

# Krypton

Szyfrujący telefon GSM



## BEZPIECZNA ŁĄCZNOŚĆ BEZPRZEWODOWA

**Krypton** jest opracowanym i wykonanym w Polsce komórkowym telefonem 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 poziomu „Poufne”. Daje możliwość pracy nie tylko w trybie szyfrowanym, ale również funkcjonuje jako standardowy aparat komórkowy. Posiadając ekstremalnie wyśrubowane parametry kryptograficzne pozwala na niezwykle szybkie nawiązywanie połączeń kryptograficznych przekazując jednocześnie głos znakomitej jakości bez odczuwalnych opóźnień. 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. Dzięki specjalnej technologii zabezpieczeń aparat sam staje się nośnikiem kluczy użytkownika i współpracuje ze Stacją Zarządzania Kluczami TEACUP. Krypton to trzy urządzenia w jednej obudowie: luksusowy aparat GSM, telefon szyfrujący, modem (standardowy EDGE/GPRS, CSD oraz szyfrujący CSD). Urządzenie odznacza się prostotą obsługi, a od użytkownika nie wymaga się specjalizowanej wiedzy w dziedzinie kryptografii.

## WAŻNE

CERTYFIKAT DO „POUFNE”

WYSOKIEJ KLASY KRYPTOGRAFIA

UNIKATOWE ZABEZPIECZENIA

ŁATWOŚĆ OBSŁUGI

INTEROPERACYJNOŚĆ

DŁUGI CZAS PRACY

SZYBKOŚĆ DZIAŁANIA

NIEZAWODNOŚĆ

## PODSTAWOWE PARAMETRY

- Cztery zakresy GSM: 900/1800/950/1900
- GPRS/EDGE klasa 10
- Czas rozmów (jawne i szyfrowane) 5 godzin, czas czuwania 200 godzin
- Książka telefoniczna na 5000 numerów przechowywana w sposób zabezpieczony
- Szyfrowany system plików
- Zabezpieczenie przed kradzieżą
- Możliwość wysyłania zaszyfrowanych wiadomości SMS
- Lista połączeń odebranych i nieodebranych
- Wszelkie informacje o aktywności abo- nenta (numery wybierane, odebrane, nieodebrane, SMSy i inne) przechowywane w sposób zabezpieczony
- Praca w trybie głośno mówiącym
- Wydzielone i zabezpieczone menu ustawień kryptograficznych
- Rejestr aktywności urządzenia oraz rejestr bezpieczeństwa
- Bezpieczna aktualizacja oprogramowania dostarczanego przez producenta
- Konfiguracja oraz zarządzanie przez www
- Zabezpieczenia na czas transportu oraz magazynowania
- Wyświetlacz graficzny 31,2x41,2mm, aktywna matryca TFT 176x220 pikseli
- Wymiary 116x51x24mm
- Bateria 1000mAh Li-Ion
- W komplecie gumowy pokrowiec zabezpieczający, ładowarka, kabel USB do transmisji danych oraz konfiguracji PKI

- Aparat stanowi zabezpieczony nośnik danych PKI użytkownika, ładowanych ze Stacji Zarządzania Kluczami TEACUP.
- Podczas nawiązywania połączenia szyfrowanego aparat automatycznie ustala najwyższy możliwy poziom kryptograficzny, na podstawie danych użytkownika.
- Połączenie szyfrowane nie powoduje utraty jakości (algorytm kompresji AMR).
- Połączenie szyfrowane nie wprowadza wyczuwalnych opóźnień (450 ms przy połączeniach pomiędzy aparatami Krypton, mniej niż 300 ms z aparatami Cygnus Titanium).
- Szyfrowanie algorytmem symetrycznym AES 256.
- Uzgadnianie kluczy sesyjnych z wykorzystaniem eliptycznego schematu Diffie-Hellmana do 521 bitów.
- Uwierzytelnienie z wykorzystaniem RSA do 4096 bitów, akcelerowane sprzętowo.
- Umożliwienie przeciwdziałania atakom typu „maskarada”, przy braku danych uwierzytelniających użytkownika, z wykorzystaniem funkcji skrótu.
- Zaawansowany algorytm pozyskiwania danych losowych, dla potrzeb algorytmów kryptograficznych.
- Rekordowo szybkie nawiązywanie połączenia szyfrowanego. Od 1.5s bez uwierzytelnienia RSA do typowo 6s z uwierzytelnieniem RSA (klucz użytkownika 2048 bitów, klucz urzędu 4096 bitów).
- Automatyczna i bezobsługowa propagacja list unieważnionych certyfikatów poprzez pobieranie odpowiednich danych z serwera LDAP oraz niezależnie poprzez wymianę tych informacji przy nawiązywaniu połączenia szyfrowanego.
- Informacja akustyczna i wizualna o procesie uwierzytelnienia oraz przejściu w tryb pracy niejawnej.
- Pełna informacja o uzyskanych parametrach kryptograficznych połączenia.
- Zaimplementowane unikatowe mechanizmy zabezpieczeń antypenetracyjnych.



## PRACA W TRYBIE SZYFROWANIA DANYCH

- Aparat umożliwia realizację połączeń w trybie danych (CSD/V.110) z innymi aparatami Krypton.
- Połączenie z komputerem odbywa się za pomocą interfejsu USB 2.0 full-speed.

## SYSTEM ŁĄCZNOŚCI SZYFROWANEJ

Krypton stanowi element systemu łączności niejawnej Sylan, na który składają się również:

- TEACUP - Stacja zarządzania kluczami odpowiedzialna za generację danych w obrębie infrastruktury klucza publicznego.
- Karty elektroniczne lub urządzenia przenośne (Krypton) 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.