Silentel®

secure
voice calls

secure
text messages

secure
chat conference

secure
files transfer

iOS ANDROID BlackBerry Windows

Connect to the world of
secure mobile communication

It is no exaggeration that information is becoming an increasingly valuable asset. For governments, companies and even individuals, the ability to access, exchange, control and protect information can determine the difference between success and failure. Current mobile lifestyle devices allow anyone -- politicians, business executives, law enforcement agents, military personnel and ordinary citizens to access and transmit sensitive information almost anytime and anywhere.

But security and privacy risks (due to accidents, loss, hacking, etc.) are escalating.

While mobile communications are convenient for users, they introduce a new and significant risk to information security. Interception and eavesdropping of mobile communications is becoming increasingly common as the costs of such technologies drop and the rewards for these illegal intercepts rise.

Because mobile communications (whether voice, text or chat) often demand time sensitive, confidential information, a single intercepted exchange can destroy business negotiations, reveal confidential alliances, or damage an organization's image and trust among partners.

What is Silentel?

Silentel technology is the serious choice for any user who wants to protect and secure his voice calls, messages, chats, sensitive documents, photos or any files against unauthorized usage.

Silentel is a fast to implement and easy to use, targeted for any type of secure mobile communication. It consists of client applications and server modules. Silentel client applications are made for end users' mobile phones and personal computers (PCs). Server modules provide mainly authorization and mutual connection between individual users.

Guaranteed security

Silentel meets NATO security requirements and is certified by several government security agencies as a product for secure mobile communication. Silentel meets and is approved up to NATO CONFIDENTIAL security level.

Secure voice calls

Secure text messages

Secure chat conference

Secure files transfer

Security mechanism

Strong cryptography

- Client and server mutual authentication (RSA 2048)
- Client-server signalization protocol (SIP) encryption (AES 256)
- Communication end-to-end encryption (AES 256)

End-to-end encryption

- All data transmitted through Silentel system are encrypted end-to-end. It means that data are encrypted before sending and are decrypted after delivery to receiver. Data are never decrypted during transfer. Moreover encryption is protected against man-in-the-middle attack.

One-time encryption keys

- Each communication is protected by an unique encryption key which is generated during communication establishment. Each encryption key is destroyed immediately after communication.

No permanent information

- No information remains being stored on user's device, not even a contact list. Even when a mobile device is lost or stolen, no Silentel information will ever be available to anybody finding the device.

Non-traceable

- Standard GSM calls are not only vulnerable for interception but moreover they are traceable as well. Mobile operator has records about all your calls and messages – to whom you have called, when and for how long. Silentel communication is transmitted only as internet data (similar to browsing on internet) what makes your calls and message non-traceable.

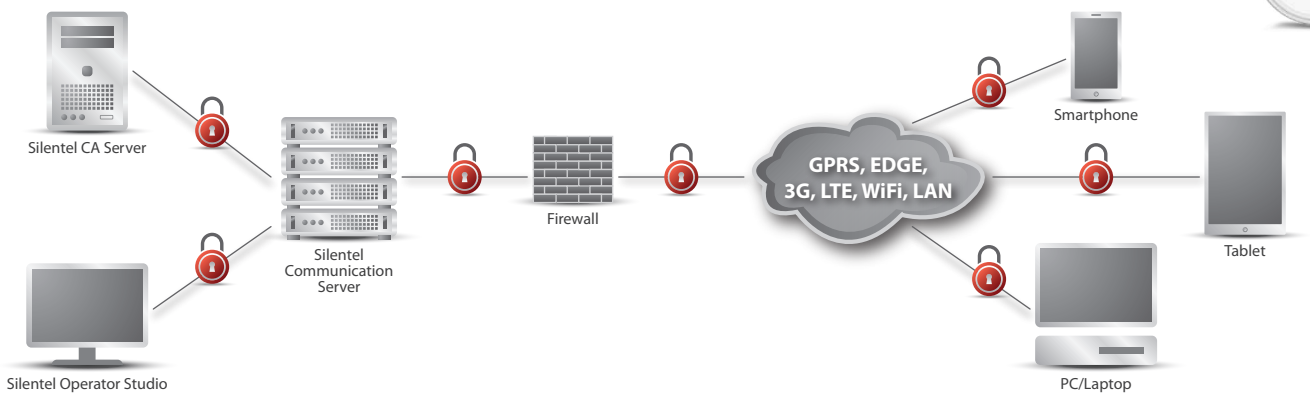
How does it work?

For a user making phone calls using Silentel there is almost no difference versus a standard mobile call. To make a secure voice call with Silentel, users simply select a recipient from the Silentel contact list and tap the "Make a call" option from menu. The Silentel application automatically creates unique encrypting keys securing the connection. During the connection, all information transmitted by the Silentel system is encrypted by the sender and decrypted by the receiver. Nobody, not even the communication server, is able to intercept the communications, either in form of voice track, in text or other data form. It is even impossible to identify to whom, as well as the time users have been communicating. After the phone call has been finished, all encrypting keys are deleted and your information will forever remain confidential.

When user closes the Silentel application, no information remains stored in the device. This means that no forensic analysis is able to retrieve any sensitive information (like voice calls, text messages, files and contacts) from the user's device.

Architecture

The core Silentel infrastructure is based on client-server principles and consists of following client and server software modules:



- Secure contact list with user presence status
- Message delivery and read confirmation
- Notifications for missed call, new message and chat
- SMS notification

Key benefits

Security and confidentiality

- Strong encryption which makes your information 100% secure.
- No third party servers – whole system is under full control of customer.

Easy to deploy, easy to use

- Designed and implemented for popular commercial devices to protect classified information.
- Intuitive and modern user interface; crystal clear sound for voice communication.

Worldwide coverage with reduced operation costs

- Supports all the most used Internet (IP) networks – GSM, 2G, 3G, 4G/LTE, Wi-Fi, LAN/WAN, Satellite.
- Supports international calls and roaming.
- Can significantly reduce charges for voice services due to low amounts of transmitted data, even being used abroad in roaming (in foreign mobile network operators).
- Allows to make phone calls completely free of charge anywhere anytime, when operating via Wi-Fi.

Silentel Client
applications are available for:

iOS ANDROID BlackBerry Windows

Ardaco, a.s. is a leading provider of Information/Communication Technology and Information security. Ardaco provides, its own developed, fully scalable Silentel® platforms for secure mobile communication including voice, data communication and messaging. In addition, Ardaco provides a full range of its proprietary products for electronic signature (including Qualified Electronic Signature QSign™ (certified by National Security Agency), QSign™ archive, QSign™ e-invoice, QSign™ e-registry) that enable secure and cost effective handling of electronic documents. Individuals, organizations and companies can reliably protect and secure their communication and information with a full range of Silentel® and QSign™ products.

Silentel was founded in 1996 by a group of technical experts and pioneered several new technologies, including patented Electronic Paper Protection Technology (PDMark®), Qualifed Electronic Signature Solutions (QSign™) and secure voice communication system for mobile smartphones Silentel® CSD (known also as SecureCall™). In 2008, Ardaco was one of the first to create a new IP-based product package for secure voice/data communication and messaging -- Silentel® IP (known also as TeamTalk™). In 2010, Ardaco pioneered a new, cost-effective, secure solution for mobile communications that can address military, police, enterprise and personal requirements.

Ardaco has its customers and partners in over 20 countries worldwide, including Europe, Middle East, Africa, Asia, North America and South America.

SECURE COMMUNICATION **SOLUTIONS** FOR MOBILE DEVICES

ARDACO
DATA & COMMUNICATION SECURITY

Ardaco, a.s.
Polianky 5
841 01 Bratislava
Slovak Republic

+421 2 3221 2311

info@ardaco.com

www.ardaco.com
www.silentel.com