

## TERMINAL SCIP

Urządzenie jest rezultatem projektu rozwojowego Nr O R00 0069 07, pt. „Kryptografia wykorzystująca krzywe eliptyczne w zastosowaniach do terminali telefonicznych i radiostacji IP przeznaczonych do pracy w sieciocentrycznych systemach koalicyjnych i narodowych” (29.06.2009 – 29.06.2011) w ramach konsorcjum Nauki i Przemysłu Wojskowej Akademii Technicznej i firmy TRANSBIT Sp. z o.o. Istotą projektu było opracowanie demonstratora - prototypu terminala telefonicznego SCIP do pracy poprzez sieci Ipv4 oraz IPv6, który mógłby wykorzystywać systemy telekomunikacyjne o małych przepustowościach, w tym środki radiowe KF/UKF, i być stosowany w obiektach dowódczo-sztabowych różnych szczebli. Terminal był tak zaprojektowany, aby możliwe było stosowanie dwu różnych metod bezpieczeństwa kryptograficznego: metody określonej przez standardy SCIP (przy pracy koalicyjnej) oraz metody narodowej, przy czym może być wykorzystany także do zastosowań specjalnych w sferze cywilnej. Opracowane rozwiązanie jest pierwszym na świecie tego typu terminalem SCIP posiadającym cechy użytkowe.



Prototyp terminala telefonicznego (zgodnie z zaleceniami SCIP) zawiera następujące elementy:

Przetwornik (cyfryzator) analogowego sygnału mowy w postaci procesora sygnałowego o dużej wydajności, stosujący algorytm pracy wokodera z predykcją liniową i mieszanym sposobem wzbudzenia (ang. Mixed Excitation Linear Prediction-enhanced).

Podwójny układ kryptograficzny bądź też dwa oddzielne układy kryptograficzne oparte na teorii krzywych eliptycznych Menezesa (ang. Eliptic Curve Menezes-Qu-Vanstone). Jeden z układów przeznaczony byłby do pracy koalicyjnej i wykonany zgodnie z zaleceniami SCIP, natomiast drugi mógłby pracować w systemach narodowych i byłby opracowany i wykonany zgodnie z obowiązującymi przepisami.

Układ pakowania utajnionych danych w pakiety IP wraz z odpowiednimi elementami sygnalizacji i sterowania, pracujący w dwu trybach: koalicyjnym i narodowym.

Opracowane rozwiązanie w pełni wpisuje się w ogólne zalecenia wprowadzenia technologii SCIP w państwach członkowskich NATO. Perspektywy produkcji obejmują w związku z tym potrzeby wyposażenia co najmniej Polskich Sił Zbrojnych.

Opracowane rozwiązanie terminala SCIP jest na dzień dzisiejszy jedynym na świecie przystosowanym do instalacji w wozach bojowych. Od marca 2013 SCIP stał się normą obowiązującą wszystkie kraje NATO i od 2016 roku łączność interoperacyjna między krajami-członkami musi być realizowana w oparciu o urządzenia tego typu. Polski przemysł i ośrodek badawczy, jakim jest WAT, uzyskały w toku konstrukcji terminala przewagę czasową nad innymi krajami. Przewaga ta powinna zostać wykorzystana do uzyskania efektów ekonomicznych w postaci szerszego rynku sprzedaży tego urządzenia.

Terminal SCIP został wyróżniony brązowym medalem na 112. Międzynarodowych Targach Wynalazczości Concours-Lepine 2013, Paryż, 29.04.–5.05.2013, Nagrodą zespołową Rektora Wojskowej Akademii Technicznej oraz medalem Eureka na 62. Międzynarodowych Targach Wynalazczości, Badań Naukowych i Nowych Technik BRUSSELS INNOVA, 13-17.

### Konsorcjum:

WOJSKOWA AKADEMIA TECHNICZNA  
im. Jarosława Dąbrowskiego  
Wydział Cybernetyki  
Institute of Mathematics and Cryptology  
Warszawa 00-908, Gen. S. Kaliskiego 2  
tel.: +48 22 683 96 87, fax: +48 22 683 79 19  
e-mail: jgawinecki@wat.edu.pl, www.wat.edu.pl

TRANSBIT Ltd.  
02-968 Warszawa,  
ul. Przyczółkowa 109 A  
TEL.: +48 22 550 48 00, FAX: +48 22 550 48 10  
biurotransbit.com.pl, www.transbit.com.pl



Wydział Cybernetyki  
Instytut Matematyki i Kryptologii  
Piotr Kacprzyk  
tel. +48 22 683 95 56  
e-mail: pkacprzyk@wat.edu.pl

