

¿Sabía Usted que sus comunicaciones celulares pueden ser interceptadas y que quienes usted menos desea podrían estar escuchándolas?

¿Analizó la posibilidad de poder hablar tranquilo cuando y donde quiera con alguien de su equipo de trabajo, sin tener esa sensación de estar siendo escuchado?

¿Está dispuesto a perder sus secretos más críticos?



La solución Sigillu ofrece

- ➔ Comunicaciones seguras en todo momento y lugar
- ➔ Encriptación robusta de grado militar: Encriptación RSA asimétrica (algoritmo ARC4) con llave maestra de 1,024 bits que se renueva automáticamente cada 30 días y llave de sesión de 256 bits, que se renueva en forma aleatoria cada 5 segundos
- ➔ El proceso de protección no requiere intervención del usuario ni es percibido por terceros
- ➔ Protección punto a punto (comunicación cifrada entre los dos equipos)
- ➔ No requiere hardware adicional ni configuración de grupos
- ➔ Tecnología israelí licenciada por el Ministerio de Defensa de Israel
- ➔ Uso de teléfonos regulares y la red celular GSM convencional
- ➔ No requiere hardware adicional

Todas las comunicaciones en el espectro radioeléctrico pueden ser intervenidas. Aún cuando su llamada pueda ser interceptada, Sigillu le provee un nivel de encriptación que la hace invulnerable.

En última instancia, la comunicación interceptada no podrá ser descifrada!

Preguntas Frecuentes

→ ¿Qué es Sigillu?

Sigillu consiste en una línea de productos desarrollados a partir de avanzada tecnología israelí, con el fin de proteger comunicaciones a través de distintos medios, incluyendo telefonía celular, líneas fijas y correo electrónico, de tal forma que, aún cuando las comunicaciones hubieran sido interceptadas, no puedan ser descifradas.

→ ¿Cuál es el origen de la tecnología Sigillu?

Se trata de tecnología israelí licenciada por el Ministerio de Defensa de Israel.

→ ¿Quién debiera considerar el uso de tecnología Sigillu?

Personas que operan con información confidencial, donde ellos mismos o terceros pudieran sufrir perjuicios si dicha información fuera accedida por las personas indebidas, debieran considerar el uso de esta tecnología. Un abogado discutiendo estrategias con un cliente, directores discutiendo detalles de una oferta relativa a una adquisición, agentes intercambiando información acerca de un allanamiento inminente, constituyen algunos ejemplos donde la tecnología Sigillu debiera ser considerada. El teléfono seguro Sigillu fué desarrollado para personas que día a día trabajan con información confidencial, tal como políticos, abogados, periodistas, fuerzas de seguridad, ejecutivos, y todos aquellos que conocen qué tan importante es prevenir que información sensible pueda caer en manos equivocadas.

→ ¿Quiénes podrían interceptar mis comunicaciones?

La complejidad de las redes de comunicaciones actuales trae aparejado el incremento en la cantidad de puntos vulnerables. Aún comunicaciones que supuestamente debían ser encriptadas pueden pasar por canales no encriptados o por operadores con ineficientes políticas de seguridad. Asimismo, un operador podría decidir apagar el encriptado de tal forma de reducir el tráfico y aumentar el rendimiento de su operación, lo que resulta imperceptible para el usuario regular. Estas vulnerabilidades hacen posible la interceptación, que podría ser conducida, por ejemplo, por competidores, empleados corruptos de una empresa de telecomunicaciones, o hasta criminales.

→ **¿Puede ser necesario utilizar esta tecnología para protegerse de ciertos competidores?**

Resulta saludable considerar que no todos los competidores se limitarán a prácticas legales para obtener información.

→ **¿Existen casos conocidos de escuchas telefónicas ilegales?**

La prensa hace referencia periódicamente a casos de escuchas ilegales (o “chuponeos”), donde las interceptaciones afectaron tanto líneas fijas como comunicaciones celulares. En la mayoría de los casos, se ha logrado confirmar la interceptación, pero no se ha logrado identificar quién la realizaba.

→ **¿Cuántos dispositivos Sigillu son necesarios para una comunicación segura?**

La tecnología Sigillu ofrece protección punto-a-punto, lo que evita puntos intermedios de gerenciamiento que podrían introducir vulnerabilidades al sistema. Por ese motivo, la tecnología Sigillu es necesaria en los dos extremos de una comunicación. Por ejemplo, si dos personas quieren mantener una conversación telefónica protegida a través de la red celular, ambos tienen que utilizar teléfonos celulares con tecnología Sigillu.

Intercepción, encriptación

→ **¿Qué es "criptografía"?**

Se denomina “criptografía” al proceso a través del cual la información se hace ininteligible para todo aquel que no posea las claves requeridas para su descifrado. Por ejemplo, el encriptado de un documento preparado con un procesador de textos, hace que sólo pueda leer su contenido quien posea la clave de descifrado correspondiente. Cualquier otra persona sólo podrá ver un conjunto de caracteres y símbolos sin significado aparente.

Como ejemplo práctico, a continuación se encriptará el siguiente texto:

• Mensaje original:

Este es un texto de prueba que se someterá a un proceso de encriptado para demostrar qué información podrá obtener quien logre acceder al documento que lo contiene pero no tenga las claves de descifrado necesarias.

• Mismo mensaje codificado (encriptado):

wcFOA6ME68+PCWRFEAf+OBm/uVwRbVkdNHR3I54k6XG9+fYvYojA2V2ZNV5FaLzSE4y77kn
sG+CWSjLXthmimDGhqjoXaDINKgHMEz6tgVq8Trz5lboZav7rA8g+aTwBRD8tbBgo+VEgAzR3
2qu754/ID0GCFEZ3NSpDLqeyE+g24T48wXGdMiXlvi/li4D/B/C0scsva2m17r1m975k50j9aSyz
FeN4WkSv9QFDg4oVPIUVfsnDWZUgXT6w/tmA4sem1Xs8KFnt+LZyzNpNqJDIPUMsb7ipCeH
NI+pm1im4a7mVXdIQ9pdnFwK348z9wj9UsANGLDK5U3gTNO21MkCqWVsTLiwWuE17LEbN
nQgAj5wu8ITAYYCKnJjiU9vNniUwUsnlvCN9kFr4l3rGw+zxkkwnhQ3Keqz4UrWnjmitMxEe9T
WiMv6lqLEOL691QsngZ/iUQVi1ON8P9ruwZ+CZ/PbOxFttXYSgn+UuxtOu8yig5bRtKQbTdAll

gXmAt9drMiZzMS0LAhBV9LJzIVLPIHFNeEt8uMDsL2c3f18z/RVzadvGj+wkrNjnY2DNZ/I3imVE
gcn9VxRSE1jbTcFLxU5BbT4KL+vg7ojsiGAQBab+7olfVwg/WMOvcFKF5s/fJOXW0PgpetoYh3
U3AmsgM14jTzGTfWCBix9RCWW0tpFkRfIIX9WtloZP1LZNtytLACQHBCCaNBq38AQIopm4W2
SG4VfMUrnUoBGaiWNEU/NOE8T9ueqFLBID+mviVZsfu5YbdFw1n5DcSz/PRllflp9HK7ojpPU3
un3bomVFrlIF8aq2Qk3LLp4UqG4HCf17Osh/q+4s1h5fTzR25/CNqcfFEcOtAbi1cW5I/+Zvzcyd
ALZbRCPIya4Cnh3xmp07CBBLJsJ2on4PouGmEjWekAyJd1kCEM900y4CokPDLomRtYkMxXm
iD5e2alslt4Lq1MU/++KzfCxdaUw===zeeM

→ **¿Qué es un “IMSI-Catcher”?**

Es un dispositivo que permite escuchar conversaciones celulares ajenas. Estos equipos pueden apuntar a un número específico o bien ser utilizados para escuchar conversaciones en forma aleatoria.

→ **¿Qué nivel de encriptación ofrece Sigillu?**

Sigillu utiliza encriptación asimétrica, con una llave maestra de 1,024 bits que se renueva automáticamente cada 30 días y una llave de sesión de 256 bits, que se renueva en forma aleatoria cada 5 segundos. La encriptación es del tipo “punto a punto”. Sigillu ofrece un sistema de encriptación robusto, de grado militar, en forma totalmente transparente al usuario, que tanto matemáticos como expertos en seguridad consideran inviolable.

→ **¿Pero las comunicaciones celulares digitales no están ya encriptadas?**

En algunos casos sí, en otros no, y en la mayoría lo están sólo entre la base y el teléfono celular, o sea que su paso por la red telefónica, que puede incluir vínculos inalámbricos, no está encriptada. Además, hace ya varios años se descubrieron vulnerabilidades en el sistema de encriptación de las redes GSM. Expertos del Instituto Technion de Israel desarrollaron un método que permite abrir la encriptación de la red GSM cuando se producen los primeros “rings,” aún antes de que comience la comunicación.

→ **¿El proceso de encriptado afecta la calidad de la comunicación?**

La degradación de la voz resulta prácticamente imperceptible al usuario al usar tecnología Sigillu.