

Szyfrujący telefon od Techlab 2000

<http://ipsec.pl/kryptografia/szyfrujacy-telefon-od-techlab-2000.html>

Firma Techlab 2000 wypuściła na rynek szyfrujący telefon GSM w całości montowany w Polsce, który dostępny będzie wkrótce w ofercie Orange.

Xaos jest czterosystemowym telefonem GSM (850/900/1800/1900) z obsługą GPRS i EDGE klasy 10. Rozmowy pomiędzy aparatami Xaos są szyfrowane algorytmem AES-256. Protokół wymiany klucza sesyjnego jest oparty o kryptografię krzywych eliptycznych (ECC) z wykorzystaniem krzywych co najmniej NIST P-224.

Wymiana klucza powoduje ok. 1,5 sekundowe opóźnienie przy nawiązywaniu połączenia. Szyfrowanie wprowadza opóźnienie w transmisji głosu rzędu 450 milisekund.

Szyfrowane są także wiadomości SMS, książka adresowa oraz rejestry połączeń.

Cena jednej sztuki w sprzedaży detalicznej bezpośrednio w Techlab 2000 wynosi ok. 1100 euro za sztukę, co jest konkurencyjną ceną za telefon szyfrujący tej klasy.

Techlab 2000 to firma, która kilka lat temu opracowała niejawną szyfr blokowy NASZ (Narodowy Algorytm Szyfrujący), używany do ochrony informacji niejawną na poziomie "ściśle tajne".

http://www.tl2000.com.pl/en/products/encrypting_gsm_phones
http://di.com.pl/news/26078,1,0,Polak_potrafi_telef
<http://www.securitystandard.pl/artykuly/58814/Xaos.upsilon.wymusza.zmiany.w.prawie.html>