GeoNet

Silentel®

Silentel

A NATO approved military grade secure mobile communication

What is Silentel?

- A NATO approved military grade secure mobile communication app

- It is a multiplatform solution for secure voice, messaging, conferencing, file transfer and mobile device management

- This includes devices using Android 6.0 and above, iOS 10.0 or above as well as Windows PC client.

iOS android Windows

What is Silentel?

Not only does Silentel protect your voice and data communication against wiretapping and interception with the highest level of security, it is also easy to use, fast to deploy and users will experience a new and simpler way of handling all their sensitive information. All this is provided at an affordable price for businesses of all sizes.

Data protection has become of paramount importance to organisations, especially with the incessant headline news stories involving data breaches of large organisations in particular. Mobile devices have become an ever increasing target for attacks and neither voice communication (whether via an operator or IP based) nor data on your phones are entirely safe.

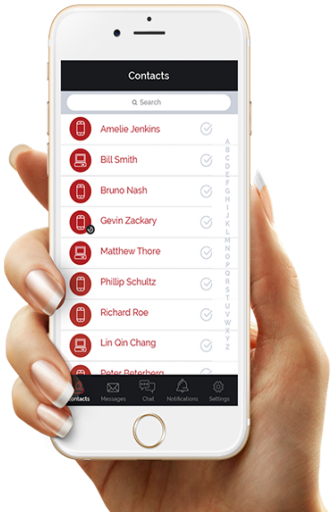
We understand the need to protect your valuable and mission critical information and have a proven track record in doing so. Our solutions have been repeatedly and stringently tested for safety and functionality by governments and related organisations, and have continuously stood up to all tests.

Features

There are a host of features that come with such an affordable service. Our user friendly app operates on a world-class infrastructure with global reach and can be downloaded from the major app stores as well as a Windows PC client.

Highest Safety

Silentel is the only truly certified software-based, secure voice and data solution approved for use with NATO members for confidential information. Since 2006, Silentel has been certified RESTRICTED and CONFIDENTIAL by a growing number of national security agencies as a secure mobile communications product.



Secure Contacts

The Silentel application uses its own contacts directory which is kept separate from all other phone contact directories. The contact list and other sensitive data are not stored on the device, such that after leaving the application, it cannot be accessed unlike with other communication apps.

Features

Secure Voice Calls

There is device-to-device encryption meaning that during a call, all information transmitted by the Silentel system is encrypted by the sender and decrypted by the receiver only.

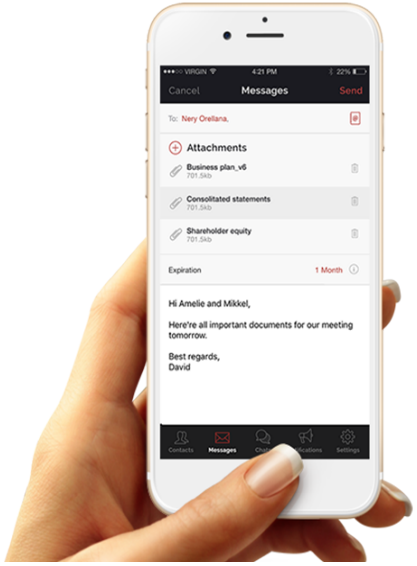
Secure Conference

Conference calls take place with secure real-time voice communication with up to 7 users. This is done using device-to-device encryption and automatic voice detection. You can have instant conference calls without a conference server.

Features

Secure Messages

The content of the message is encrypted before sending for total security. Only after the message has been delivered to the receiver is the content is decrypted. Only the receiver can decrypt and read the message. A third party does not have access to decrypt and read the message.



Secure File Transfer

Silentel also allows you to send encrypted text files, images, audio and videos just like WhatsApp, but in a more secure way and in multiple formats.

So you can take a picture or record a video using the phone camera, or record an audio message or upload a file whilst in the Silentel application. This can then be sent to any recipient in an easy and simple way.

Features

Secure Data Storage

No Silentel data is stored on the user's device, not even the contact list. Even if a mobile device is lost or stolen, no Silentel information will ever be available to anybody who finds the device. This means that no forensic analysis will retrieve any sensitive information, such as voice calls, text messages, files and contacts.

In addition, the SilentelSafe app provides secure storage for your sensitive documents, photos or any files.

Multiple Languages

The language options cover:
- English
- Spanish
- German
- Russian
- Czech
- Slovak
- Simplified Chinese (Mandarin)

Features

Flexibility In Selecting Specific Features

Features such as voice, conference, chat, file transfer, can be purchased separately e.g. only having voice calls is possible.

Flexible Licensing Arrangement

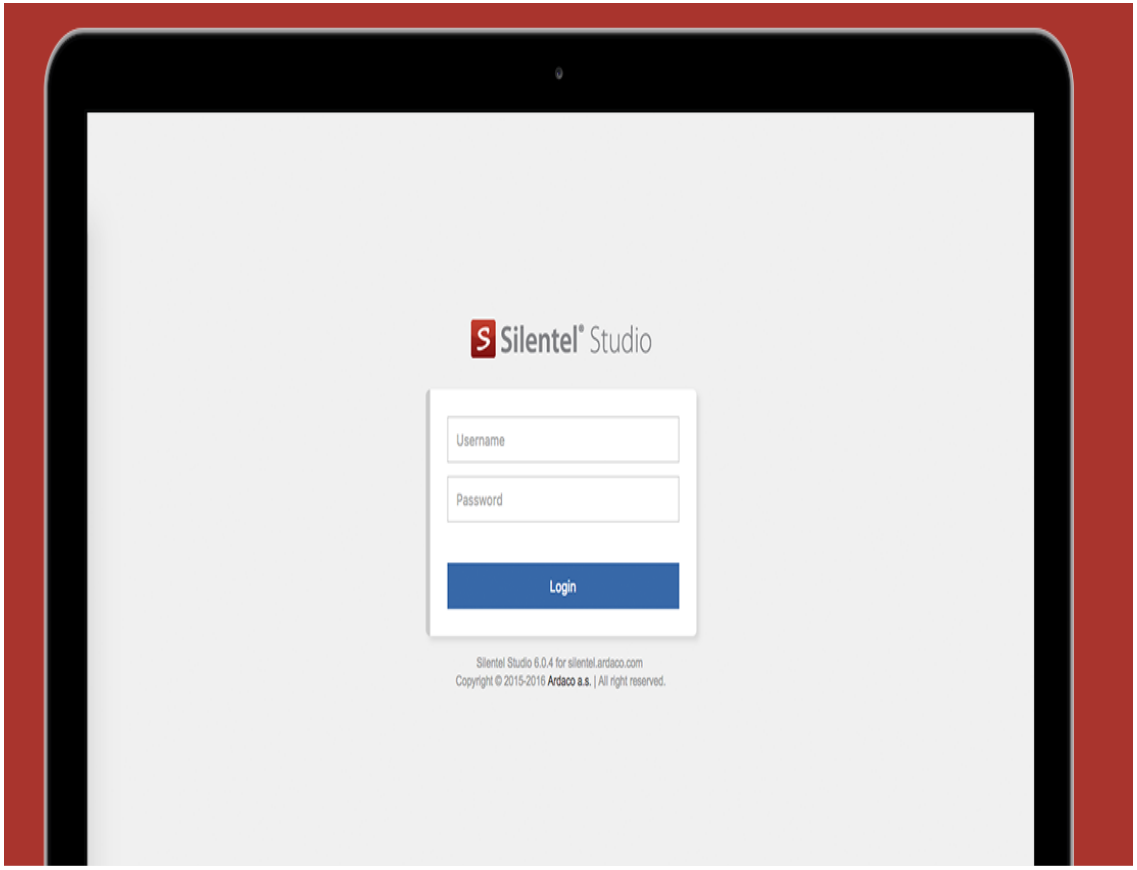
We operate a user-bound licence scheme where a user can use the app on any number of devices that they are logged on to.

Specific Universal Communication Only Available Through GeoNet Telecom

In addition to all the Silentel features above, GeoNet have partnered with a highly experienced security company which allows universal communication to anyone who has the Silentel app using a highly secure infrastructure. This mechanism permits communication outside of your own contact group such that, one Silentel user can communicate with any other user even if they are not in their contact group . This is currently not possible if you sign up for the service directly with Silentel. They only permit contact between users assigned to a designated group.

Silentel Studio

Silentel Studio a Mobile Device Management system providing a smarter and simpler way to manage your users and closed communication groups. It covers one of the important elements of security being, how you manage your communication solution.



Silentel Studio

Create, Edit And Remove Users

Not only can the administrator create, edit and remove users but they can also set and reset users' passwords, lock and unlock users, set users expiration date, enable and disable communication features for each user.

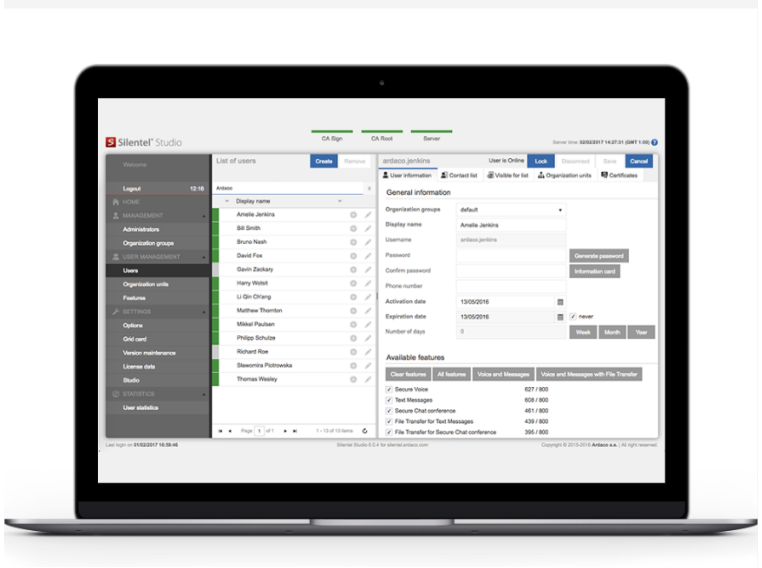
Users' Contact List

Contact Lists can be edited uniquely for each user. You can even separate between the list of contacts which the user can see (Contact List) and the list of contacts to whom the user is visible (Visibility List).

Silentel Studio

Separate Closed Communication Groups

You can create additional separate Closed Communication Groups. Each group can be managed by a Group Administrator who only has access to that closed group.

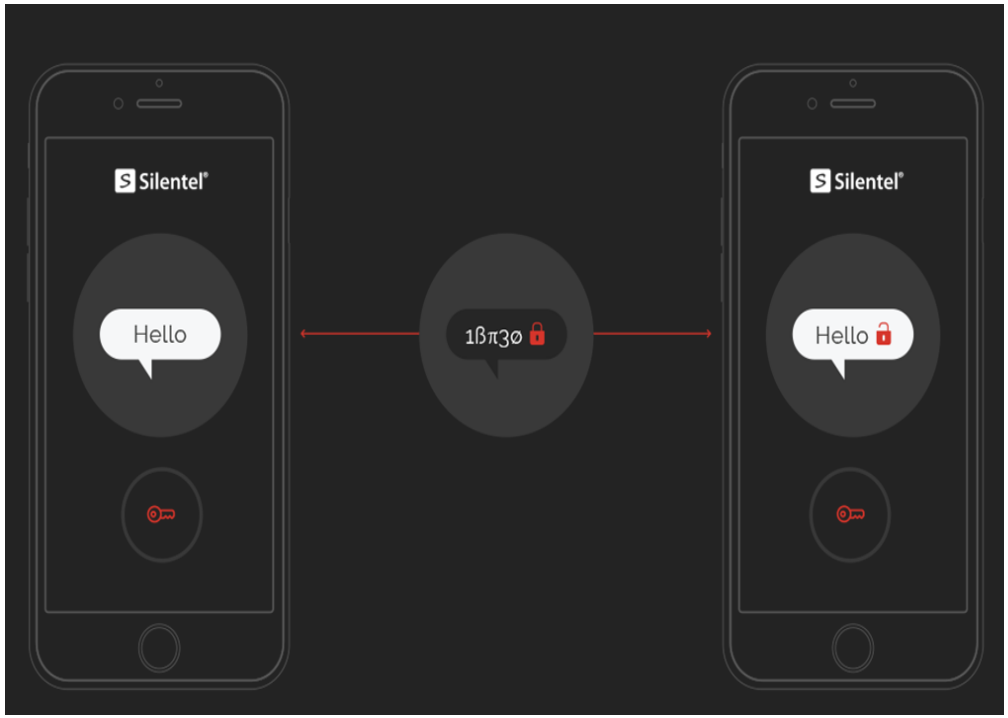


User Statistics

Generate usage statistics to check if your system is being used effectively. These can be exported to Excel, in XSLX format, for analytical reporting purposes.

Security

More than 10 years of proven security, regular independent certifications from several NATO countries combined with military grade encryption makes your information secure at all times.



Security

Device-to-Device Encryption

Communication data is encrypted before sending and is decrypted only after delivery to the receiver, which is done directly on the users' devices. Data is never decrypted during transfer. The encryption keys are not held on Silentel servers so it is not possible to decrypt the content even at that level.

One-time Encryption Keys

Each communication is protected by a unique encryption key which is generated during communication establishment. This means that each communication between two users, even each communication between the same two users, has unique encryption keys which cannot be predicted. Each encryption key is destroyed immediately after the communication ends.

Secure Data Not Stored On Device

No secure data is stored on the user's device, not even the contact list. Even if a mobile device is lost or stolen, no Silentel information will ever be available to anybody finding the device. This means that no forensic analysis will retrieve any sensitive information, such as voice calls, text messages, files and contacts from the user's device.

Security

Privacy

Service providers store a huge quantity of personal metadata about the subscribers including their communication and location. The Silentel system does not require any personal data such as - name, address, GSM number or location. Communication is transmitted only as data (similar to internet browsing) in encrypted form making your calls and messages untraceable.

NATO Approved

Silentel has NATO approval and is certified by a growing number of National Security Agencies within NATO countries. It is the first solution world-wide for secure mobile communication that was positioned in the NATO Information Assurance Products Catalogue (NIAPC). NIAPC brings together all information security (InfoSec) and information assurance (IA) products and services that are evaluated and deemed suitable for use in the NATO environment (NATO nations and NATO civil and military bodies).

InfoSec is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. The primary focus is the balanced protection of the confidentiality, integrity and availability of data while maintaining a focus on efficient policy implementation, all without hampering organisation productivity. This is largely achieved through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan.

IA is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

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

Security


Compare security encryption
STANDARD GSM
COMMON ENCRYPTION
SILENTEL
Passive Attack
Active Attack (Fake BTS)
MOBILE NETWORK
ALICE
BTS
BTS
BOB

Security

Issues With Standard GSM

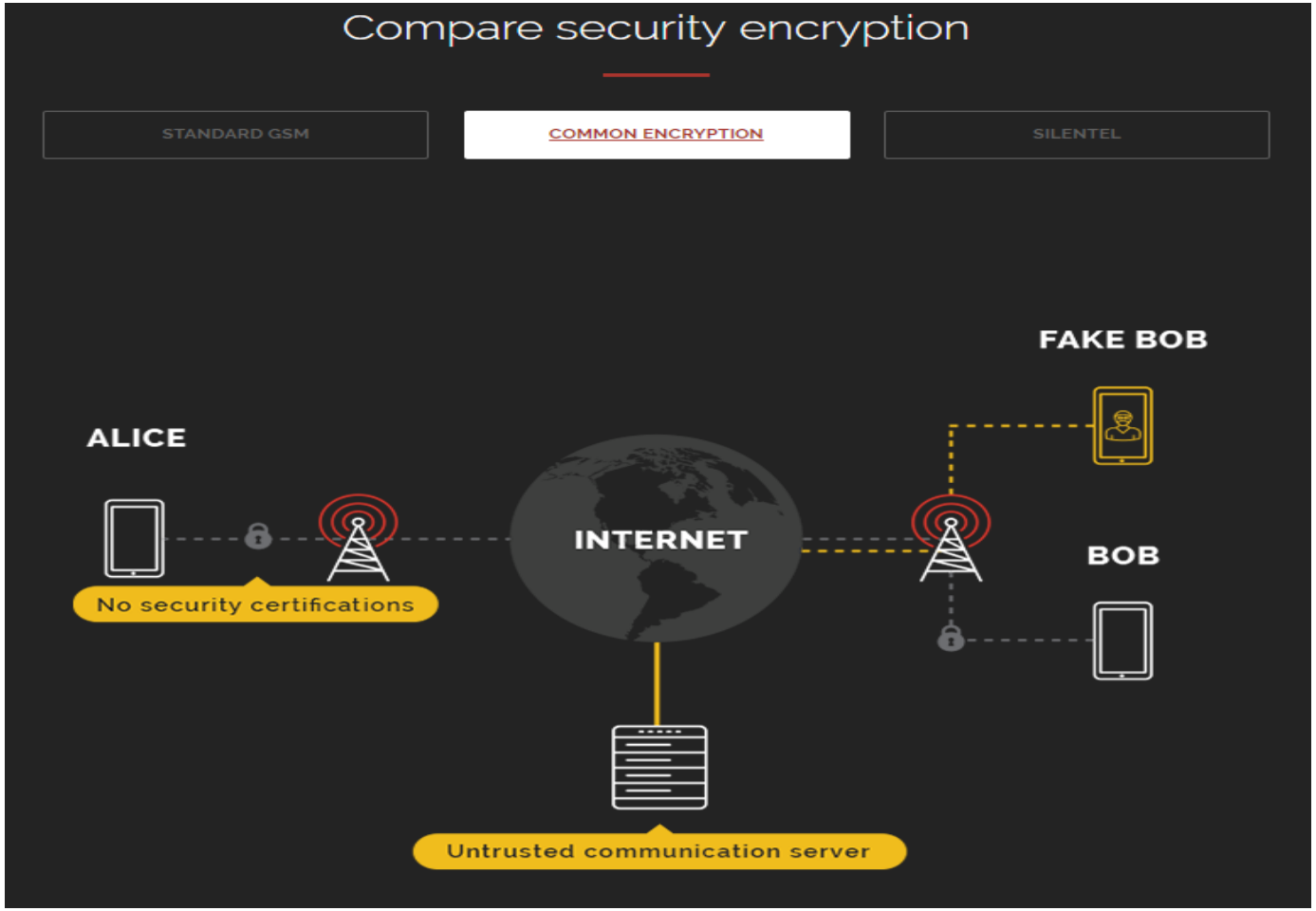
Active Attack

Design weaknesses in the GSM standard can lead to the creation of fake mobile towers and/or base transceiver stations (BTS) set up between the target mobile phone and the actual towers. Unfortunately, ill-doers have created many demonstrations and manuals on how to perform such attacks based on open-source software and commonly available hardware at attractive price points, and thus are adopted by a dangerous number of lawbreakers.

Passive Attack

Did you know that GSM signal is always encrypted? Unfortunately, this encryption is so outdated and weak that there exists several techniques which enable decrypting your communication with up to a 99% success rate.

Security


Compare security encryption
STANDARD GSM
COMMON ENCRYPTION
SILENTEL
FAKE BOB
ALICE
INTERNET
BOB
No security certifications
Untrusted communication server

Security

Issues With Common Encryption

No Security Certifications

The first and most important factor to consider regarding security is if a third-party security evaluation is available. Without this, the supplier can claim any kind of security mechanism since there is no way the client can verify or prove the contrary.

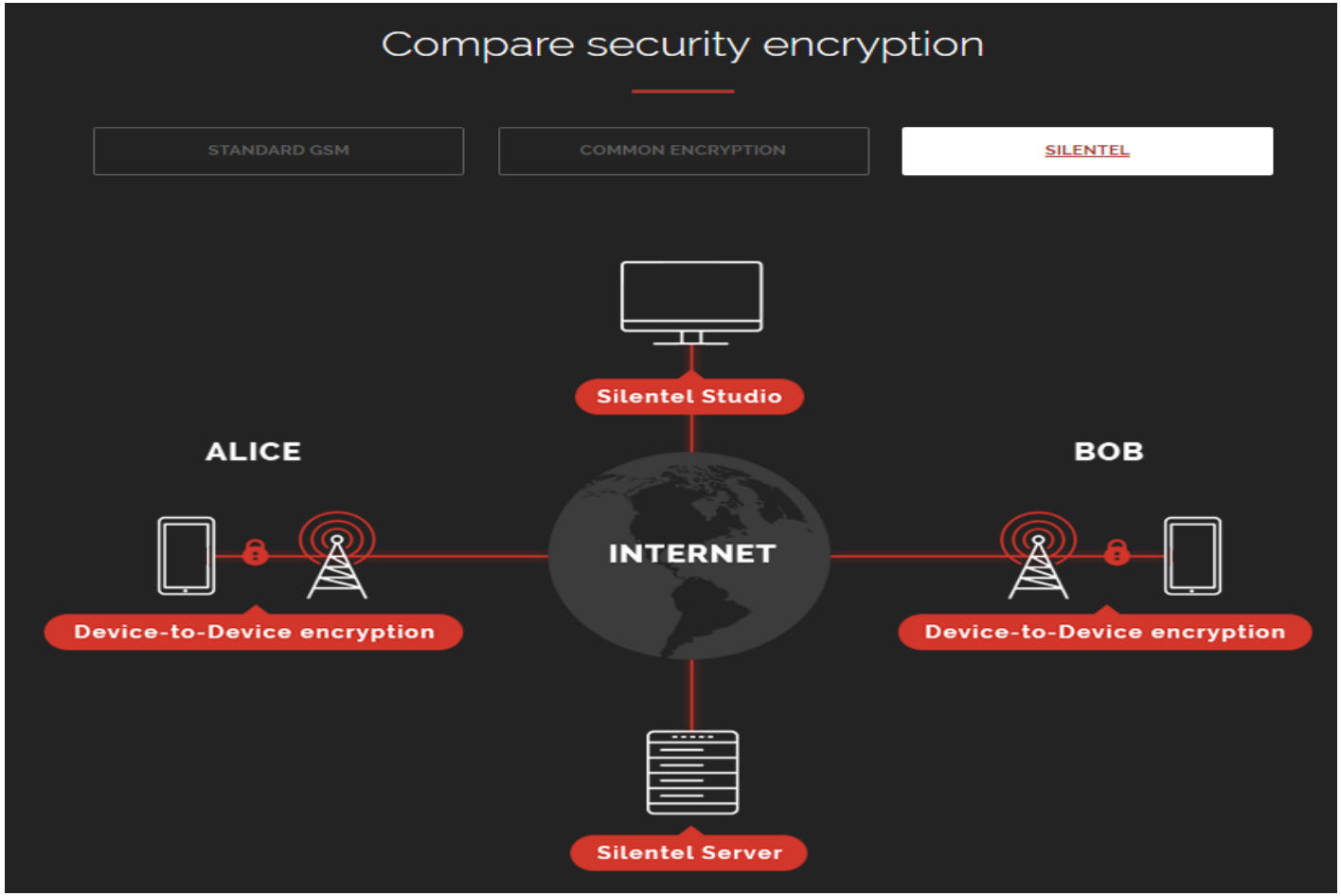
Untrustworthy Communication Server

Most encryption applications use a central communication server. Claims that an application that uses end-to-end encryption is fully secure are baseless when a communication server is able to be used to intercept or reconstruct the session encryption key or can re-encrypt the communication.

Fake Identity (“Fake Bob”)

Most encryption applications allow open registration. Under these cases there is no real control of the communication group or the identity of the contacts joining the group thus, there is a higher risk of sending messages to someone who has created a fake identity.

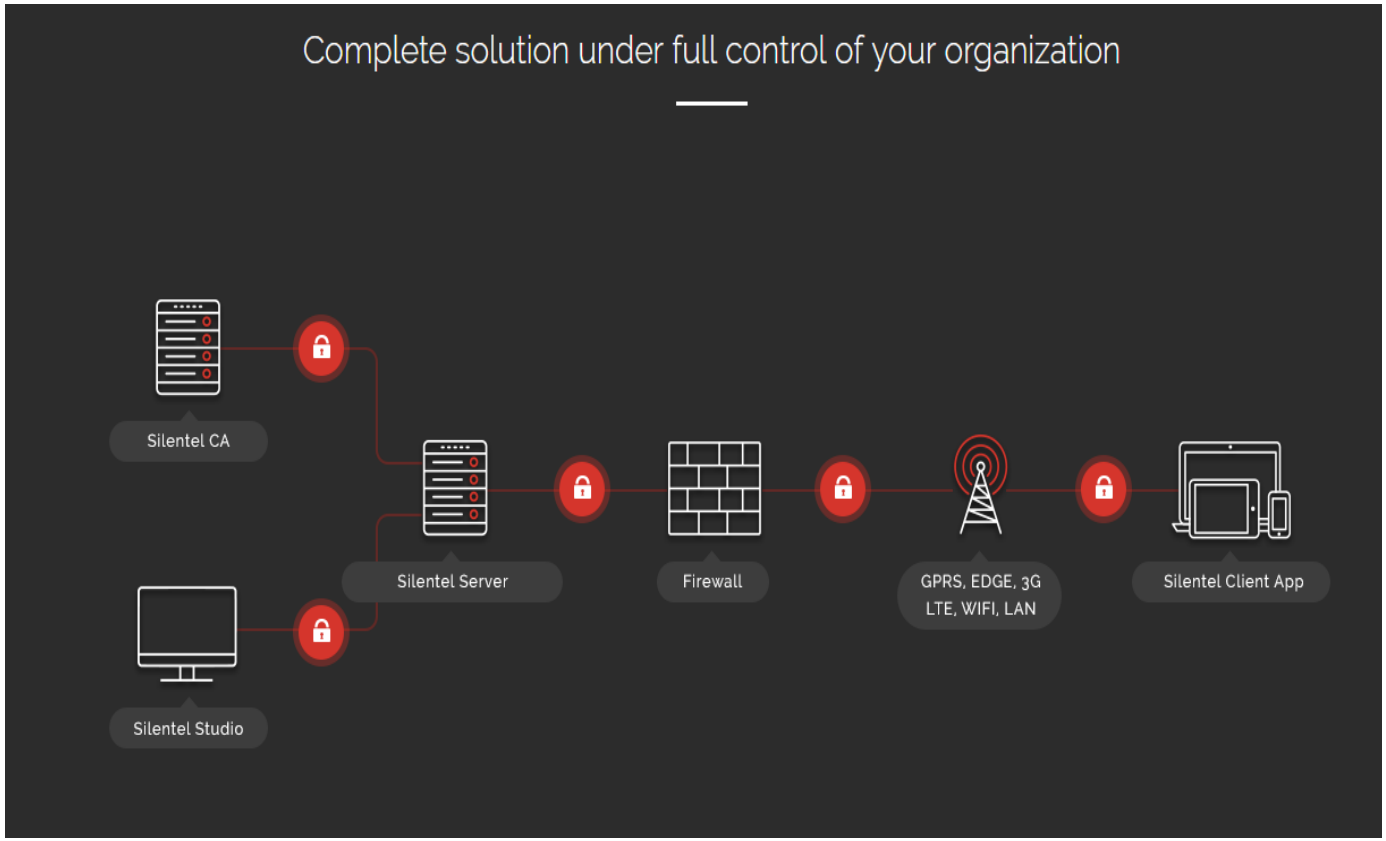
Security


Compare security encryption
STANDARD GSM
COMMON ENCRYPTION
SILENTEL
Silentel Studio
ALICE
BOB
INTERNET
Device-to-Device encryption
Device-to-Device encryption
Silentel Server

Security

Silentel Set-up

The advanced security protocol means that the encryption keys are securely kept from all users and thus they are unable to be decrypted to access any data or voice content.



Silentel Benefits

Guaranteed Security

More than 10 years of proven security, regular independent certifications from several NATO countries combined with military grade encryption means that your information secure at all times.

Time Saving

Silentel not only protects your sensitive information but in addition, provides the ability to minimise the time spent on having personal or secret meetings for physical delivery of documents and other materials. You will save valuable time as well as significantly reduce travel costs.

Quick Deployment

Silentel is easy to use and fast to deploy. Users will adapt quickly to a new and simpler way of handling any sensitive business information. It does not require any specialist skills for installation, maintenance or use. It can be used on all the major mobile operating systems and Windows PC client.

Flexible Solutions To Fit Your Needs

Silentel solutions cater for the needs of individuals, small businesses as well as large enterprises and governmental institutions. Standard turn-key services can be deployed in a matter of a few hours for your entire organisation. Tailor-made solutions are available to fit specific needs. Customers have the option of having Silentel as a managed service through a download on a mobile device or Windows PC, or alternatively through an on-premise solution with a mobile security card (MSC) where the software is set up on their own servers.

Enquires

Please do not hesitate to contact us regarding this product with any questions or to register your interest.

Sales & Information

Telephone: +44 20 3747 4669

Email: sales@geonettelecom.com

Address:
GeoNet Telecom Limited
Weatherill House Business Centre
23 Whitestone Way
Croydon
CR0 4WF
United Kingdom

Website: www.geonettelecom.com