

Łódź, 2014 r.

JNS Sp. z o.o.
ul. Wróblewskiego 18
93-578 Łódź
NIP: 725-189-13-94
tel. +48 42 209 27 01, fax. +48 42 209 27 02
e-mail: biuro@jns.pl

SZYFROWANIE POŁĄCZEŃ



JNS Sp. z o.o. z siedzibą w Łodzi, przy ul. Wróblewskiego 18, 93-578 Łódź, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi, XX Wydział Krajowego Rejestru Sądowego pod numerem KRS 0000228071. NIP 725-189-13-94 Wysokość kapitału zakładowego: 100 000, 00 PLN.

Str. 1/6

I. Opis rozwiązania

Kradzież informacji staje się coraz powszechniejszym problem. Dziś dotyczy on, już nie tylko wielkich korporacji, lecz także wszystkich:

- **przedsiębiorstw,**
- **samorządów, organów państwowych,**
- **a nawet osób prywatnych, mogących być narażonych na nieuczciwe działania konkurencji.**

Dzieje się tak z powodu coraz niższych cen podsłuchów i coraz większej dostępności urządzeń inwigilujących.



Policja notuje coraz więcej przypadków:

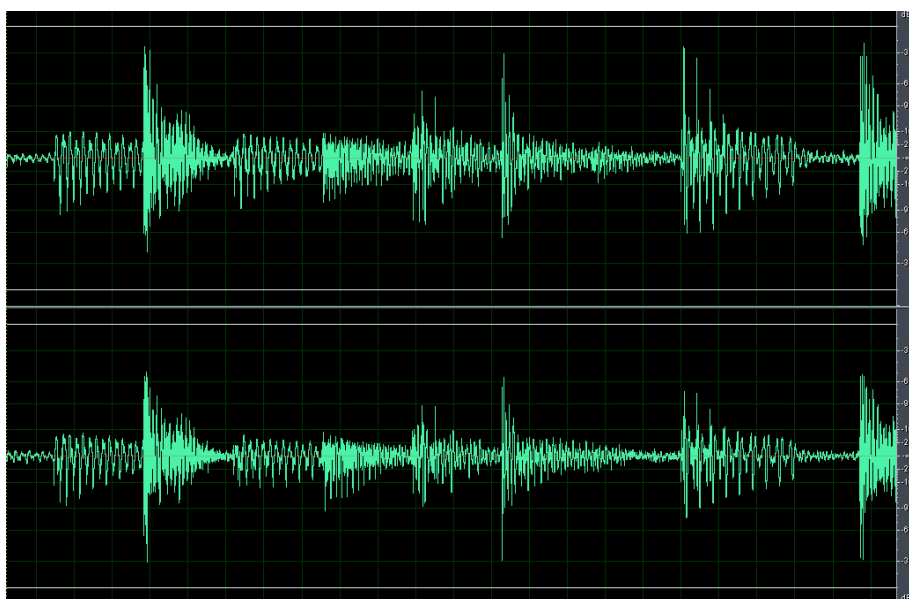
- **podśluchiwanie kadry zarządzającej przez pracowników w celu szantażu,**
- **wykradania poufnych informacji oraz sprzedawania tych informacji mediom bądź konkurencyjnym korporacjom.**

Z tego powodu firma JNS postanowiła poszerzyć swoją ofertę o system szyfrowania rozmów i dać swoim klientom, możliwość ochrony przed zagrożeniami związanymi z podsłuchami.

System szyfrowania rozmów oferowany przez firmę JNS posiada certyfikat NATO i jest stosowany między innymi przez rząd niemiecki.

II. Zalety rozwiązania urządzenia szyfrującego firmy JNS

Dzięki zastosowaniu rozwiązania proponowanego przez JNS klient w trosce o **bezpieczeństwo i jakość** swoich rozmów/wiadomości, nie musi już decydować się na **żaden kompromis**. W przeciwieństwie do źle wyglądających i rzucających się w oczy telefonów szyfrujących, telefony wykorzystujące szyfrowanie sprzętowe nie zwracają na siebie uwagi.



Prezentowane **urządzenie** (hardware) ma wygląd karty **micro SD**. Karta jest instalowana w telefonie, a nie jak w przypadku oprogramowania szyfrującego (software) w jego systemie operacyjnym. Dzięki takiemu rozwiązaniu wszelkiego rodzaju **wirusy i awarie software`u telefonu nie stanowią już zagrożenia dla odbywania bezpiecznych, szyfrowanych połączeń telefonicznych**.

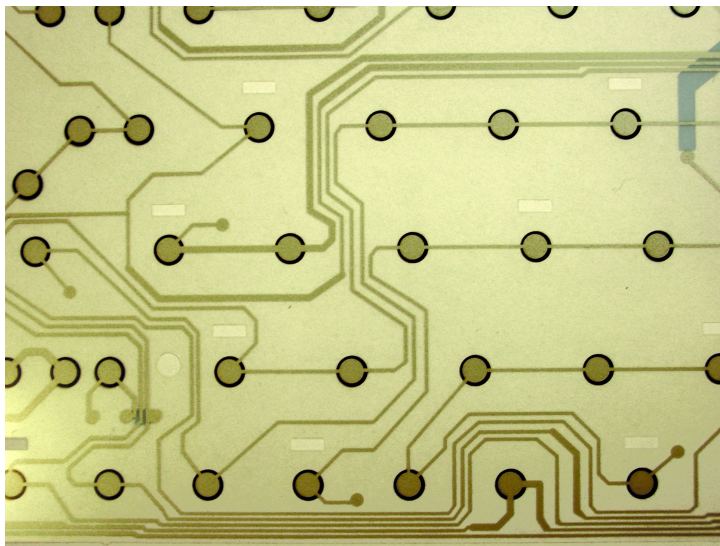
Inne zalety szyfrowania oferowanego przez JNS to:

- **certyfikat bezpieczeństwa NATO**, stale używany przez wysokich urzędników niemieckich,
- **szyfrowanie połączeń telefonicznych i wiadomości (SMS, E-mail)** oparto o technologię **SNS** uznaną za standard przez niemiecki Urząd ds. Bezpieczeństwa Informacji,
- wyeliminowanie zagrożenia wynikającego z niedoskonałości systemów operacyjnych telefonów,
- rozszerzanie pamięci telefonu,
- **brak możliwości ingerowania w oprogramowanie szyfrujące**,

- świetna jakość połączeń,
- szybka autoryzacja połączeń,
- **możliwość korzystania z bezpiecznych połączeń na wielu telefonach** poprzez przełożenie urządzenia w formie karty micro SD, bez konieczności wykupywania dodatkowych licencji,
- **możliwość szyfrowania połączeń stacjonarnych z telefonami w sieci ISDN,**
- łatwa, intuicyjna obsługa,
- **nie powoduje szybszego rozładowywania baterii telefonu,**
- kompatybilność z najnowszymi modelami telefonów Nokia.

III. Zasada działania urządzenia szyfrującego

Jest wiele możliwości przechwytywania rozmów telefonicznych/wiadomości. Z tego powodu szyfrowanie informacji **nie może opierać się wyłącznie na jednej metodzie zabezpieczenia naszej prywatności**. W celu ochrony poufności przesyłana mowa/wiadomość jest poddawana szyfrowaniu w telefonie użytkownika za pomocą **AES (Advanced Encryption Standard)** i klucza szyfrującego o długości 128 bitów.



Szyfrowanie rozmów odbywa się metodą „od końca do końca”. Oznacza to, że głos przebiega przez sieć komunikacyjną całkowicie zaszyfrowany od telefonu pierwszego rozmówcy do telefonu drugiego rozmówcy. Taki sposób zabezpieczenia **kompletnie uniemożliwia nieuczciwym osobom przechwycenie rozmowy, zarówno z powietrznego złącza transmisyjnego, jak również w obrębie przewodowej sieci telefonicznej**.

Przed rozpoczęciem szyfrowania połączenia pomiędzy telefonami rozmówców musi zostać uzgodniony klucz szyfrowy. Odbywa się to dzięki zastosowaniu wersji protokołu ECDH (Elliptic Curve Diffie-Hellman) wymagającego uwierzytelnienia. **Rozwiązanie tego typu pozwala na wykorzystanie krótszych kluczy i przyspieszenie obliczeń kryptograficznych przy zachowaniu najwyższego stopnia bezpieczeństwa.**



Ponadto proponowane przez JNS urządzenie zabezpiecza połączenia wykorzystując certyfikat oparty na uwierzytelnianiu użytkownika. Dla klienta oznacza to, że nikt nie będzie w stanie podszyć się pod jego rozmówcę. **Urządzenie zidentyfikuje strony komunikujące się ze sobą za pomocą ich tożsamości kryptograficznej (fingerprint) zawartej w certyfikatach użytkowników a nie za pomocą numerów ich telefonów.**

Urządzenie umożliwia również stosowanie systemu nazw domen do zabezpieczania rozmów wewnątrz organizacji. Jeżeli użytkownik zarejestruje nazwę domeny to zostanie ona wpisana do certyfikatów wszystkich użytkowników należących do tej konkretnej domeny i równocześnie stanie się integralną częścią tożsamości kryptograficznej każdego takiego użytkownika.



Każda nowa karta szyfrująca jest dodatkowo zabezpieczona kodem Zero-PIN. Jest to jednorazowy kod aktywacyjny karty stanowiący dowód na to, że nikt przed klientem z niej nie korzystał. Po podaniu Zero-PIN-u użytkownik jest proszony o podanie nowego, własnego numeru PIN, który będzie chronił kartę szyfrującą przed nieautoryzowanym użytkowaniem.

IV. Szyfrowanie połączeń stacjonarnych

Poza zabezpieczaniem przesyłanych informacji w sieci GSM możliwa jest także ochrona telefonów działających w sieci ISDN. Firma JNS oferuje trzy urządzenia umożliwiające szyfrowanie 1, 4 lub 30 telefonów stacjonarnych jednocześnie. System szyfrujący urządzeń współpracuje z tymi samymi kartami szyfrującymi jak te, które są używane w telefonach komórkowych.

V. Kompatybilne modele telefonów Nokia

Seria E	Seria N	Seria 52XX	Seria 62XX	Seria C
E 51, E 51 (z kamerą), E 63, E 66, E 71, E 75, E 90.	N 78, N 79, N 81, N 82, N 85, N 86 8MP, N 95, N 97, N 97 mini, N 97 mini gold.	5228, 5230, 5230 Nuron, 5235, 5250, 5530 XpressMusic, 5730, 5800 XpressMusic.	6210 navigator, 6220 classic.	C6-00