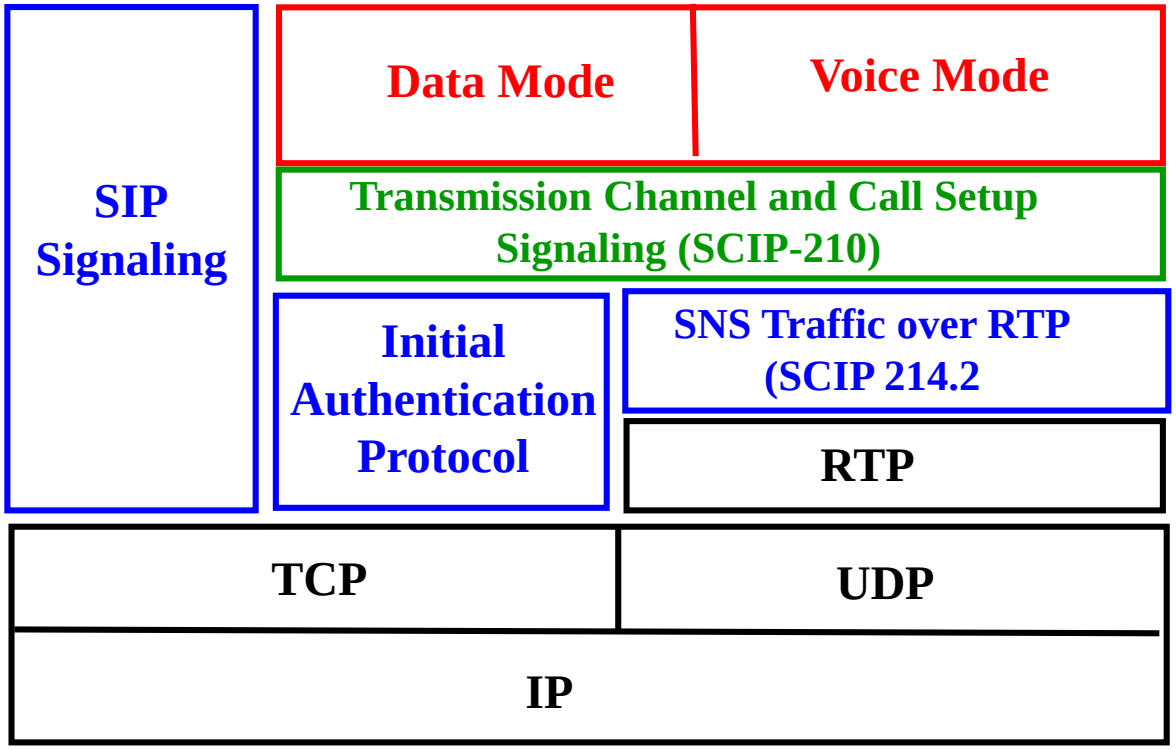
4. **Signaling Plan (SCIP 210)**
   – zawiera ujednolicone procedury zestawiania połączenia, przy czym dla łączności fonicznej wysyłany jest strumień ramek MELPe/G.729D a dla transmisji danych wykorzystywana jest procedura ARQ. W trakcie sygnalizacji przekazywana jest także informacja o rodzaju szyfrowania (koalicyjne, misyjne lub narodowe).

Idea SCIP

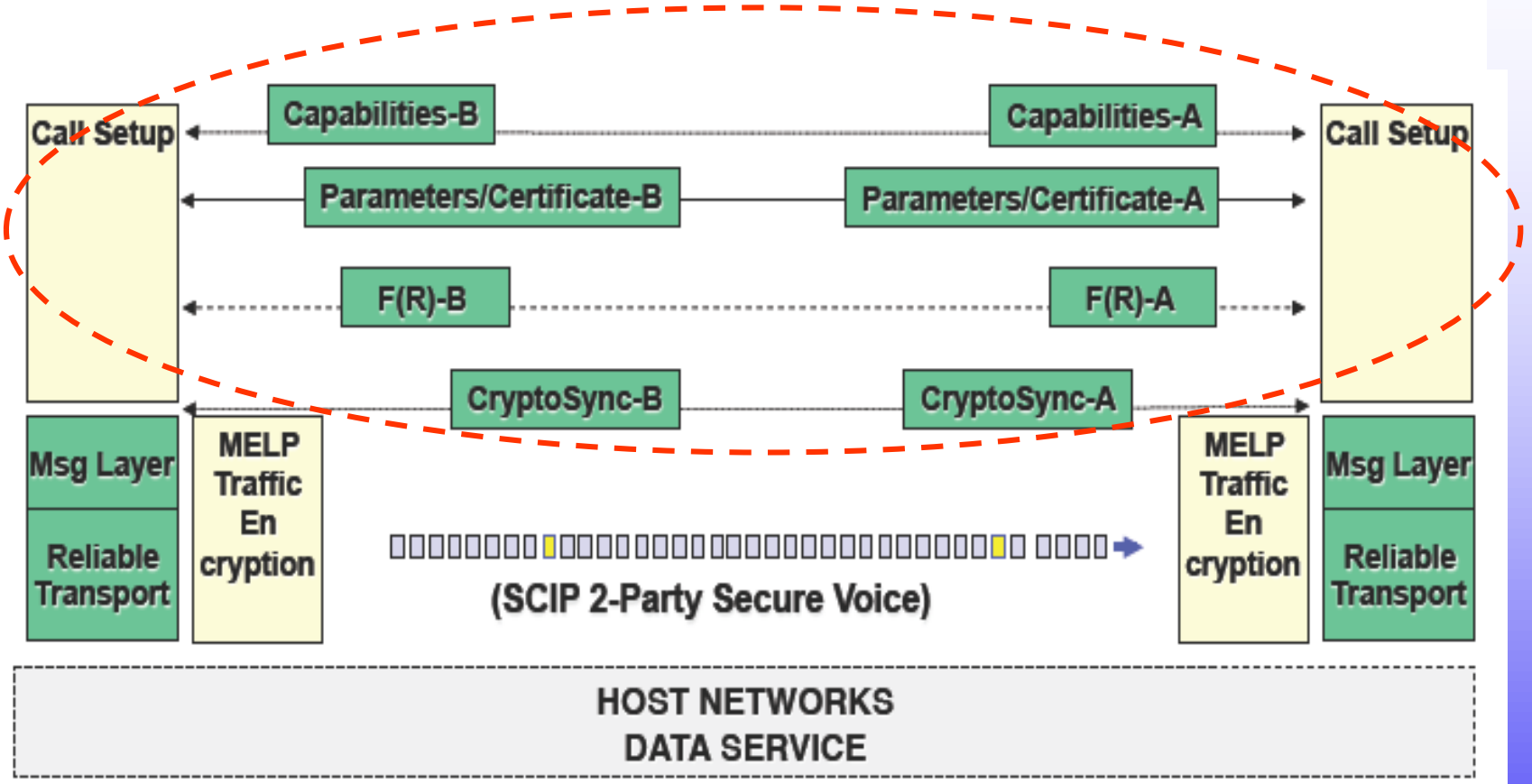
- Definiowanie kanałów dla sygnalizacji i szyfrowanych danych użytkownika realizowane jest na poziomie warstwy aplikacji (Layer 7)
- Minimalne wymagania transmisyjne dla technik i protokołów komunikacyjnych poniżej warstwy sieciowej (Layer 3)
- Kanały SCIP zapewniają własny system sterowania błędami (SCIP Reliable Transport Channel)
- Szyfrowanie danych użytkownika przez kanał SCIP z minimalnymi wymaganiami na pasmo (przepływność) – stosowanie kodeków Voice: MELP, G729,…
- Szyfrowanie typu E2E (wymagana transparentność bitowa kanału dla sygnalizacji i danych)
- Kanały SCIP mogą być transportowane zarówno przez sieci z komutacją kanałów jak przez sieci z komutacją pakietów (IP)



SCIP – Protocol stack



Standaryzacja protokołów dla różnych communities



SCIP: NATO planning

Future SCIP systems of NATO:

- NATO already operates SCIP systems in the Afghan Mission Network

- NATO Cryptographic Interoperability Strategy provides for use of SCIP both NATO RESTRICTED as also for NATO SECRET

- NATO will „secure language" in their future infrastructures by both

Secure Voice over IP (SVoIP $\Rightarrow$ SCIP)

as well as through

Voice over Secure IP (VoSIP $\Rightarrow$ Network Security)

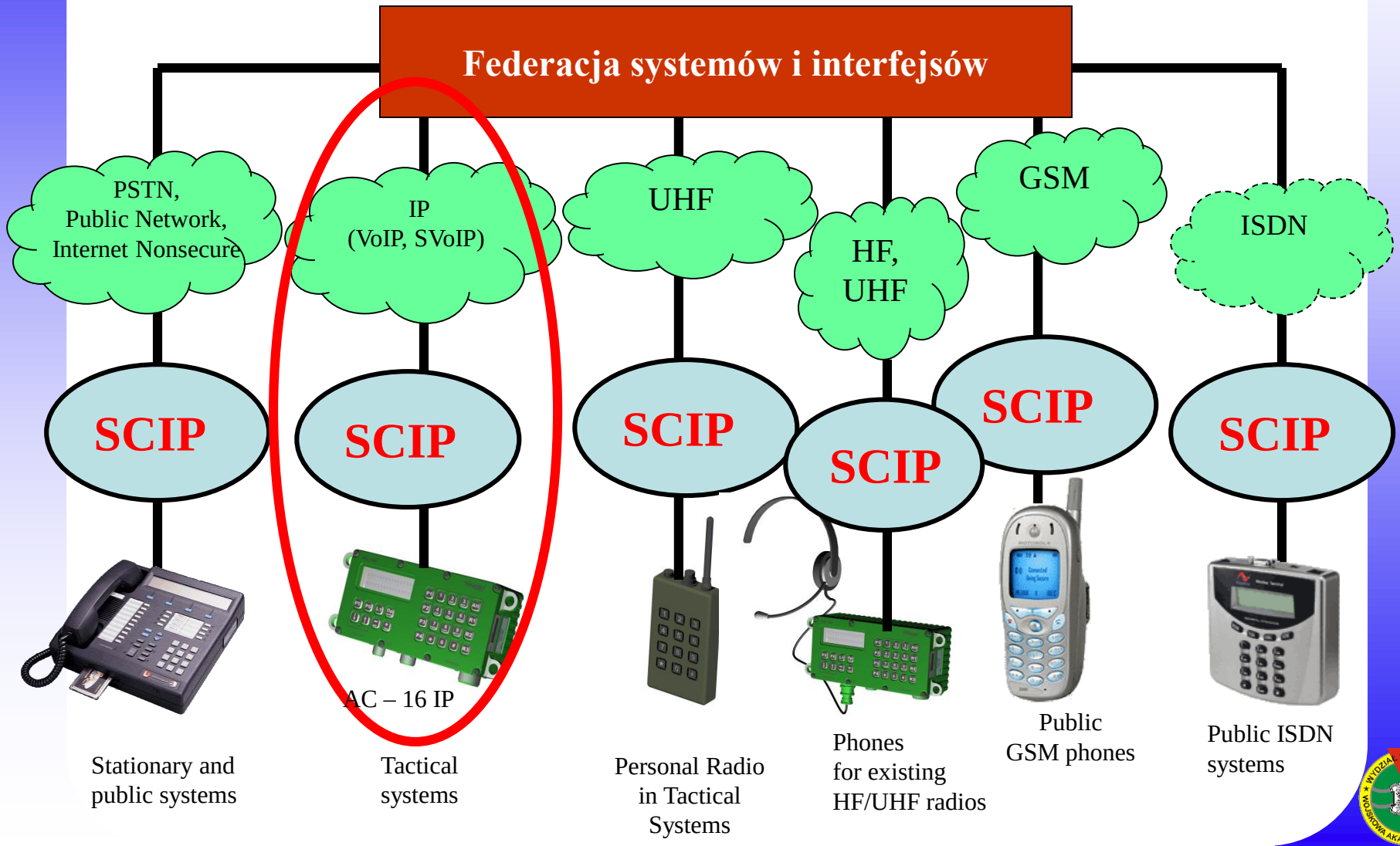
Zamierzenia NATO w kontekście rozwoju bezpiecznej łączności fonicznej

W styczniu 2012r. NC3B przyjął strategię bezpiecznej łączności fonicznej *„NATO Secure Voice Strategy”*, która zakłada m. in.:

- **wycofanie z eksploatacji do końca 2013 r. w strukturach NATO oraz państwach członkowskich systemu STU-IIB wraz z KDC (Key Distribution Center),**
- **wycofanie systemu NISE *(NATO Secure ISDN Equipment)* jako technologii nieperspektywicznej,**
- **powszechne stosowanie technologii IP *(VoSIP, SVoIP)* oraz stosowanie terminali SCIP,**
- **interoperacyjność pomiędzy występującymi technologiami sieciowymi będzie zapewniona poprzez stosowanie getway’ów SCIP.**

Koncepcja ujednolicenia terminali i radiostacji w technologii SCIP

Ujednolicenie ⇒ dotyczy procedur sygnalizacji, cyfryzacji mowy i kryptografii.



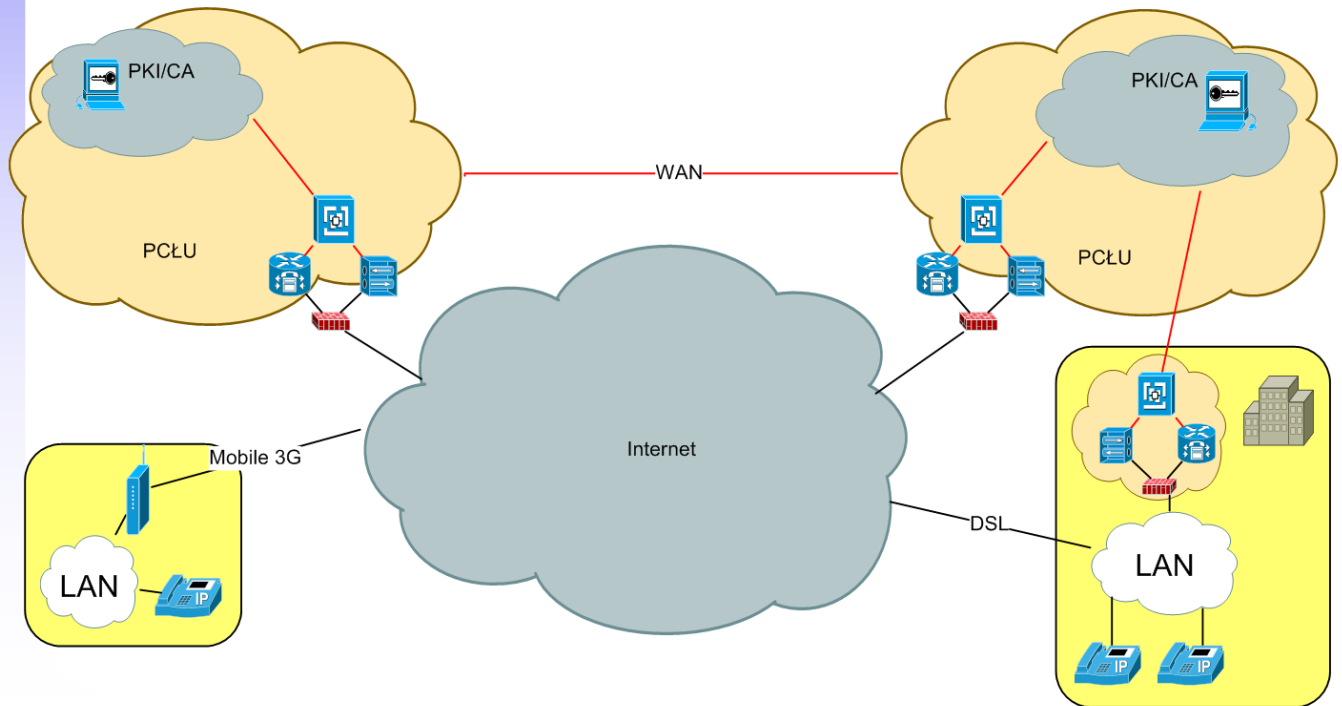
Program NCBiR INNOTECH (ścieżka programowa IN-TECH)

Konsorcjum: - WAT (WEL - IT)
- Asseco Poland S.A.
- Transbit Sp. z o.o.

Projekt pt:

„Wykonanie prototypu bezpiecznego systemu do przesyłania danych pomiędzy różnymi sieciami niejawnymi z wykorzystaniem sieci publicznych”

Okres realizacji: 2013 - 2015



Narodowe Centrum Badań i Rozwoju

Program NCBiR PBS (III konkurs, ścieżka programowa A - wniosek

Konsorcjum: - WAT (WEL – IT, WCY)
- Transbit Sp. z o.o

Projekt pt.:

„Implementacja bezpiecznego systemu komunikacji osobistej w sieciach otwartych (publicznych) z wykorzystaniem protokołu SCIP poprzez interfejs Bluetooth”

Okres realizacji: 2015 - 2017

Dziękuję za uwagę