



**NATO approved solution for
voice and data communication**

Why to use **secure communication**?



Implementation and use of **secure mobile communication** is today an unavoidable request – the many cases of mass surveillance is a witness thereof.

More than **80% of all communication is made with mobile phones** and not through fixed lines or stationary systems.

Researchers prove **mass usage of surveillance devices**. The availability of such technology is strongly increasing and the price decreasing.

Gartner (the world's leading research and advisory company) calls for using voice and data encryption.

Why to use **secure communication**?



Implementation and use of **secure mobile communication** is today an unavoidable request – the many cases of mass surveillance is a witness thereof.

More than **80% of all communication is made with mobile phones** and not through fixed lines or stationary systems.

Researchers prove **mass usage of surveillance devices**. The availability of such technology is strongly increasing and the price decreasing.

Gartner (the world's leading research and advisory company) calls for using voice and data encryption.

Are **common encryption apps** secure enough?



Most of them were already hacked, exists specialized surveillance or spying systems targeted for specific apps.

Encryption only during transmission. No data protection on users' devices. No user identity authentication.

No certification. No independent third party security evaluation.

For governments and enterprises – they don't meet any security requirements or standards. Individual user don't have any possibilities to be convinced or inspect the security.

The ability to protect sensitive information with **proven security** can determine the **difference between success and failure**.



*CIA can effectively bypass WhatsApp,
Telegram, Signal, Confide*



*WhatsApp design feature means some
encrypted messages could be read by
third party*



*One photo could have hacked your
WhatsApp and Telegram accounts*

What is **Silentel**?



Silentel 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 eavesdropping and interception.

With **Silentel** you can easily use your mobile device for all types of communication and storing information without compromising your privacy.

Customers including **Public Safety authorities**, **Military**, **Intelligence services** and other **Government organizations** in more than 50 countries rely on the security and quality of Silentel applications.

Silentel guaranteed security



Silentel is the first solution world-wide for secure mobile communication that was positioned in the NATO Catalogue (NIAPC).

Since 2006, Silentel is certified by a growing number of National Security Agencies as a product for secure mobile communication up to levels RESTRICTED and CONFIDENTIAL.

Silentel is the first tempest-certified solution for standard mobile devices in the EU. Compromising emanations (tempest) test done according to the NATO SDIP-27 standard.

Silentel is designed to comply with the latest NATO and US standards in security - using standard commercial devices to protect classified information. Service, maintenance and training costs in case of the Silentel solution are a fraction of the cost of private or dedicated communication systems.



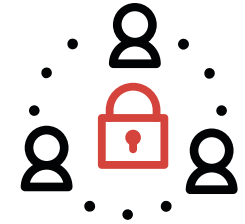
Features for secure communication



Secure Contacts



Secure Voice calls



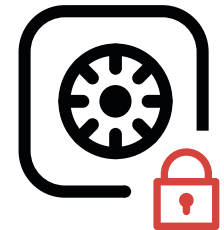
Secure Conference



Secure Messages



Secure File transfer



Secure File storage

Secure Contacts



Silentel application uses own **contacts which are separated from other phone contacts.**

The contact list for each user is created by the communication group manager via **Silentel Studio.**

Silentel contacts are only available when the application is running. After switching off the application, they are **completely erased and are not stored on the phone.**

For each contact is displayed – user presence status (online, offline, invisible) and “in call” notification.

Secure Voice calls



Standard voice calls between two participants, but device-to-device encrypted.

During the call, all information transmitted by the Silentel system is **encrypted by the sender and decrypted only by the receiver**.

During the voice call:

- **Add** participant(s) – and switch to conference
- **Mute** the microphone
- Switch to external **Speaker**
- Switch to **Bluetooth hands-free**

Secure Conference



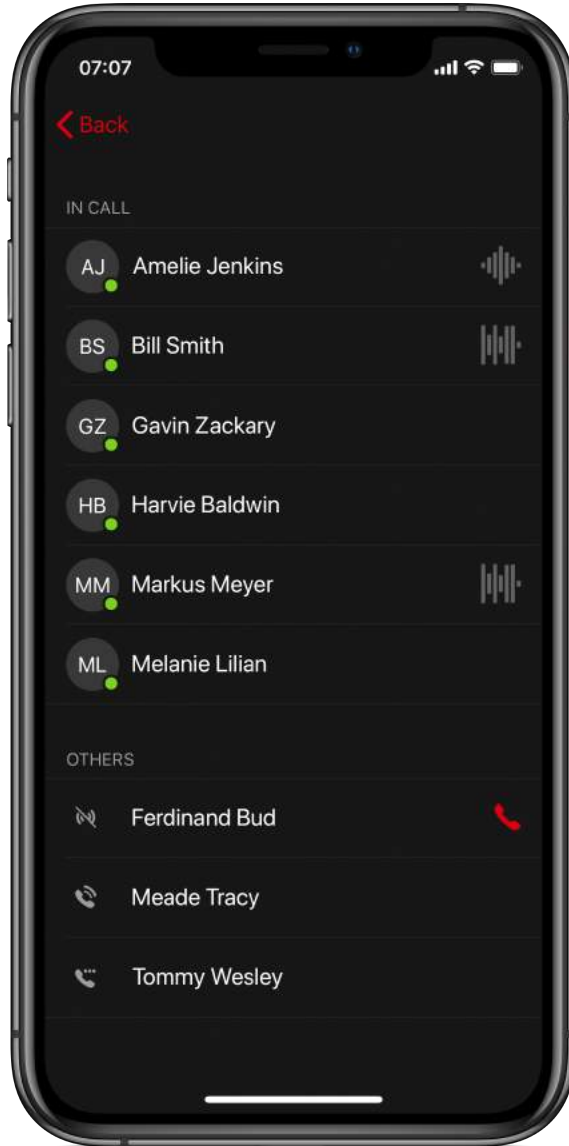
Secure conference allows **real-time communication between two or more users.**

Conference provides **automatic voice detection** - the voice of the participant starts playing automatically when he starts talking.

Other **users can be added** during the conference itself.

The user can **leave the conference** at any time and then **re-join it again.**

Secure Conference



Secure conference – List of participants

The conference allows you to view the list of participants with the following details:

- Who **is present** - received a conference call
- Who **is not present** - was invited but did not accept or already leaved a conference call
- Who **is currently talking**

Secure Messages

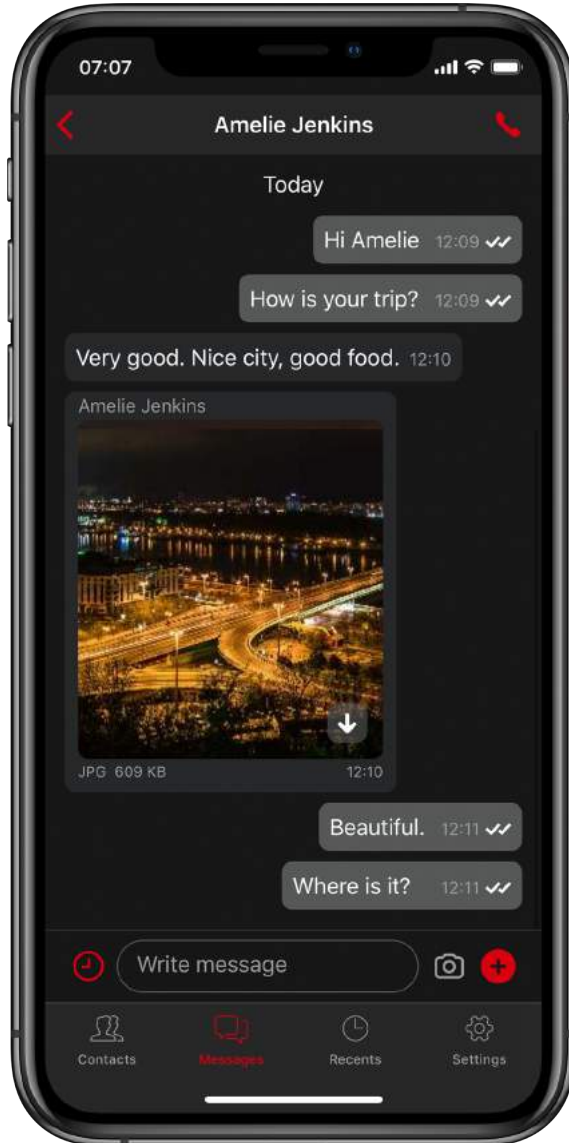


The content of the message is **encrypted before sending**. Only after the message has been delivered to the receiver, the content is decrypted. Except from the sender and receiver, **nobody can decrypt and read** the message.

Message details – shows date and time of sending, delivery and receipt of the message.

Message expiration - set up a desired time expiration by sender. Text message is automatically wiped after expiration time is achieved.

Secure File transfer

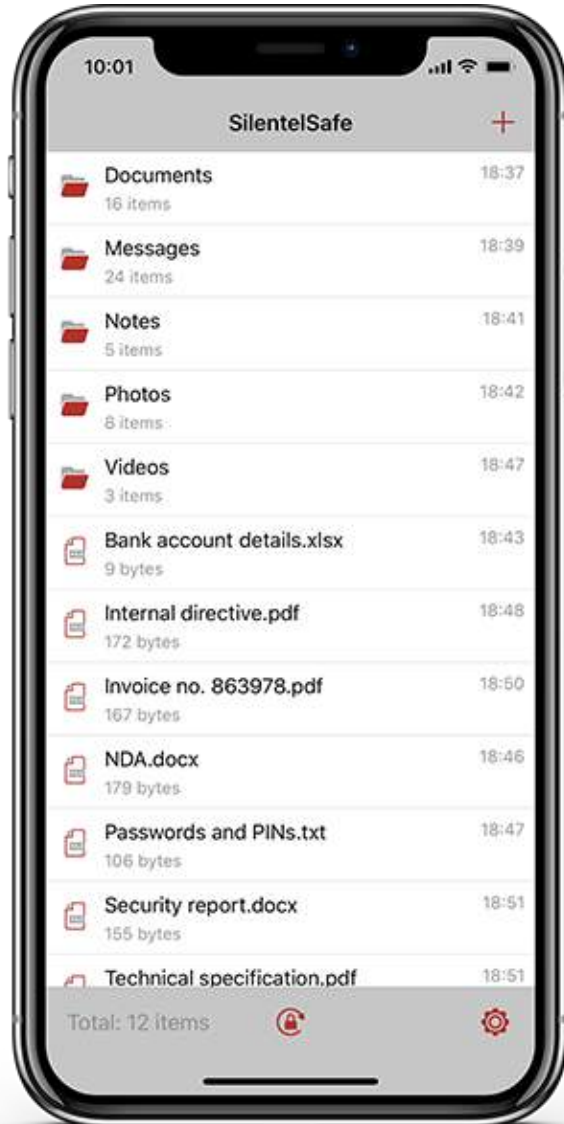


Sending encrypted documents, images or any other files.



The Silentel application offers to take pictures or video using the camera, record audio and send it as a file to a recipient in an easy and simple way.

Secure File storage



SilentelSafe provides secure storage for your sensitive documents, photos or any other files.

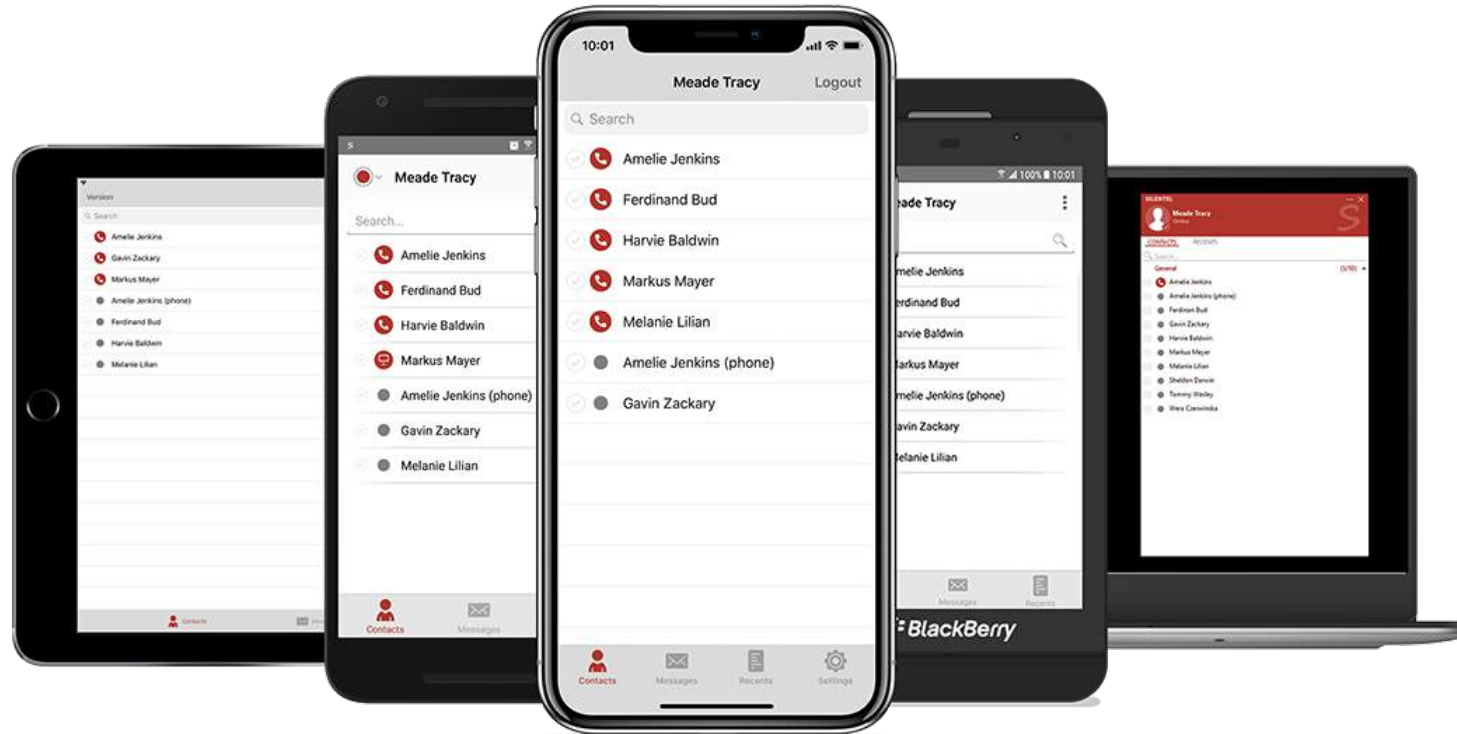
SilentelSafe features:

- Store securely all your sensitive documents
- Import documents from third party applications
- Share securely your sensitive documents with others using Silentel

Multiplatform



Silentel is available for most used devices and operating systems.



IPHONE



IPAD



ANDROID
PHONE



ANDROID
TABLET

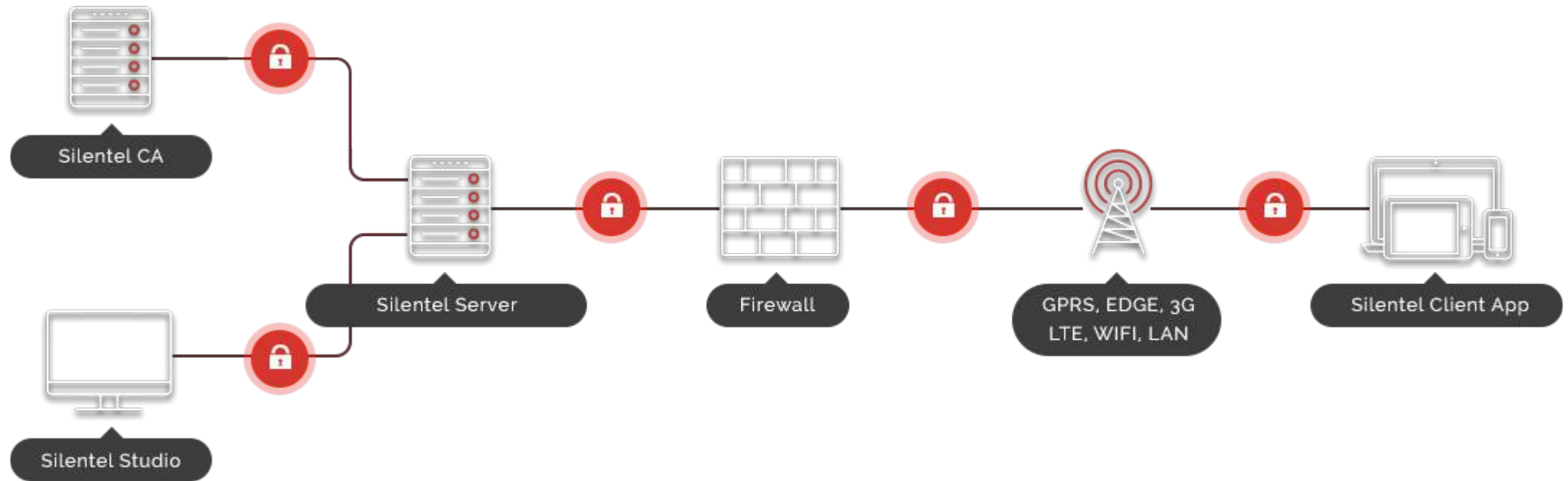


BLACKBERRY



WINDOWS PC

Complete solution under full control of your organization



Silentel Server

Distribution of encrypted communication data between clients.

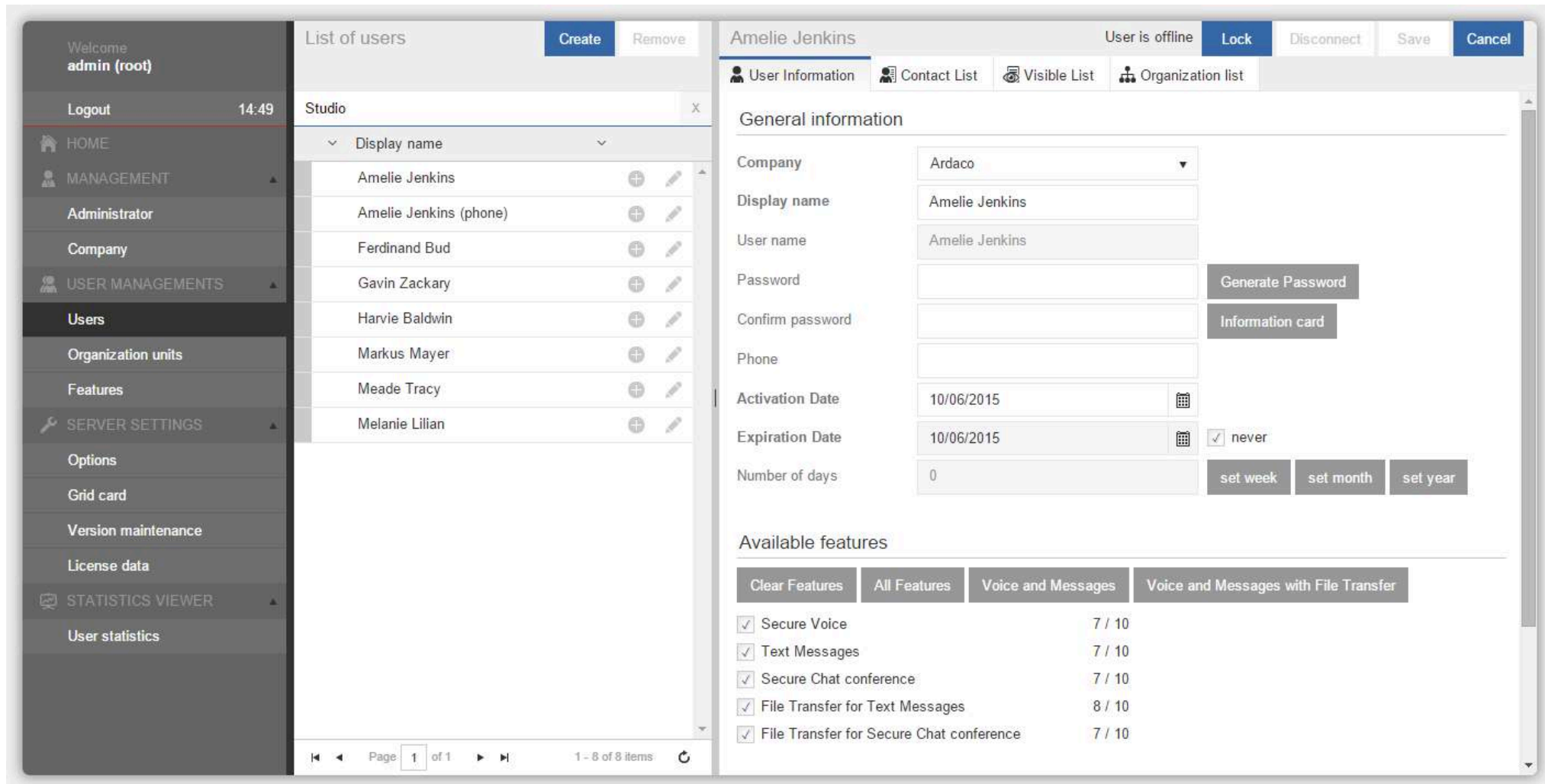
Silentel CA

Implements public key infrastructure (PKI) for cryptographic operations.

Silentel Studio

Manage your users and closed communication groups.

A smarter and simpler way to manage your secure communication system



The screenshot displays the Silentel Studio user management interface. On the left is a dark sidebar with navigation options: HOME, MANAGEMENT (Administrator, Company), USER MANAGEMENTS (Users, Organization units, Features), SERVER SETTINGS (Options, Grid card, Version maintenance, License data), STATISTICS VIEWER, and User statistics. The main area is divided into two panels. The left panel, titled 'List of users', shows a table of users with columns for 'Display name' and actions (add/edit/delete). The right panel, titled 'Amelie Jenkins', shows user details and settings. At the top right of the right panel are buttons for 'Lock', 'Disconnect', 'Save', and 'Cancel'. Below these are tabs for 'User Information', 'Contact List', 'Visible List', and 'Organization list'. The 'User Information' tab is active, showing fields for 'Company' (Ardaco), 'Display name' (Amelie Jenkins), 'User name' (Amelie Jenkins), 'Password', 'Confirm password', 'Phone', 'Activation Date' (10/06/2015), 'Expiration Date' (10/06/2015), and 'Number of days' (0). There are also buttons for 'Generate Password', 'Information card', 'set week', 'set month', and 'set year'. At the bottom of the right panel is a section for 'Available features' with a table of feature status.

Available features	
Clear Features	All Features
<input checked="" type="checkbox"/> Secure Voice	7 / 10
<input checked="" type="checkbox"/> Text Messages	7 / 10
<input checked="" type="checkbox"/> Secure Chat conference	7 / 10
<input checked="" type="checkbox"/> File Transfer for Text Messages	8 / 10
<input checked="" type="checkbox"/> File Transfer for Secure Chat conference	7 / 10

Web-based application for remote **management of Silentel Server** and the **management of Silentel users**, their contact list and permissions.

User account management:

- Create, edit, lock, disconnect and remove users
- Edit the users' contact list which is unique for each user
- Setup initial password or reset password for users
- Enable or disable communication features for users (secure calls, conference, messages, files)
- Allocation of the users to the Organization Units
- Generate usage statistics to check if your system is used effectively.

Separated communication groups – Users (or licenses) can be assigned into separated groups. Each group can be managed by a **group administrator** that can access and manage only users within the group.

Highest security designed for users



Make your work go faster

- Protect your sensitive communication = ability to minimize the time spent on personal meetings or physical delivery of documents
- You will save valuable time as well as significantly reduce travelling costs

Save time, money and resources

- Easy to use & fast to deploy
- Users will quickly adapt to a new and simpler way of handling any sensitive or confidential information
- No special skills neither for use, installation nor maintenance

Solution that fits your needs

- Standard turn-key services can be deployed in a matter of a few hours for the whole organization
- Tailor-made solutions are available to fit specific needs

Customers in more than 50 countries rely on the security and quality of Silentel applications

About **Ardaco** company



Ardaco, established in 2001, is a leading provider of **Information and Communication security**.

Ardaco develops and provides its own fully scalable **Silentel platform for secure mobile communication**. In addition, Ardaco provides a full range of its proprietary products for **qualified electronic signature – QSign** that enable secure and cost-effective handling of electronic documents.

Individuals, **companies and governmental organizations in over 50 countries worldwide** protect and secure their communication and information with the wide range of Silentel and QSign products.

ISO 9001:2008 certification and regular auditing ensure that we achieve and maintain rigorous standards of both **quality and reliability**. Our key experts are security cleared to the highest levels, including NATO and EU security clearances.



Representative for Argentina:

www.gigsrl.com

info@gigsrl.com

www.silentel.com

