

Ardaco, a.s. is an innovative leader in the area 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 full range of its own developed products in the area of electronic signature, including Qualified Electronic Signature QSign™ (certified by National Security Agency), QSign™ archive, QSign™ e-invoice, QSign™ e-registry, all for secure and cost effective handling of electronic documents. Individuals, organizations and companies can reliably protect and secure their communication and information with full range of Silentel® and QSign™ products.

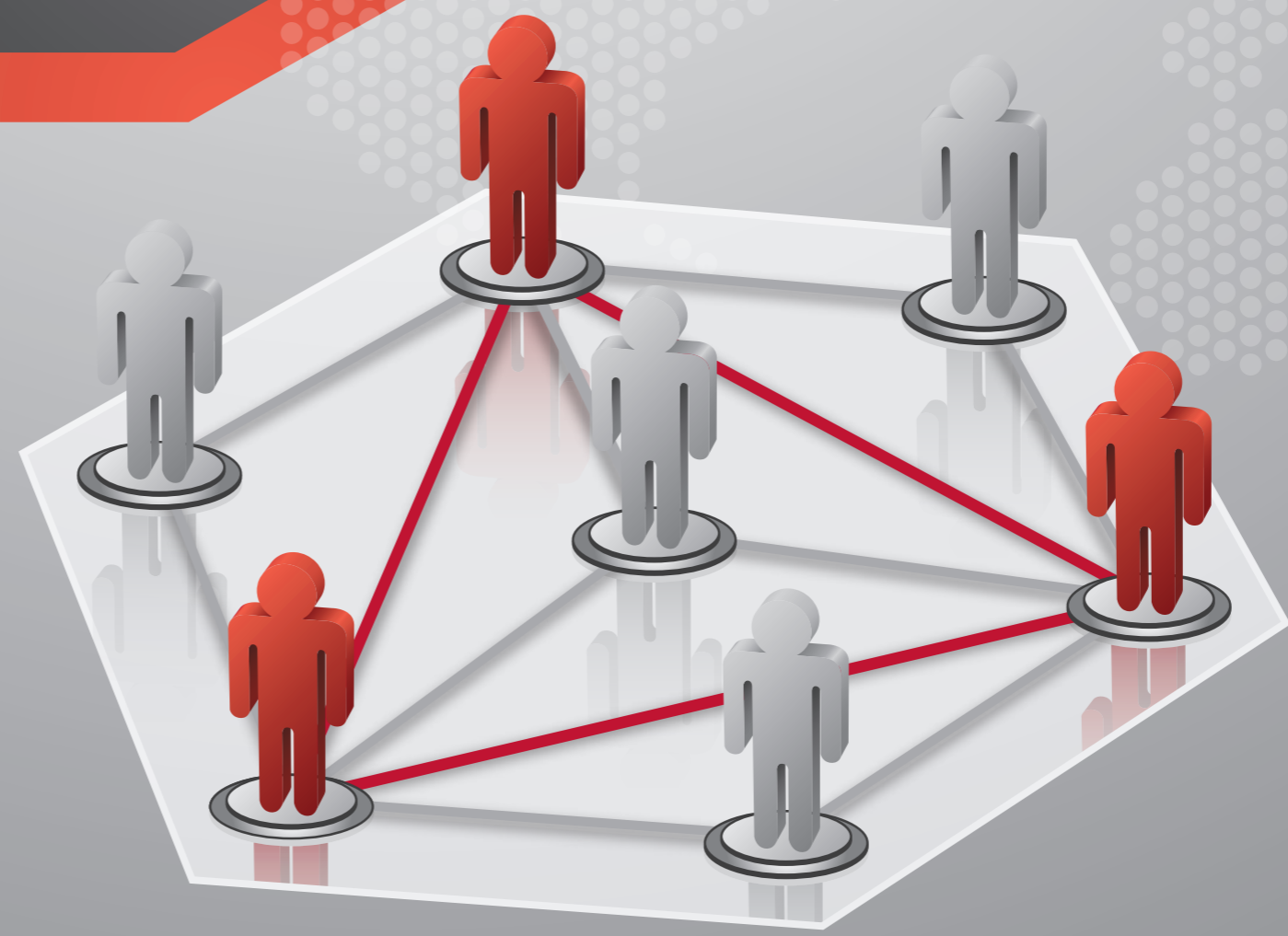
The company was founded in 1996 by a group of technical experts and in the coming years pioneered several new technologies, including patented Electronic Paper Protection Technology (PDMark®), Qualified Electronic Signature Solutions (QSign™) and secure voice communication system for mobile smartphones Silentel® CSD (known also as SecureCall™). In 2008, as one of the first companies worldwide, Ardaco created a new IP based product package for secure voice/data communication and messaging called Silentel® IP (known also as TeamTalk™). In 2010 Ardaco pioneered a new secure messaging system for mobile communication and world most innovative and economical mobile communication solutions for military, police, crises management organisations, integrating Team Talk with typical military or police existing infrastructures such as radios, satellite communication and private communication systems.

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

Silentel®

ENJOY
the **World**
of **SECURE**
COMMUNICATION

Enjoy
Silentel®



ARDACO, a.s.
Polianky 5
841 01 Bratislava
Slovakia
Tel.: +421 (2) 3221 2311
Fax: +421 (2) 3221 2312
info@ardaco.com
sales@ardaco.com

www.ardaco.com

SECURE COMMUNICATION **SOLUTIONS** FOR MOBILE DEVICES

What is SILENTEL®?

Silentel is a complex mobile communication system designed to secure business or private communication using standard communication devices such as mobile phones, laptops and computers. Silentel offers strong protection for voice and data communication against interception and wiretapping.

Silentel runs on most common commercially available devices, significantly reducing the cost to deploy and raising usability to unmatched levels. Voice and data streams, encrypted with advanced strong encryption algorithms, are transmitted with uncompromised voice quality and close to zero latency.

SILENTEL® PROTECTS YOUR BUSINESS MOBILE COMMUNICATION

How does it work?

For a user making a phone call using Silentel there is almost no difference from making a standard telephone call. To make a secure voice call with Silentel, simply select user from the Silentel contact list and press the "green" dial button. 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 encrypt the communication, neither in form of voice track, nor text or other data form. It is even impossible to identify to whom, as well as the time you 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 Silentel application, no information remains stored in the device. It means that no forensic analysis is able to retrieve any sensitive information (like voice calls, text messages and contacts) from the user's device.

Supported platforms

Server Modules:



Client applications:



symbian

Network

Any IP-based network:

- › GSM, 3G, GPRS, EDGE, UMTS, CDMA, W-CDMA
- › Wi-Fi
- › LAN / WAN

SILENTEL® Enterprise and Government solutions

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

Silentel Communication Server

- › Server application representing the core part of overall communication system to provide interconnection of all users within Silentel system.

Silentel CA Server

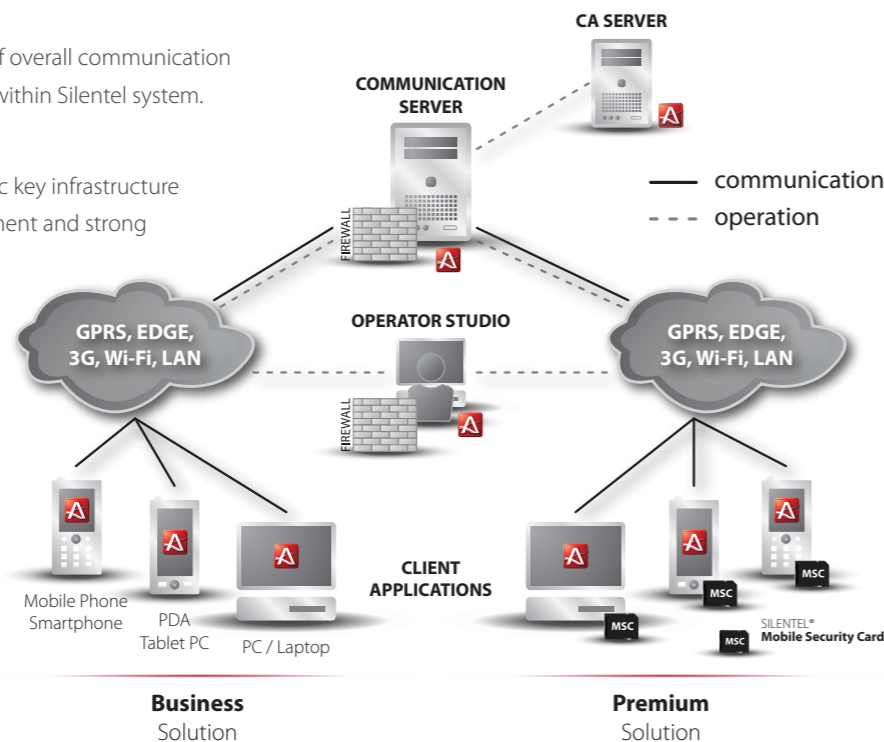
- › Certification authority (CA) to implement public key infrastructure (PKI) necessary for cryptographic key management and strong authentication within Silentel system.

Silentel Operator Studio

- › Standalone application for remote management of Silentel Communication Server and the management of Silentel users and their privileges.

Silentel Client applications

- › Silentel for iOS
- › Silentel for Android
- › Silentel for Symbian
- › Silentel for Windows Mobile
- › Silentel for Windows



Silentel is available in two editions – Business and Premium. The different versions vary mainly in the level of security and implementation on clients' side.

Silentel Business Solution

- › The implementation of the pure software mobile security encryption
- › Client requires only software application installed on client's device

Silentel Premium Solution

- › The combination of software and hardware security modules to achieve military-grade level security
- › Client requires installed software application in combination with Silentel Mobile Security Card (MSC) SD card plugged in into client's device
- › Enhanced security solution for highly demanding customers

SILENTEL® Technical & Security facts

Business

Premium

Communication modes

- › Secure voice calls - software encryption
- › Secure voice calls - hardware encryption
- › Secure text messages - software encryption
- › Secure text messages - hardware encryption
- › Secure managed conferencing
- › Secure contact with user presence status

Security mechanism

- › Client password-based and server certificate-based authentication (RSA 2048)
- › Client-server certificate-based mutual authentication (RSA 2048)
- › Client-server signaling channel encryption (AES 256)
- › Communication end-to-end encryption (AES 256)
- › Emergency mechanism in case of user's device is lost or stolen (disconnect Silentel application, wipe all data and revoke certificates)

Hardware encryption

- › Cryptographic functions provided by Silentel Mobile Security Card (MSC)
- › DPA/SPA and physical attack secured (tamper-proof)
- › Common Criteria EAL 5+ certified

LEGEND: **Business** Silentel Business Solution **Premium** Silentel Premium Solution ✓ Supported — Not Supported