



**TechLab 2000**  
R & D Company

# Cygnus Titanium

Cyfrowy telefon oraz modem szyfrujący



## BEZPIECZNA ŁĄCZNOŚĆ

**Cygnus Titanium** jest opracowanym i wykonanym w Polsce aparatem szyfrującym kierowanym do odbiorców o wysokich wymaganiach w dziedzinie zabezpieczeń jak i do zastosowań specjalnych: policja, wojsko. Przeznaczony jest dla użytkowników, którzy chcą chronić przesyłane dane, gdyż stanowią one tajemnicę handlową, jak również dla tych którzy działają w myśl ustawy o ochronie informacji niejawnych. Zapewnia poufność oraz uwierzytelnienie sesji łączności do klauzuli „Poufne”. Daje możliwość pracy nie tylko w trybie szyfrowym, ale również nawiązania połączenia z dowolnym innym aparatem telefonicznym w trybie jawnym. Wspiera wszystkie usługi oferowane w polskich sieciach publicznych, a ponadto umożliwia szyfrowane połączenie trójstronne z aparatami analogowymi i cyfrowymi rodziny Cygnus. Przeprowadzone testy potwierdziły jego poprawną pracę także na łączach IP i satelitarnych. Jest interoperacyjny z innymi rozwiązaniami telekomunikacyjnymi projektowanymi przez TechLab 2000 obejmującymi telefony analogowe, cyfrowe oraz GSM. Proces uwierzytelnienia stron połączenia odbywa się z wykorzystaniem mechanizmów Infrastruktury Klucza Publicznego. Nośnikami danych użytkownika są karty elektroniczne, zaś same dane generowane są przez Stację Zarządzania Kluczami TEACUP. Cygnus Titanium to trzy urządzenia w jednej obudowie: luksusowy aparat ISDN, telefon szyfrujący, modem (standardowy oraz szyfrowy). Urządzenie odznacza się prostotą obsługi, a od użytkownika nie wymaga się specjalistycznej wiedzy w dziedzinie kryptografii.

## WAŻNE

CERTYFIKAT DO „POUFNE”

BEZPIECZEŃSTWO POŁĄCZEŃ

WYSOKIEJ KLASY KRYPTOGRAFIA

PRZEBADANE ZABEZPIECZENIA

LATWOŚĆ OBSŁUGI

INTEROPERACYJNOŚĆ

WSPARCIE DLA USŁUG ISDN

PRACUJE NA ŁĄCZACH IP I SAT

## WYBRANE FUNKCJE APARATU

- Praca w trybie jawnym lub szyfrowania połączenia głosowego oraz transmisji danych
- Identyfikacja numeru dzwoniącego (CLIP/CLIR)
- Książka telefoniczna na 1000 numerów
- Automatyka sekretarka
- Lista ostatnio wybieranych numerów
- Nagrywanie przeprowadzanych rozmów (wyłącznie w trybie jawnym) oraz dedykowanych powitań
- Lista połączeń odebranych i nieodebranych
- Przesyłanie prostych wiadomości tekstowych (UUS-1)
- Zestawianie połączeń trójstronnych (3PTY) – w trybie jawnym oraz szyfrowanym
- Informacje o koszcie bieżącego połączenia (AOC)
- Obsługa przekierowań
- Automatyczne powtarzanie wybierania numeru (ARD)
- Automatyczne dodawanie numeru operatora oraz specyficznych prefiksów
- Praca w trybie głośno mówiącym
- Wyciszenie (MUTE)
- Menu programowe z podziałem funkcjonalności na standardową oraz kryptograficzną
- Programowanie z poziomu użytkownika większości funkcji aparatu
- Szerokie możliwości konfiguracji kryptograficznej
- Rejestr aktywności urządzenia oraz rejestr bezpieczeństwa
- Bezpieczna aktualizacja oprogramowania dostarczanego przez producenta
- Zabezpieczenia na czas transportu oraz magazynowania
- Praca w trybie awaryjnym bez zasilania sieciowego (1 godzina)
- Klawiatura alfanumeryczna z przyciskami funkcyjnymi (repetycja numeru, praca głośnomówiąca)
- Wyświetlacz graficzny 128x64
- Obudowa metalowa z plastikowym panelem górnym
- Czytnik kart elektronicznych sterowany z klawiatury

## SZYFROWANIA POŁĄCZENIA

- Podczas nawiązywania połączenia szyfrowanego aparat automatycznie ustala najwyższy możliwy poziom kryptograficzny, na podstawie danych odczytanych z karty użytkownika, lub ewentualnie na podstawie jej braku.
- Połączenie szyfrowane pomiędzy aparatami cyfrowymi nie powoduje utraty jakości głosu (kodowanie transparentne) oraz wyczuwalnego opóźnienia.
- Przy połączeniu z aparatami analogowymi jakość zakodowanego głosu odpowiada technologii wykorzystywanej w sieciach komórkowych.
- Przy połączeniach ustalonych na poziomie „Poufne” stosowany jest niejawni, opracowany przez DBTI ABW, algorytm symetryczny.
- W pozostałych przypadkach szyfrowanie algorytmem symetrycznym AES 256 lub AES 192.
- Uzgadnianie kluczy sesyjnych schematem Diffie-Hellmana do 4096 bitów.
- Uwierzytelnienie z wykorzystaniem RSA do 4096 bitów.
- Umożliwienie przeciwdziałania atakom typu „maskarada”, przy braku danych użytkownika.
- Wysokiej jakości generator losowy oparty na zjawisku fizycznym.
- Nawiązanie połączenia w trybie jawnym, przejście w tryb szyfrowania połączenia przez naciśnięcie jednego przycisku, czas przejścia od 0,5 do kilku sekund w zależności od rodzaju połączenia oraz typu uwierzytelnienia (np: Diffie-Hellman 3072 bity, dane użytkownika 2048 podpisane kluczem 4096, całkowity czas nawiązywania sesji szyfrowanej 3 sekundy).
- Automatyczna propagacja list unieważnionych certyfikatów.
- Informacja akustyczna i wizualna o procesie uwierzytelnienia oraz przejściu w tryb pracy niejawniej.
- Zaimplementowane mechanizmy zabezpieczeń antyemisyjnych oraz antypenetracyjnych.



## PRACA W TRYBIE POŁĄCZENIA DANYCH

- Urządzenie automatycznie rozpoznaje typ urządzenia zdalnego i w zależności od tego realizuje połączenie jawne lub szyfrowane.
- Wykorzystuje protokół multilink PPP ze statycznym lub dynamicznym przydziałem pasma.
- Realizuje podzbiór standardu V.34 w trybie pracy szyfrowej przy połączeniach z aparatami analogowymi.
- Połączenie z komputerem odbywa się za pomocą interfejsu USB 2.0 full-speed.

## SYSTEM ŁĄCZNOŚCI SZYFROWANEJ

Cygnus Titanium stanowi element systemu łączności niejawniej Sylan, na który składają się również:

- Stacja zarządzania kluczami TEACUP odpowiedzialna za generację danych w obrębie infrastruktury klucza publicznego.
- Karty elektroniczne jako nośniki danych użytkownika.
- Urządzenia końcowe: aparaty analogowe Cygnus Gold, Cygnus Platinum; aparaty cyfrowe Cygnus Diamond, Cygnus Titanium, Cygnus Titanium Plus; aparaty GSM Xaos Gamma, Krypton.