enigCOMMS

by

enigmedia

INDEX

THE COMPANY	3
THREAT ON THE COMMUNICATIONS	4
ENIGMEDIA's SOLUTION: enigCOMMS	6
TECHNICAL SOLUTION	8
SYSTEM ARCHITECTURE	11

THE COMPANY

We are a company specialized in security software development for communication systems and data transmission in cooperative and industrial fields. We work in order to offer the most secure products to our clients while adapting them to their needs in the current technological context.

SERVICES

Our business model include:

Our products	Ad Hoc developments for secure communications	Technological licensing for third party individuals
Secure communications solutions called enigCALL and enigCOMMS. Specifically designed for the corporative field.	We adapt our technology to create ad hoc softwares in order to satisfy specific necessities.	Encryption technology licensing to integrate it on our clients products and solutions.

OUR SCIENTIFIC ADVISORS

Whitfield Diffie
Discoverer of the Public Key Cryptography

Pedro Crespo
Inventor of the ADSL

Murilo Baptista
Pioneer in Chaos Encryption

Hector Mancini
World Reference in Experimental Chaos

THIRD-PARTY VALIDATIONS

EAL1 CERTIFICATION by CCNI - Centro Criptológic Nacional.

Strategic Alliances with:
· AENOR Committee- ISO 27000- ISO Security Group
· Law Enforcements
· IT Security Companies

We have been included in Gartner Market Guide for Mobi Voice and Texting Protection

THREAT ON THE COMMUNICATIONS

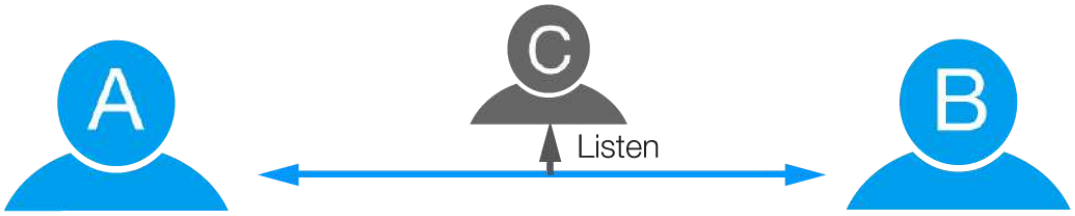
There are diverse threats detected in the communications field that enigCOMMS faces. Currently, the communications are threatened while data transfer is being done as well as when data is received on by the receiver.

The following images show the most common and harmful ones.

THREATS IN DATA TRANSMISSION

✓ **Eavesfropping**

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.



✓ **MiTM (MiTM: Man in The Middle)**

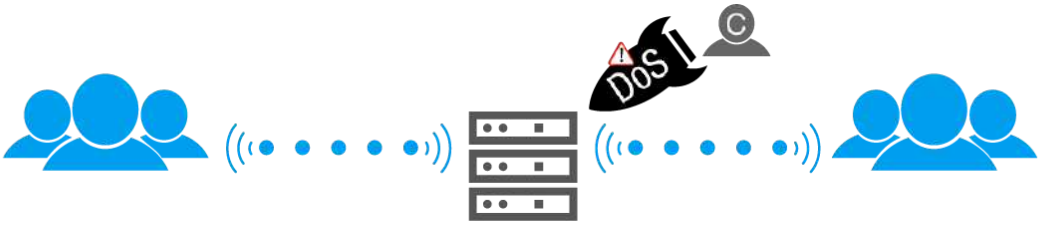
In this attack the attacker takes the place of the interlocutors, acquiring the ability to read, insert and modify the content of the messages between the two points. The interlocutors don't know that the link between them has been violated.

✓ **Communications monitoring and traceability**

The privacy of the communications is not protected in many countries, allowing telecommunications operators to store and record conversations. Those conversations are sold to third companies or processed and analyzed by government entities without any legal permission.

✓**DoS: Denial of Service**

The aim of this attack is to prevent users from using secure communications services, forcing them to use unsafe communications solutions.



THREATS IN COMMUNICATIONS DEVICES

✓ **Conversations records in endpoint (Malware)**
The attack consists on the installation of a malicious software in a device with the main purpose of recording conversations (calls, messages, files, etc.).

✓ **User credentials duplication**
The attacker uses a copy of the user's credentials in another device, so the attacker simulates being the original user to the rest of the user's contacts. It is based on the obtention of the user's credentials on an insufficiently protected device.

✓ **Theft or loss of a user's communication device**
Although the communication has not been intercepted, the traces of the conversations (contact lists, messages, call history, etc.) are accessible in case that an attacker gets with the device.

SOCIAL THREATS

The risks of the information of an organization do not always come from external attacks. In many cases the information leakage happens due to an unsafe handling of the communication tools or even to disloyal or criminal attitudes by the members of an organization.

✓ **External filtration of internal communications**

✓ **Unauthorized communications with contacts outside the organization**

✓ **Non-secure application configuration**

✓ **Retaliation of discontented ex-workers**

ENIGMEDIA's SOLUTION: enigCOMMS

enigCOMMS, the secure business communications service of Enigmedia, ensures the highest security level for your mobile phone to make:

Phone Calls | **Video Calls** | **Instant Messaging** | **File Transfer**

By using this service, your company's communications will turn to be completely private and confidential, preventing external individuals from getting access to the most critical and confidential information of your company. At the same time, it protects the organization towards industrial espionage, government monitorization or cybercriminal attacks.

WHY enigCOMMS?

✓ **Security certified by COMMON CRITERIA and designed according to internationally recognized safety standards and protocols.**

✓ **Robust and lightweight encryption designed to be used efficiently in networks with bandwidth or latency limits or packet loss.**

✓ **No relation with the user's telephone number in order to avoid the monitoring and traceability of government or telephony operators.**

✓ **Digital certificates associated to the user and device. This allows a quick remote revocation of the application in case of loss or theft of the device.**

✓ **Secure communications with all your contacts: enigCOMMS allows to establish secure communications between users not only on the corporative internal environment. Thanks to the Guest Mode, each user user has guest licenses that allow to make secure calls to any contact from the phonebook, even with not licensed Enigmedia users.**

✓ **Additional device protection mechanisms (robotic device detection, application PIN, etc.) to increase the level of security.**

✓ **Easy to install and use without the need of security knowledge from end users.**

✓ **App customization with the corporate image of the client. This makes it a better and friendlier work tool for the workers.**

✓ **Integration of the secure access with other corporate systems in a unique App, in order to reduce the corporate information leakage: email, CRM, Cloud Storage, etc.**

✓ **Centralized management from a web application at the service of the IT staff of the organization.**

✓ **It can be used anywhere in the world and with any type of wireless data network (2G, 3G, 4G, WIFI).**

✓ **It can be deployed in physical or virtual servers in the Data Center or Private Cloud of the final client.**

✓ **Cross-platform: Android and iOS.**

TECHNICAL SOLUTION

✓ **Point-to-Point Communication**

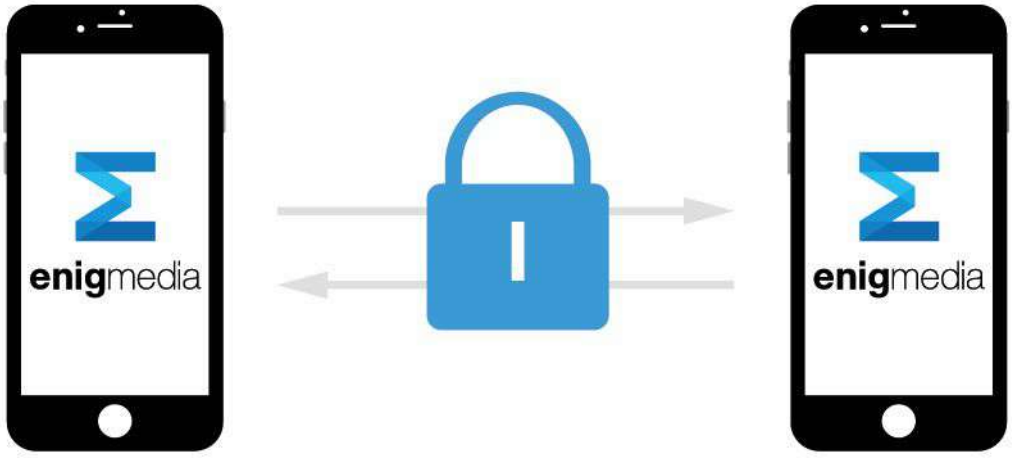
enigCOMMS servers only take part during the call signaling process. Once it is established, the point-to-point communication, audio and video data are directly sent between the devices without being processed or stored in any other intermediate element of the system.

For this reason, Enigmedia, as the service provider, does not have access to the information exchanged between the users during the communication.

✓ **End-to-end encryption**

In order to make the exchanged information inaccessible not accessible to third parties, regardless of the WIFI, 2G or 3G network, the information is encrypted and decrypted at the end point of the communication. The keys are only known by the extremes.

The data is encrypted by the issuer user at the source and is decrypted by the receiving user at the destination. Thanks to this, even if an attacker manages to obtain the encrypted data of the communication, this data would not be interpretable.

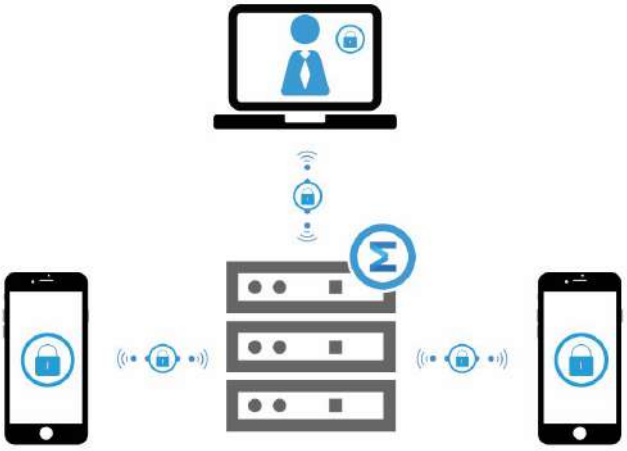


Point-to-Point communication and End-to-End encryption

✓ **Users and services authentication**

enigCOMMS identifies and authenticates the users using digital certificates, that get linked to the devices. This protects users from MiTM attacks.

All the communications that are made between devices and Enigmedia's services for the calls establishment, configuration settings, etc. are made through secure TLS channels that use the digital certificates in order to verify the endpoint's identity.

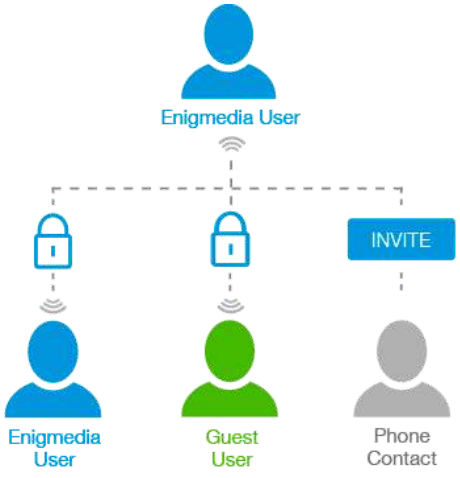


✓ **Guest mode**

enigCOMMS allows to secure the user's communications with all the external contact network. Assigning invitations, it is possible to communicate safely too with those contacts that do not belong to the organization.

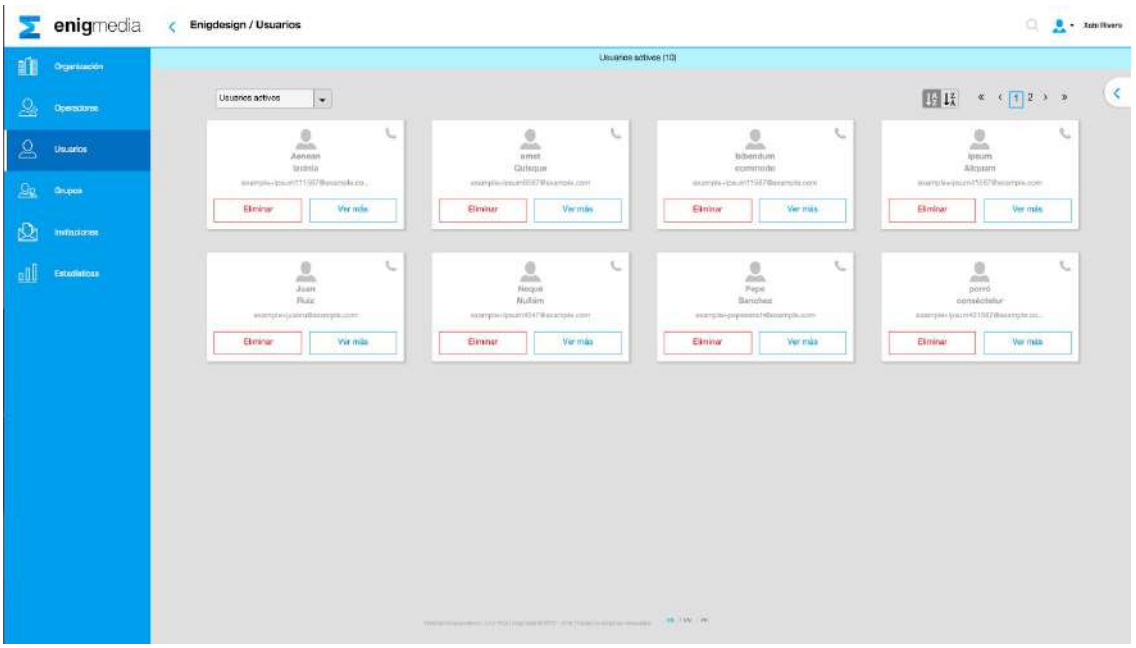
These invitations allow the guest contact to communicate privately only with the user who has sent the invitation, allowing to make and receive calls, video calls, establish conversations via instant messaging and transfer files.

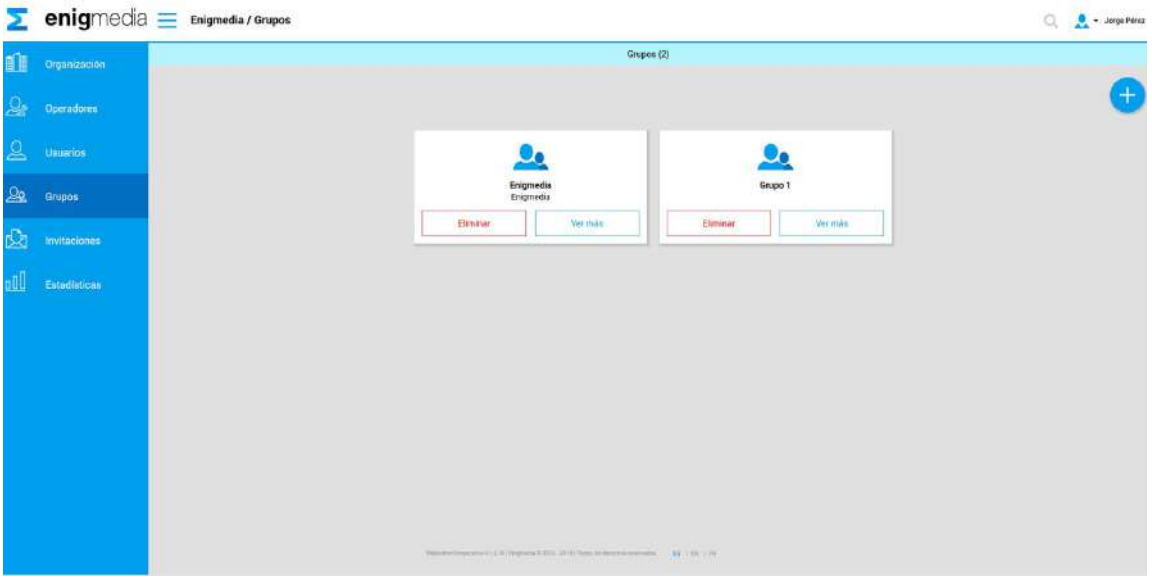
The user can autonomously manage the invitations from the app, assigning them to any of the contacts that he wants to integrate into their private communications network and revoking them to those contacts with whom they no longer need to establish secure conversations.



✓ **Centralized administration**

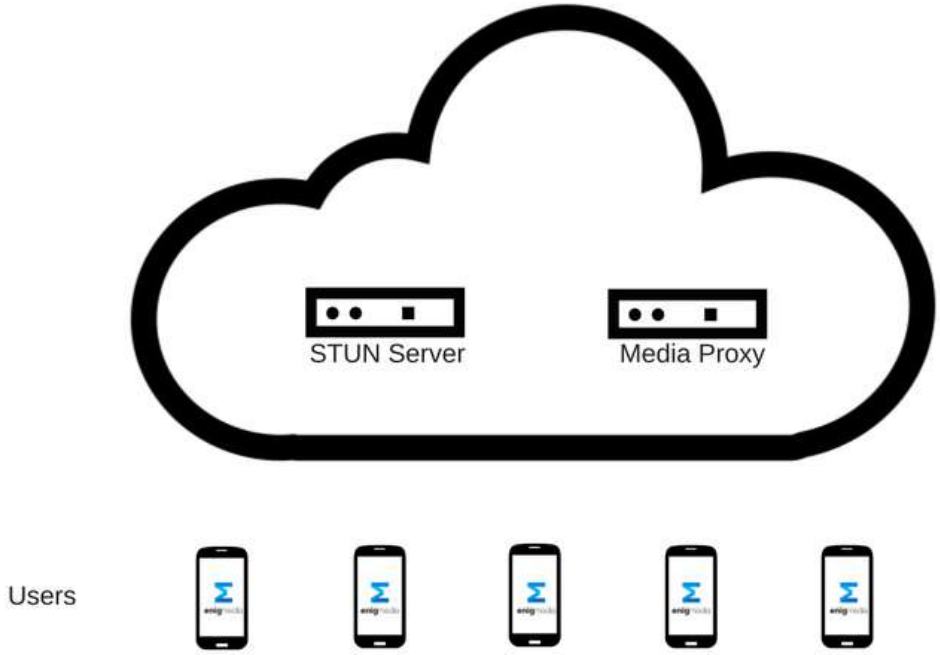
enigCOMMS offers a web based tool to administrate and configure the systemf. It allows to create and revoke users and to define the security policies in the communications, as well as to access to statistics and brochures about the system use.

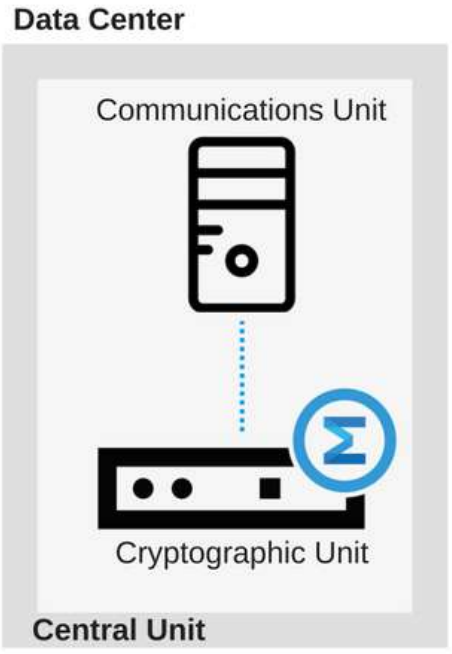




SYSTEM ARCHITECTURE

STANDARD SYSTEM





SYSTEM WITH REDUNDANCY