

# Cygnus Diamond

Cyfrowy telefon oraz modem szyfrujący



## BEZPIECZNA ŁĄCZNOŚĆ

Cygnus Diamond jest opracowanym i wykonanym w Polsce aparatem szyfrującym kierowanym do odbiorców o wysokich wymaganiach w dziedzinie zabezpieczeń, oczekujących zaawansowanej funkcjonalności telekomunikacyjnej, a przy tym niskich kosztów zakupu. Przeznaczony jest dla użytkowników prywatnych, jak i instytucjonalnych, którzy chcą chronić przesyłane dane, gdyż stanowią one tajemnicę handlową, jak również dla tych którzy działają zgodnie z ustawą o ochronie informacji niejawnych. Zapewnia poufność oraz uwierzytelnienie sesji łączności do poziomu klauzuli „Zastrzeżone”. 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. Jest interoperacyjny z innymi rozwiązaniami telekomunikacyjnymi projektowanymi przez TechLab 2000 obejmującymi telefony analogowe, cyfrowe oraz GSM. Cygnus Diamond to trzy urządzenia w jednej obudowie: luksusowy aparat ISDN, telefon szyfrujący, modem (standardowy oraz szyfrujący). Urządzenie odznacza się prostotą obsługi, a od użytkownika nie wymaga się specjalistycznej wiedzy w dziedzinie kryptografii.

## WAŻNE

CERTYFIKAT DO „ZASTRZEŻONE”

BEZPIECZEŃSTWO POŁĄCZEŃ

WYSOKIEJ KLASY KRYPTOGRAFIA

ŁATWOŚĆ OBSŁUGI

INTEROPERACYJNOŚĆ

WSPARCIE DLA USŁUG ISDN

NISKA CENA

## WYBRANE FUNKCJE APARATU

- Praca w trybie jawnym lub szyfrowania połączenia głosowego oraz transmisji danych
- Identyfikacja numeru dzwoniącego (CLIP/CLIR)
- Książka telefoniczna na 1000 numerów
- Automatyczna 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)
- Wyświetlacz graficzny 128x64
- 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)
- Zaimplementowane mechanizmy zabezpieczeń antyprzenikalnych.
- Klawiatura alfanumeryczna z przyciskami funkcyjnymi (repetycja numeru, praca głośnomówiąca)

## SZYFROWANIA POŁĄCZENIA

- Szyfrowanie algorytmem symetrycznym AES 256 lub AES 192.
- Uzgadnianie kluczy sesyjnych schematem Diffie-Hellmana do 4096 bitów.
- Uwierzytelnienie z wykorzystaniem funkcji skrótu (zabezpieczenie przed atakiem typu „maskarada”).
- 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.
- Nawiązanie połączenia w trybie jawnym, przejście w tryb szyfrowania połączenia przez naciśnięcie jednego przycisku, czas przejścia poniżej 1 sekundy.
- Informacja akustyczna i wizualna o procesie uwierzytelnienia oraz przejściu w tryb pracy niejawnej.
- Dane kryptograficzne potrzebne w procesie uzgadniania klucza pozyskiwane z generatora pseudolosowego.
- Automatyczna wymiana kluczy sesyjnych podczas połączenia.
- Zamazywanie danych kryptograficznych wykorzystywanych w zakończonym połączeniu.



## 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 Diamond stanowi element systemu łączności niejawnej 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.

