

Protección contra escuchas Encriptación voz GSM



CEAS - INTERNACIONAL



¿Qué es CEAS Secure Talk ?

- Es un sistema que cifra su llamada a través de un teléfono móvil GSM y frustra absolutamente su escucha. La encriptación usa el algoritmo AES 256 el cual es actualmente el standard de seguridad más alto del mundo.
- Es un sistema con seguridad de extremo a extremo. La conversación completa de un usuario a otro es cifrada.
- SecureTalk es unote los producto de la compañía CEAS que trata con la seguridad de las comunicaciones móviles y con el desarrollo de soluciones para protección de la información.

SecureTalk requiere

- **Smartphone**
 - Teléfono móvil standard con Symbian OS
- **SecureTalk – aplicación de software**
 - Proporciona un completo valor de cifrado de la llamada por el algoritmo AES 256 o GOST
- **SecureSafety – modulo hardware**
 - El usuario comunica a través de cualquier micro-auricular standard conectado al SecureSafe
- **Servicio de datos activado (CSD)**
 - Canal de datos standard 9.6 kb/s (para transferir datos y fax)
 - Número de datos puede ser requerido o no (depende del operador)

Características SecureTalk

- Permite el cifrado de la comunicación de voz a través del teléfono móvil en la red GSM
- Algoritmo AES con una clave de 256-bit para cifrado de voz
- Alternativamente algoritmo GOST o otros algoritmos de cifrado definido por el usuario
- Clave de cifrado de un vez – siempre hay nueva clave de cifrado creada con cada nueva llamada de teléfono. La clave usada con la llamada de teléfono actual será automáticamente destruida después de completar la comunicación.
- El algoritmo Diffie-Hellman proporciona un intercambio de claves de una vez
- El algoritmo RSA autentifica la llamada de teléfono
- Puede ser usado en cualquier red GSM de 900/1800/1900 que soporte la llamada de datos (CSD)
- Soporta roaming – el trabajo de cifrado de la llamada también en el extranjero dependiendo del operador
- La calidad de la voz es la misma que en una llamada de teléfono normal – compresión de voz AMR
- La lista de contactos es guardada en un formato cifrado en el teléfono móvil
- Usted puede elegir un teléfono móvil de la lista de teléfonos móviles compatibles Symbian (los modelos actuales soportados pueden ser encontrados en la tabla de abajo)
- Todas las funciones del teléfono móvil están accesibles sin ninguna restricción

Algoritmo cifrado de voz	AES 256 o GOST
Algoritmo intercambio clave	Diffie-Hellman 2048
Algoritmo autenticación llamada	RSA con la clave 2048
Compresión de voz	AMR-NB 6.4 Kbps
Seguridad – codificado de voz	Extremo a extremo
Forma de comunicación	Full-duplex
Red GSM	900/1800/1900 MHz
Soporta Roaming	Si
Almacenar clave segura	Módulo Silentel SecureSafe
Sistema operativo soportado – Symbian OS (UI Serie 60, Serie 80)	v6.1, v7.0s, v8.0, v8.1
Suportados – teléfonos móviles	Nokia N70, N90, 6630, 6680, 6681, 6682, 9500, 9300, 3230, 6260, 6600, 6670, 7610, 7650, 3650, 3660, Nokia 9300 Communicator, Nokia 9500 Communicator

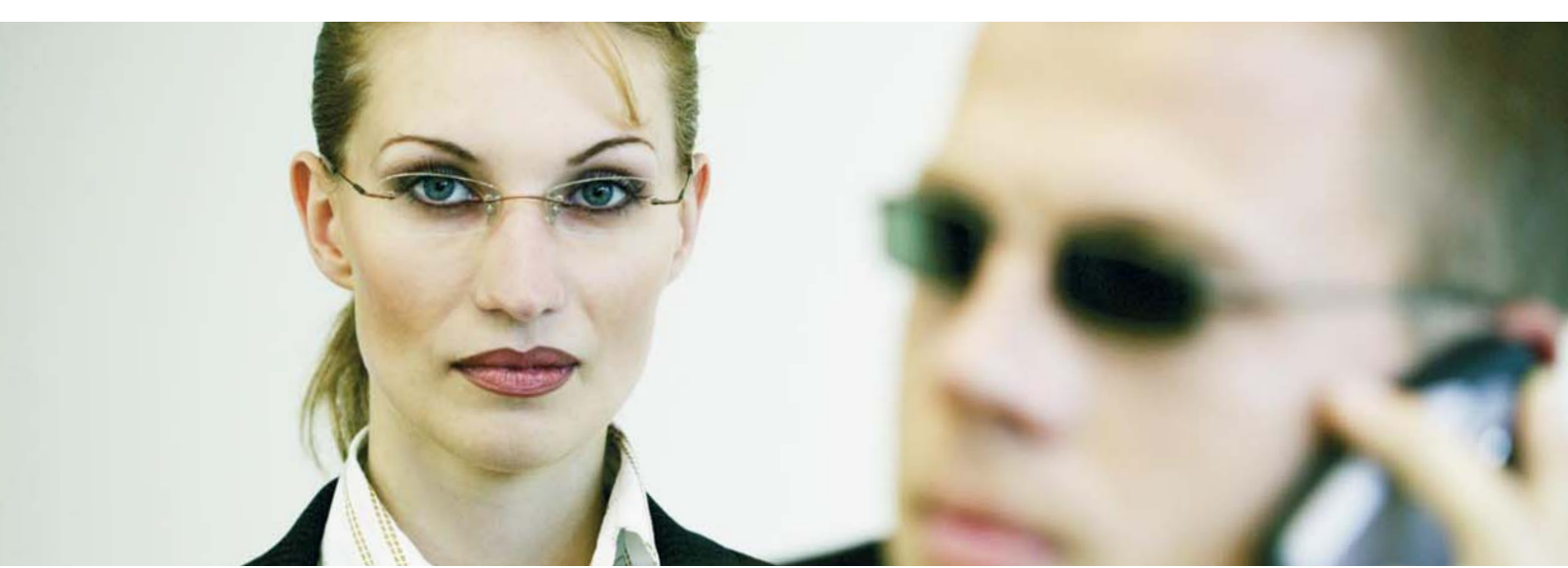
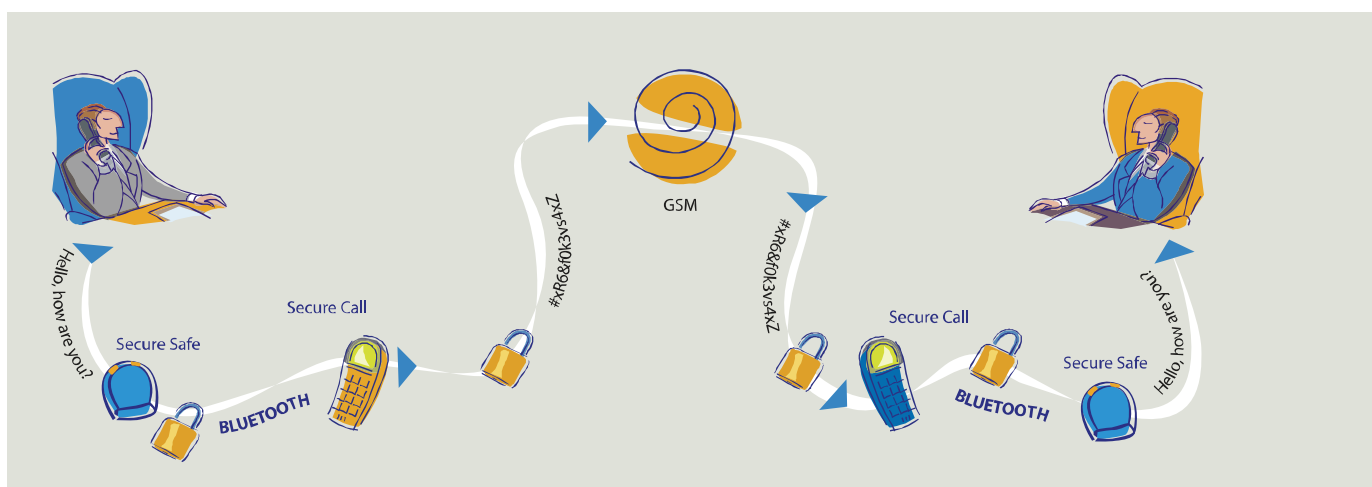


Diagrama de comunicación usando la versión SecureTalk Profesional



Características del SecureSafety – modulo hardware

- Usuario comunica a través de micro-auricular (cualquier standard)
- Conexión con el teléfono móvil es a través de Bluetooth
- La conexión Bluetooth es cifrada adicionalmente con AES 256 (sobre cifrado Bluetooth original)
- Autenticación
- Administra las claves
- Procesador Crypto para generación de la clave
- Tarjeta smart segura para guardar las claves privadas y para operaciones de crypto (FIPS 140-1 Nivel 2)

Especificaciones técnicas del modulo SecureSafety

Interface USB	mini-USB 1.1	Tamaño	56 mm x 54 mm x 29 mm
Especificación Bluetooth	1.1, clase 2	Peso	58 g
Área frecuencia BT	2 402 – 2 480 GHz	Batería	Li-ion 850 mA/h
Alcance BT	max. 10 m	Fuente Alimentación	110/240 VAC (60/50 Hz)
Velocidad Transmisión BT	224 kbit/s	Temperatura Funciona	-10 a +55 °C
Tiempo conversación	hasta 14 horas	Temperatura Almacenaje	-20 a +70 °C
Tiempo Stand by	hasta 480 horas	Humedad operativa	10 a 80 RV

Protección contra escuchas

Encriptación voz en Equipos



■ *Comunicación vía Satélite de banda ancha para todo el mundo.*

- Primer sistema de alta velocidad en red de datos con cobertura mundial.
- Gran velocidad hasta 492 kbit/s con opción de banda Ancha garantizada.
- Servicios adicionales de voz, SMS e ISDN.
- Accesibilidad simultánea a los servicios, igual que en su oficina.
- Terminales extremadamente ligeros: robustos, fáciles de cargar, fáciles de configurar y sencillos de usar.
- Los Servicios Agregados adicionales complementan el paquete permitiendo economía sustancial, además del control de utilización, seguridad y soporte.

CEAS CONTINENTAL - Información General de Movilidad.



Una nueva era ha empezado - CEAS CONTINENTAL - es el primer servicio portátil de comunicaciones móviles proveyendo servicios de voz y datos a gran velocidad simultáneamente a través de un Terminal sencillo de operar, verdaderamente transportable y con cobertura mundial. También es el primer servicio móvil de comunicaciones móviles a ofrecer velocidades de datos garantizadas bajo demanda.

El servicio de CEAS CONTINENTAL ha sido desarrollado para permitir accesos a contenidos y soluciones de Internet a Intranet, video bajo demanda, videoconferencia, fax, correo electrónico, telefonía, acceso a LAN con velocidades hasta 492 kbit/s prácticamente en cualquier lugar del mundo.

Lanzado en diversos estadios, de acuerdo con el sucesivo desarrollo de los satélites I-4 de Inmarsat-4, el servicio CEAS CONTINENTAL cuenta con disponibilidad para Europa, África, Oriente Medio, Asia-Pacífico y las Américas.

Las personas necesitan trabajar fuera de sus oficinas cada vez más. En conjunto con la utilización creciente de laptops, PDAs y teléfonos móviles, estos hechos hacen con que movilidad y oficinas móviles sean aparatos esenciales de empresas pequeñas y medianas. La posibilidad de acceso a informaciones de datos corporativos y correo electrónico en todos los momentos y en todos los lugares está visto como una prioridad estratégica.

- Comunicaciones: gran calidad de telefonía, SMS, ISDN y acceso inmediato a correo electrónico.
- Compatibilidad de video: videoconferencia, Broadcast, sistema de comunicación store y forwarding, tasas de datos garantizadas bajo demanda para aplicaciones como streaming.
- Acceso de datos: Web y conexiones Internet en gran velocidad y transferencia de archivos.
- Flexibilidad del sistema: IP y aplicaciones con cambios de circuitos de datos pueden ser usadas simultáneamente.
- Seguridad: acceso seguro a redes corporativas VPN's, soporta prácticamente todas las criptografías conocidas.

■ **VENTAJAS Comunicación vía Satélite de banda ancha para todo el mundo.**

- ✚ **Cobertura Global:** CEAS CONTINENTAL entregará cobertura de red ininterrumpida a través de casi toda la masa terrestre. Los usuarios podrán tener banda ancha donde quiera que vayan, no sólo en las principales ciudades o en el aeropuerto. CEAS CONTINENTAL cubre Europa, África, el Medio Oriente, Asia y América.

- ✚ **Voz y datos en banda:** ancha simultáneamente Con un solo dispositivo CEAS CONTINENTAL, usted tiene acceso a aplicaciones de datos a velocidades de hasta medio megabit y puede hacer una llamada telefónica al mismo tiempo. En una primicia mundial para los servicios móviles, usted también puede seleccionar capacidad garantizada de transferencia de datos cuando lo necesite, con una gama de velocidades que se ajustan a los requerimientos de sus aplicaciones. Y para garantizar la disponibilidad del ancho de banda, la capacidad de la red puede ser re-direccionada a áreas de uso frecuente.

- ✚ **Altamente portátil:** Los terminales CEAS CONTINENTAL son compactos, livianos y se pueden llevar tan fácilmente como un computador portátil: el terminal CEAS CONTINENTAL más liviano pesa menos de un kilo. Es posible montar una oficina con banda ancha totalmente funcional en cuestión de minutos.

- ✚ **Totalmente flexible:** CEAS CONTINENTAL es compatible con los últimos servicios IP, además de los tradicionales servicios de voz y datos por conmutación de circuitos. Al integrarse de forma perfecta con sus redes corporativas, resulta compatible con aplicaciones ya existentes a la vez que ofrece una vía sin obstáculos para la actualización. Existen terminales para un solo usuario o para grupos pequeños, que pueden estar conectados a un portátil a través de una conexión por cable o inalámbrica. Y la interfaz del usuario puede personalizarse de acuerdo a sus requerimientos.

- ✚ **Fácil de usar:** CEAS CONTINENTAL está diseñado para la simplicidad y el fácil uso. No se requiere experiencia técnica especializada para armarlo y utilizarlo. Es fácil de gestionar los costos porque usted puede rastrear el uso del servicio y los cargos en tiempo real. Puede usted utilizar el mismo dispositivo en todo el mundo, y la interfaz del usuario es estándar para todos los terminales. Y nunca hay problemas de compatibilidad con redes locales de telecomunicaciones porque usted se conecta directamente al satélite.

- ✚ **Completamente seguro:** Inmarsat tiene una amplia experiencia en suministrar comunicaciones seguras a clientes de las fuerzas armadas y gubernamentales. CEAS CONTINENTAL cumple estos requisitos exactos y es compatible con todos los principales productos VPN y los estándares de encriptación.

Protección contra escuchas

Encriptación voz en Equipos

CEAS BASICO ALTO RENDIMIENTO

Teléfono móvil encriptado de alto rendimiento. Seguridad y multimedia todo en uno.

Secure Celular

■ Sistema de encriptación

- En este equipo CEAS se ha apoyado en su amplia experiencia en seguridad y tarjetas inteligentes para desarrollar el módulo de encriptación en una tarjeta miniSD.

■ Sistenzador de voz

- Hace uso de la última tecnología 9600 bps para sonido de alta calidad en comunicaciones encriptadas.

■ Características Técnicas

- Llamadas encriptadas o normales o otros teléfonos móviles o fijos equipados.
- Posee un algoritmo simétrico (no publicado) con llave secreta de 128-bit
- Directorio seguro.
- Permite crear grupos de hasta 50 llaves de tráfico
- Tribanda 850/900-1800-1900
- Pantalla alta resolución: QVGA, 256K,color, 240x320 píxeles
- Tecnologías integradas: tonos hifi, MP3,SMS, MMS, WAP, GPRS*, Bluetooth*, lector MP3 y vídeo cámara, todo con un almacenaje de hasta 40 MB
- Cámara de 1,3 megapíxeles con flash y zoom X8
- Características físicas
 - Tamaño: 115x47x20,8 mm
 - Peso: 125 g



Hig Secure Celular Satélite – Hi Fi.

- Hay otra versión superior, es la versión multired. Además de tener todas las características técnicas, tiene la capacidad de poder conectarse mediante un modem a la red fija (PSTN/ISDN) o a la red satélite (Satélite Inmarsat).



Hig Secure Fijo.

- Así mismo, hay un equipo encriptado fijo, que igualmente puede realizar llamada fijas encriptadas o no.



Protección contra escuchas

Encriptación voz en Equipos

CEAS SECRAFONO Y WI- FI

Secure Celular encriptado y secrafone por Software

- Este modelo de teléfono trabaja con el sistema encriptado y secrafone por hardware (con el chip Crystall instalado). El software puede borrarse si se resetea el teléfono, y puede provocar conflictos con otro software, los algoritmos de encriptación solo llegan a 64 o 128 bits NO HAY ACCESO A NINGUNA PANTALLA PARA CAMBIAR LA CLAVE.



- Este tipo de encriptación se instala un software programado a medida para cada caso, trabajamos con los modelos de teléfonos mas actuales. Estos terminales, funcionan exactamente como un teléfono normal, hasta que se activa su modo seguro. La función de comunicación segura se activa en cuanto se detecta otro terminal seguro al otro lado de la comunicación. Estos sistemas son grandes herramientas para la protección de sus comunicaciones, cuando el presupuesto no permite utilizar sistemas mas avanzados. Los modelos de Teléfonos encriptados y secrafonos son compatibles con los sistemas de telefonía de todo el mundo.

Secure Celular – Fijo con WI - FI

- Se trata del primer teléfono fijo-móvil libre del mercado. Es un terminal libre, compatible con todos los operadores de telefonía móvil del mercado, que funciona como fijo en casa y como móvil fuera de ella. El teléfono móvil detecta la zona de cobertura de red LAN. Automáticamente realiza las llamadas a fijo a través de la línea telefónica, incluso en “modo fijo” las llamadas entrantes al número móvil se reciben igual en el. Al salir de la zona de cobertura LAN, se conecta a la red GSM y todas las llamadas realizadas se cursarán a través de la red móvil. Si el usuario tiene una llamada a través de la red GSM y entra dentro del área de cobertura LAN, la llamada continuará sin ningún corte sobre la red GSM.

■ Características técnicas

- Móvil dual: utiliza tecnología GSM y Wi-Fi de forma compatible
- Válido para cualquier operador móvil del mercado
- - VoIP Integrada y Conexión de datos GPRS
- Cámara VGA integrada (640x480 pixel)
- Browser WAP 2.0
- Tiempo de conversación: 160 min / 240 min (WLAN/GSM)
- Teléfono tribanda
- Elección de red preferida (fija o móvil) Dentro de la red fija permite forzar el marcado por GSM marcando 3 asteriscos (***) antes del número
- - **Seguro: utiliza la encriptación WPA2 para la conexión, la más segura del mercado.**

Protección contra escuchas

Encriptación voz en Equipos



CEAS BASICO CON SELECCIÓN DE BANDAS



Secure Celular Selector de Bandas

- Así mismo, normalmente en un país, la intervención de celulares se realiza a través solo de la banda más común (una o dos de las de 800, 900, 1800 o 1900) o en la que trabaja el operador contratado (Tricom, Orange, Telefónica, Porta, Claro, etc...), pero solo una porque el costo de intervención de todas es muy elevado e imposible, así como los equipos de interceptación solo dan opción a dos bandas, por lo que este celular tiene la opción de seleccionar la banda de emisión, es decir, que si cambiamos la banda de 900 a 1800 por ejemplo, este no podrá ser intervenido o escuchado, así como la encriptación de GSM que lleva casi ningún país puede descifrarla, por lo que no puede ser intervenido en el AIRE..., solo en colaboración con la empresa operadora del servicio, es decir, si es la policía, tiene que tener autorización judicial para ir a la empresa distribuidora de servicios (Orange, Telefónica, etc..) y realizar una intervención en el número del chip del titular...



Hig Secure Celular Temporal.

- Así mismo, CEAS dispone de terminales activados para un plazo de 15 días en determinado país que incluye número de celular, es decir, usted viaja a USA, y se le entrega un celular normal que puede realizar llamadas donde desee con la garantía que a usted no lo escuchan (no garantizamos que el otro celular comunicado no sea intervenido), pero transcurridos los 15 días este número de celular desaparece..., ya que es un número de celular "virtual" que en realidad no está registrado ni existe, por lo que es imposible su interceptación..



Hig Secure Chip Celular.

- CEAS también dispone de un chip con número encriptado, solo tiene que cambiar el chip de su celular, y se comunica a través de una línea exterior, con que las llamadas no pueden ser intervenidas, pero las llamadas son más caras.



Hig Secure Celular Integrado.

- CEAS recomienda como la opción más factible y económica con una seguridad Nivel II, un celular HI-FI con un chip encriptado, pues es prácticamente imposible su intervención