enigCOMMS

por

enigmedia

ÍNDICE

LA COMPAÑÍA

Somos una empresa **especializada en el desarrollo de software de seguridad para sistemas de comunicaciones y transmisión de datos** en entornos corporativos e industriales**.** Trabajamos para ofrecer a nuestros clientes los productos más seguros adaptándonos a sus necesidades en el contexto tecnológico actual.

SERVICIOS

Nuestros modelos de negocio incluyen:

Productos propios	Desarrollos a medida de comunicaciones seguras	Licenciamiento tecnológico para terceros
Solución de comunicaciones seguras, enigCALL y enigCOMMS, especialmente diseñados para el ámbito empresarial.	Adaptamos nuestra tecnología creando **softwares ad hoc** para satisfacer necesidades específicas.	**Licenciamiento de tecnología** de cifrado para clientes que necesiten integrarlas en sus productos y soluciones.

NUESTROS CONSEJEROS CIENTÍFICOS

Whitfield Diffie
Descubrió la clave pública
de la criptografía

Pedro Crespo
Inventor del ADSL

Murilo Baptista
Pionero en encriptación basada en la Teoría del Caos

Hector Mancini
Delegado con derecho a voto en los Premios Nobel de Física

VALIDACIONES DE TERCEROS

Certificación COMMON CRITERIA por **CCNI - Centro Criptológico Nacional**

Alianzas estratégicas con: **AENOR** Committee - ISO 27000-ISO Security Group / **Instituciones legales / Compañías de seguridad IT**

Nos incluyen en el análisis de mercado de **Gartner: Market Guide** en los productos representativos para la Protección de Voz y Texto en Móviles.

AMENAZAS EN LAS COMUNICACIONES

Las amenazas detectadas en el campo de las comunicaciones y a las que **enigCOMMS** es resistente son muy diversas. Actualmente, las comunicaciones están amenazadas tanto mientras se realiza la transmisión de datos como una vez recibidos estos en los destinatarios. A continuación se muestran las amenazas más comunes y dañinas.

AMENAZAS EN LA TRANSMISIÓN DE DATOS

✓ **Interceptación / escucha (Eavesdropping)**
Se trata de un ataque indetectable, ya que captura los datos que están en el "aire", guarda la información, la analiza y la reconstruye para reproducir la conversación original.

✓ **Suplantación de identidad → MiTM (MiTM: Man in The Middle)**
Es el ataque en el que, haciéndose pasar por los interlocutores (suplantando su identidad), se adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre las dos partes sin que ninguna de ellas sepa que el enlace entre ellos ha sido violado.

✓ **Monitorización y trazabilidad de las comunicaciones**
En numerosos países la privacidad de las comunicaciones no está protegida legalmente lo que permite que los operadores de telecomunicaciones registren y almacenen las conversaciones para ser analizadas y procesadas de forma sistemática por entidades gubernamentales sin necesidad de orden judicial o para comercializar dicha información.

✓ **Ataque de denegación de servicio (DoS: Denial of Service)**
Este ataque tiene como objetivo impedir a los usuarios el uso de servicios de comunicaciones seguras, forzándoles a utilizar otros medios de comunicación inseguros.

AMENAZAS EN LOS DISPOSITIVOS DE COMUNICACIÓN

✓ **Grabación de conversaciones en destino (malware)**
Este ataque se basa en la instalación de software malicioso en los dispositivos de comunicación para grabar las conversaciones (llamadas, mensajes, documentos, etc.) en el propio dispositivo para posteriormente enviar dicha información al atacante.

✓ **Duplicación de credenciales de usuario**
Se trata de un ataque basado en la obtención de las credenciales de un usuario en un dispositivo insuficientemente protegido y utilizar una copia de las mismas en otro dispositivo simulando el atacante ser el usuario original ante el resto de los contactos del usuario.

✓ **Robo o pérdida del dispositivo de comunicación de un usuario**
Aunque una comunicación no haya sido interceptada durante su transmisión en los dispositivos de los interlocutores quedan rastros de las conversaciones (listas de contactos, mensajes, historial de llamadas, etc.) accesibles en caso de que un atacante se haga físicamente con el dispositivo.

AMENAZAS SOCIALES

Los riesgos para la información de una organización no siempre vienen de ataques externos, en multitud de ocasiones la fuga de información de una organización se debe a un manejo no seguro de las herramientas de comunicación por parte de los miembros de una organización o incluso a actitudes desleales o delictivas de los mismos.

✓ **Filtración al exterior de comunicaciones internas**

✓ **Comunicaciones no autorizadas con contactos externos a la organización**

✓ **Configuración no segura de aplicaciones**

✓ **Represalias de ex-trabajadores descontentos**

LA SOLUCIÓN DE ENIGMEDIA: enigCOMMS

El **Sistema Privado de Comunicaciones Seguras** de Enigmedia garantiza un **nivel de seguridad máximo** en tu dispositivo móvil para:

Llamadas de voz

Videollamadas

Mensajería instantánea

Transferencia de ficheros

Utilizando esta herramienta, **las comunicaciones de la organización serán totalmente privadas y confidenciales,** evitando que la información de la organización sea accesible para terceros y **protegiendo tu organización del espionaje industrial, monitorización de gobiernos hostiles y ataques de ciberdelincuentes.**

¿Y POR QUÉ enigCOMMS?

✓ **Seguridad certificada** por **COMMON CRITERIA** y diseñada siguiendo estándares y protocolos de seguridad internacionalmente reconocidos.

✓ **Cifrado robusto y ligero** diseñado para ser utilizado de forma eficiente en redes con limitaciones de ancho de banda, latencia o pérdida de paquetes.

✓ **No relación del usuario con número de teléfono** de cara a evitar la monitorización y trazabilidad gubernamental ni de los operadores de telefonía.

✓ **Certificados digitales asociados al usuario y dispositivo** que permite una rápida revocación remota de uso de la aplicación en caso de pérdida o robo del dispositivo.

✓ **Comunicaciones seguras con todos tus contactos:** Enigmedia no limita la comunicación segura al entorno corporativo interno, mediante la asignación de invitaciones temporales a sus contactos de la agenda el usuario puede comunicarse de forma segura con ellos sin ningún coste para el contacto invitado.

✓ **Mecanismos de protección adicional de dispositivo** (detección de dispositivo rooteado, PIN de aplicación, etc.) para incrementar el nivel de seguridad.

✓ **Facilidad de instalar y usar** sin necesidad de conocimientos de seguridad por parte de los usuarios finales.

✓ **Personalización de las aplicaciones con la imagen corporativa del cliente** para facilitar a los usuarios su adopción como herramienta de trabajo.

✓ **Integración del acceso seguro a otros sistemas de uso corporativo** en una misma aplicación para reducir los riesgos de filtración de información corporativa: email, CRM, Cloud Storage, etc..

✓ **Gestión centralizada desde un panel Web** por parte del personal IT de la organización.

✓ **Accesible desde cualquier país** y tipo de red de datos inalámbrica (2G, 3G, 4G, WII).

✓ **Despliegue en servidores físicos o virtuales** en el Centro de Procesamiento de Datos o Cloud Privada del cliente final.

✓ **Soporte multiplataforma:**

SOLUCIÓN TÉCNICA

✓ Comunicación Punto-a-Punto

Los servidores de **enigCOMMS** únicamente intervienen en el proceso de señalización de las llamadas. Una vez establecida la comunicación de extremo a extremo, los datos de audio y vídeo se envían directamente entre los dispositivos sin procesarse ni almacenarse en ningún otro elemento intermedio del sistema.

✓Cifrado Extremo-a-Extremo

A fin de que la información intercambiada entre los usuarios no sea accesible por terceros, independientemente de la red WIFI, 2G o 3G a la que se conecten los usuarios,la información se cifra y se descifra en los extremos de la comunicación con claves únicamente conocidas por los extremos.

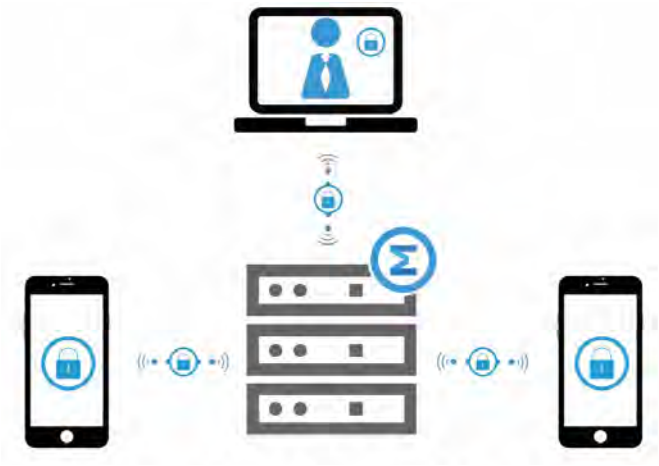
Los datos son cifrados por el usuario emisor antes de ser enviados, y son descifrados por el usuario receptor una vez son recibidos, de forma que aunque un atacante se hiciera con los datos cifrados de la comunicación estos datos no serían interpretables.

Comunicación Punto a Punto y Cifrado End-to-End

✓ Autenticación de usuarios y servicios

Además de proteger la transmisión de la información **enigCOMMS** identifica y autentica a los usuarios mediante certificados digitales que se vinculan a sus dispositivos evitando ataques de suplantación de identidad y MiTM.

Todas las comunicaciones que se realizan entre los dispositivos y los servicios de Enigmedia para el establecimiento de llamadas, ajustes de configuración, etc. se realizan a través de canales seguros TLS que utilizan los certificados digitales para verificar la identidad de los extremos.



✓ Modo invitado

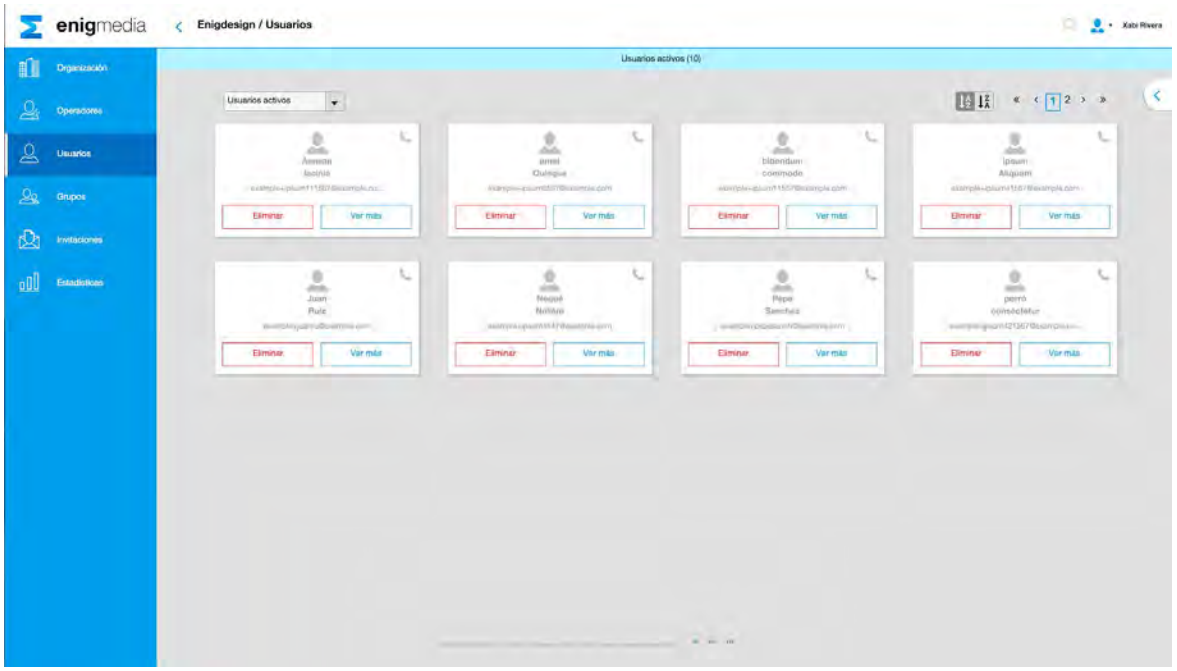
enigCOMMS permite securizar las comunicaciones del usuario con su red de contactos externa, es decir, con aquellos contactos que no pertenecen a la organización, mediante la asignación de invitaciones.

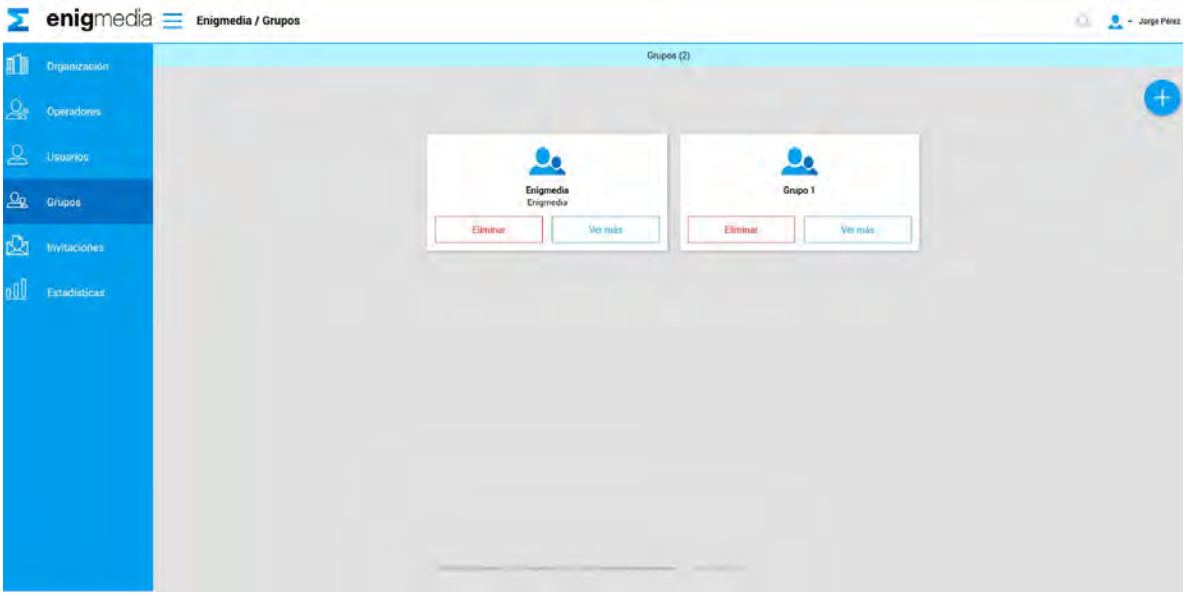
Estas invitaciones permiten al contacto al que se le asignan comunicarse de forma privada únicamente con el usuario que le ha invitado tanto para realizar como recibir llamadas, videollamadas, mantener conversaciones a través de mensajería instantánea o transferir ficheros.

El usuario pueda gestionar sus invitaciones de forma autónoma desde la app instalada en su dispositivo asignándolas a los contactos a los que desee integrar en su red privada de comunicaciones y revocándolas a aquellos contactos con los que ya no necesite establecer conversaciones seguras.

✓ Administración centralizada

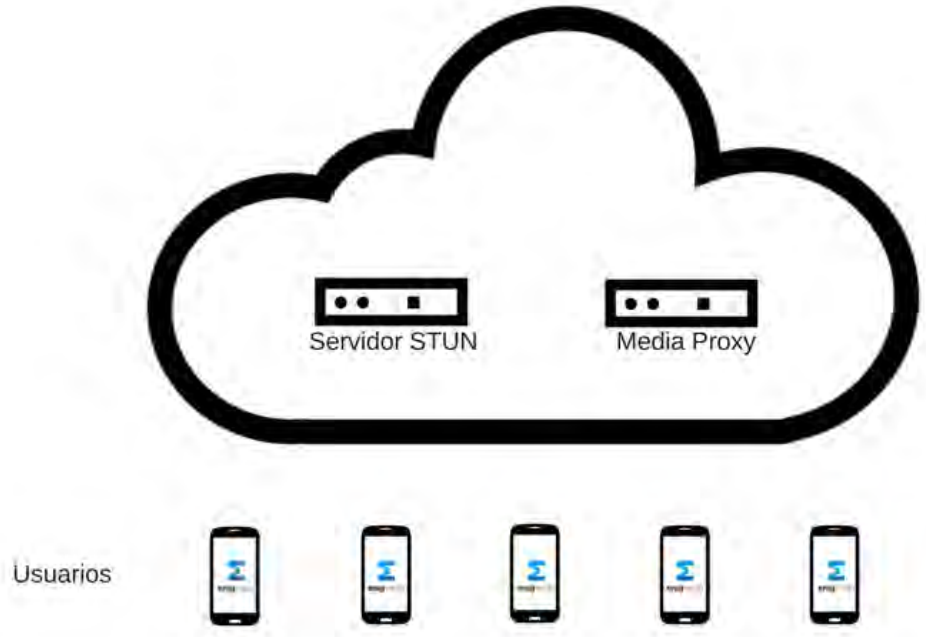
enigCOMMS dota al equipo IT de la organización de una herramienta Web para gestión y configuración del sistema. Permite la creación y revocación de usuarios, definición de políticas de seguridad en las comunicaciones así como acceso a estadísticas e informes de uso del sistema.





ARQUITECTURA DEL SISTEMA

SISTEMA ESTÁNDAR



SISTEMA CON REDUNDANCIA