FREQUENTLY ASKED QUESTIONS - FAQ

WHAT IS SECFONE?

SECFONE is an Internet based global communication system with its centre in Switzerland providing secure, non-interceptable phoning.

Using SECFONE subscribers can call each other in a non-interceptable way within a secure network. SECFONE also allows the secure sending of files and messages. Within the worldwide network of SECFONE all calls are intranet calls. The service is provided for a monthly fee with no minute or connection fees. You can easily turn your smart phone into a Secphone mobile if you subscribe to the service.

Order the SECFONE service, insert your SECFONE cryptocard, install the SECFONE software from the Google Play web store and you can make secure calls immediately. The network communication technology developed by SECFONE itself, MVCN™ (Manageable Virtual Closed Network), is an IP based (operating through the Internet), virtually closed network. The devices operating as the end points of the network carry out a secure peer-to-peer communication with each other.

WHAT MAKES IT SECURE?

The security of SECFONE rests on a three-pillar system: a special secure network solution, a unique cryptochip and a software protecting the phone together make SECFONE calls non-interceptable.

The security of SECFONE is guaranteed by a patented secure network solution called MVCN (Manageable Virtual Closed Network). Using this method, SECFONE is able to manage calls within an Internet based but closed and coded secure network. The unique security characteristics of the MVCN network make SECFONE calls non-interceptable.

The coding of the special network solution is such that the information coded by the sender can only be decoded by the recipient of the communication. For this reason, SECFONE communication is not interceptable for anybody else besides the recipient. The communication of the devices using the network is also protected against each other, thus the number of SECFONE devices using the same MVCN network can be freely increased without reducing the level of security.

In the MVCN network all keys are secret. None of the keys protecting the network pass through the network itself at any time, these keys never actually leave the target hardware on which they are stored and managed. In the MVCN network there is no uncoded information traffic, not even when establishing contact and no concentrator is required.

The centre of the SECFONE network is located in Switzerland. For security reasons the centre does not store the keys for protecting the end points and needed for decoding and SECFONE calls do not pass through the centre, not even in coded form.

Would you like to learn more? Learn more on the special security characteristics of the MVCN network from our MVCN publication or from our home page.

The special coding technology of the MVCN network provides extremely high coding security but for the full protection of the network we also need to make sure that the keys themselves protecting the network are safe.

For this reason reason the secure use and storage of the network protection keys is done by a special cryptochip. The keys stored in the cryptochip never actually leave the chip, during use the chip itself does the actions necessary with keys. Due to the special hardware structure of the cryptochip, the information stored in it cannot be extracted neither electronically or mechanically as any such attempts at reading will destroy the chip and cause the stored data to be lost before the information could be obtained. This way the keys guaranteeing the security of the MVCN network are safe within the cryptochip.

The cryptochip is built into a special micro SD card, this is the SECFONE SD Cryptocard. The SECFONE SD Cryptocard can be inserted into any device that can accept an SD card.

The third level of protection of the SECFONE software is also the protection of the devices used for phoning, that is protection against spy softwares. During every call the SECFONE VoIP application continuously monitors the device used for the conversation in order to ensure that no other software can access the voice signals. In case the SECFONE VoIP application detects a spy software on the phone, it turns off immediately.
The special closed MVCN network, the unique cryptochip protecting the network keys and the application protecting the phone, together guarantee the security of SECFONE calls.

WHAT SECURITY TECHNOLOGIES DOES USE THE SECFONE?

uses a triple channel encryption protocol: the data channel is encrypted with a 448-bit Blowfish CBC-algorithm which makes the encryption/decryption process fast, while the control (identification) channel uses 2048 bit RSA encryption and the identification of the devices is carried out by 1024 bit RSA encryption;

- encryption procedure is operated by an EAL 4+ certified microSD-card;
- periodic symmetric key change is implemented (in every 5 minutes);
- it provides outstanding voice quality compared to the solutions available on the market we have tested so far
- prevents the possibility of installing any malware, virus or spy programs on the phone by straining off all possible installment attempts of such programs and immediately warning against the danger. The user may install such programs only by manual approval notwithstanding the warnings given by the SECFONE-application several times.

FROM WHICH COUNTRIES OF THE WORLD CAN THE SECFONE PROTECTION AGAINST INTERCEPTION BE USED?

It can be used from any country in the world where the local Internet service and your Internet subscription allows it.

HARDWARE REQUIREMENTS

- The device needs to have a functional MicroSD Card slot, that is free SD card space (the SECFONE card has 2 GByte free space where the applications or data needed from the normally used SD card can be placed.)
- Minimum CPU requirement of the device is 1 GHZ
- Minimum RAM requirement is 512 MB*
- Minimum free space on the phone: 15 MB (SMS+Base+VoIP)

(*) The minimum requirement depends on the requirements of other applications frequently used on the smartphone.

OPERATING SYSTEM REQUIREMENTS

Officially, SECFONE is supported on Android OS versions 2.2 and 2.3, 4.0, 4.1 and their sub-versions (minor revisions).
Android OS 3.x (a.k.a. Honeycomb) support is in the works, but is not official at the time of writing.

WHITELIST - OFFICIALLY SUPPORTED MOBILE PHONES

Basically on all phones or TABLET PCs with ANDROID operation systems but with the below additional comments.

We consider a phone/operating system combination to be officially supported only if we have managed to fully test and confirm that SECFONE is properly working on that particular phone and particular operating system version.
Given the large number of Android devices and distributions out there, this list is not definitive and does not mean that SECFONE will not work on other (not-confirmed by SECFONE) phones too.
We are continuously working on expanding this list.

- HTC Desire
- HTC Desire S
- HTC Evo 3D
- HTC Incredible S
- HTC One V
- HTC Sensation
- LG Optimus 2x
- Motorola Defy +
- Motorola Razr XT910
- Motorola Razr XT912
- Samsung Galaxy Note
- Samsung Galaxy S
- Samsung Galaxy S II
- Samsung Galaxy S III
- Samsung Galaxy S IV
- Samsung Galaxy W

Conditionally work

- Sony Ericsson Xperia x10 Android 2.1-update1 - ONLY WITH HEADSET!

CONFIRMED LIST OF NOT SUPPORTED DEVICES

We consider a device to be officially not-supported, only if after fully testing SECFONE on that device, we have confirmed that a subset of SECFONE's functionalities is not feasible on it.

- HTC Hero Android 1.5/2.1
- Huawei U8500 Android 2.2.1 (low CPU)
- Samsung Galaxy Mini Android 2.2.1 (low CPU)
- Samsung Galaxy Spica Android 2.1-update1 (low CPU)

CAN I USE MY PHONE AS SECFONE?

Yes, you can. However your phone has to meet the requirements of SECFONE.

Once you ordered and get the SECFONE cryptocard and signed the SECFONE service contract, you should insert the SECFONE cryptocard into your smartphone's microSD card slot. Install the SECFONE app from Google Play, and enjoy sharing your information privately. See Phone requirements and whitelist for detailed information on system requirements and tested mobile phones.

In case you do not yet have a smart phone, as a first step we recommend purchasing a device with Android to which belongs at least a 100 MB/month Internet subscription. Then getting to know the phone and after having used it (1-3 months) purchasing SECFONE as a second step. You can of course differ from this proposal and can buy the two devices at the same time, especially if you have an IT advisor.

IS IT SAFE TO USE SECFONE ON FREE OR OPEN WIFI?

Yes, it is safe.

SECFONE provides its own encryption system from any network. You have the very same ultimate security level on EDGE, 3G, LTE, Wifi, or any Internet connection.

Note: Encrypted Wifi provides protection only between your device and the Wifi router. If you send clear data throught an encrypted Wifi network, data is accessable in clear (readable) format at the Internet port of the Wifi router. Since Wifi routers are managed locally (for example by an Internet Café), local staff of the premise can access your information, for this reason it is not recommended to use SECFONE with WIFI networks coded in such locations.

WHAT IS SECFONE CRYPTOCARD?

Cryptochips are special chips that protect mobile computer data. Also known as Trusted Platform Modul, or TPM. Cryptochips provide the highest security level, higher than any software based solution.

SECFONE Cryptocard is a cryptochip integrated into a micro SD card. It stores and uses all keys needed for encryption, so keys never leave the secure store of the cryptochip, never relayed to the memory of the phone and never sent over any network.

SECFONE Cryptocard is an unreadable, unwriteable, military standard black-box that provides encryption services.

IS SECFONE A SOFTWARE BASED SECURE MOBILE COMMUNICATION SOLUTION?

Definitely not. SECFONE is the only hardware based secure mobile communication solution available for public.

Like all smartphone apps, SECFONE also has a software user interface. However, SECFONE app does not store any keys used to provide mobile security. All keys are generated and stored at production in unique Sefone SD cryptocards, which should be inserted into your smartphone's microSD card slot. These keys never leave the cryptochip. The cryptochip works as a black box: gets the information to encrypt, encrypts it with its own keys, and sends back the encrypted information. SECFONE cryptocards can not be read or copied by design. So during the manufacturing of the individual SD CryptoCard, neither the manufacturer nor the manufacturing process allows any possibility for access to the keys.

WHAT IS THE CRYPTOCHIP (TPM)?

This is the name of a special security chip and also the specification defining it, the role of which is to protect the data of mobile computers. The separate security chip represents a higher level of security than any other software based solution.
The chip built into the SD card is a target hardware that stores and also uses the keys used for encrypting. It carries out the mathematical calculations with the keys as well, thus the keys never leave the secure storage of the chip and this way never get into the memory of the phone or get transmitted on the network.

CAN I KEEP MY OWN GSM NUMBER?

Within the SECFONE network you will receive your own individual calling number on which you become available to other Secfne users. This does not impact the number used for normal GSM calls, which can still be kept and used.

WHAT KIND OF INTERNET CONNECTION DOES SECFONE NEED?

SECFONE works on all kinds of Internet connections (EDGE (2.5G), 3G, Wifi). The ability to use SECFONE depends on the quality of the Internet subscription. Problems may occur with 5-10% of the calls that may unfavourably impact the proper execution of the conversations. During driving when changing cells, at certain route sections or locations disturbances or break ups may occur in conversations similarly to GSM calls.

DOES SECFONE WORK WITHOUT SIM CARD?

Yes, SECFONE definitely works without SIM card. If you have a smartphone with any Internet connection, and you have inserted the SECFONE cryptocard, and you have a live SECFONE subscription for that card, you can use your smartphone as a SECFONE.

DOES SECFONE SELL PHONES?

No, SECFONE does not sell phone sets as any masrt phone can be turned into a SECFONE if:

- it is a mobile phone with Android operation system that has an SD card slot
- and it has Internet access (WiFi, mobile Internet etc.)

DOES SECFONE SUBSCRIPTION FEE INCLUDES INTERNET ACCESS?

No, SECFONE subscription fee does not include Internet access. Internet access has to be provided by the user by any means available in his/her country. Since SECFONE network that provides secure mobile calls is global, you can make secure calls from any place in the world. Once you have a SECFONE subscription, the only thing you need to make secure calls is an Internet connection. The ability to use SECFONE depends on the quality of the Internet subscription. Problems may occur with 5-10% of the calls that may unfavourably impact the proper execution of the conversations. During driving when changing cells, at certain route sections or locations disturbances or break ups may occur in conversations similarly to GSM calls.

DOES SECFONE SMS REALLY DESTRUCTS ITSELF?

Yes. If the sender checks the "Self destruct" checkbox when sending the SECFONE SMS, the message is destructed 20 seconds after reading. SECFONE SMS is destructed on the sender's SECFONE too.

CAN I CHANGE MY SECFONE PIN CODE?

No, you can not. The SECFONE PIN code placed into SECFONE Cryptocard at production. Since SECFONE Cryptocard can not be read or written - thus provides the highest security level available -, it is physically impossible to change SECFONE PIN code. Furthermore if missed three times at any time without time limitation, it can be restored with significant cost only (anticipated at 100 EUR).

HOW MUCH INTERNET DATA SECFONE NEEDS MONTHLY?

With daily usage 1 GB data is enough for SECFONE, but minimum 100 MB data traffic may be sufficient already. 55-60 hours of talking on SECFONE means approximately 1 GB data stream.

WHAT DOCUMENTS ARE REQUIRED FOR MAKING A SUBSCRIPTION contract?

In case you wish to subscribe as an individual, your personal ID card, address card and a public utility bill will be required together with a signed copy of these documents.
In case of businesses a specimen signature, a certified copy of the company register not older than 30 days and the personal documents (ID card and address card of the signatory) together with the signed copies of these documents are required.

WHEN AND HOW DO I RECEIVE MY CARD?

After having signed the User Agreement and having paid the price of the cards, you will receive the cryptocard needed for using the service from NICOpro Kft. directly. We also undertake on the spot installation if agreed in advance.

WHO CAN I CALL WITH SECFONE?

You can call any other SECFONE subscriber that you know the SECFONE number of.
Secure communication can be established only between two SECFONEs - smartphones with SECFONE Cryptocard, SECFONE software and live SECFONE subscription - if the caller party have the SECFONE number of the called party. No SECFONE phonebook exists.

Institutions, companies and organizations may subscribe in tens, hundreds or even thousands to involve their employees and protect against interception.

HOW CAN I START USING THE SERVICE AFTER HAVING PURCHASED THE CARD?

After having connected the SD card and installing the software restart the phone and the service can be used immediately. On the spot installation is available if agreed in advance.

HOW SHALL I START USING IT?

Following installation you can call the known SECFONE users or enter contacts using the key pad of the SECFONE application. Using SECFONE SMS you can send encrypted messages with attachments up to 5 GB.

IF I INSERT THE SECFONE SD CRYPTOCARD, WHY CAN'T I SEE WHICH OF MY CONTACTS HAVE SIMILAR ACCESS LIKE WITH VIBER FOR EXAMPLE?

SECFONE is one of the highest quality service providing secure communication, for this reason it does not allow access to the SECFONE numbers of other users.

HOW CAN I STORE THE SECFONE NUMBERS OF CONTACTS?

From the call list in the SECFONE application or using the "Add new" menu option.

WHAT ARE THE CONTACT DETAILS OF THE OFFICIAL DISTRIBUTOR CUSTOMER SERVICE OF NICOPRO KFT?

Please send your inquiries by e-mail to **nicopro@nicopro.hu.** We answer all inquiries.
Web sites:**www.SECFONE.nicopro.eu; www.nicopro.eu**

I EXPERIENCE DELAY, SHIFT IN THE CONVERSATION COMPARED TO REAL TIME. WHY?

The secure mobile communication service of SECFONE operates on the Internet. So when the Internet service used is not appropriate for shorter periods, you may perceive delays or interruptions in the communication. The system detects this and constantly attempts to correct. When the quality of the Internet connection is restored, the conversation will be uninterrupted again. In case the degree of shift is disturbing, initiate a new call.

THE CONVERSATION GETS INTERRUPTED. WHAT CAN BE THE REASON?

The interruption of SECFONE conversations that rarely occurs may be caused by the temporary deterioration in the quality of Internet access.
The ability to use SECFONE depends on the quality of the Internet subscription. Problems may occur with 5-10% of the calls that may unfavourably impact the proper execution of the conversations. During driving when changing cells, at certain route sections or locations disturbances or break ups may occur in conversations similarly to GSM calls.
In case an application attempts to access the microphone, it may also cause the immediate interruption of the conversation. This might, for example, be triggered by speech recording on smart phones. **For this reason, the recording of conversations must be done in a different way to which the ABSONIC speech management and recording products of NICOpro Kft. may also provide a solution (www.nicopro.hu).**

DOES AN INCOMING REGULAR GSM CALL INTERRUPT MY SECFONE CONVERSATIONS?

The SECFONE conversation is paused on the other party's phone in case of an incoming regular GSM call to the phones of either of the parties. The "Line busy" signal is shown on the display of the phone which in itself does not interrupt the conversation. As soon as the GSM call is ended SECFONE communication is restored.

THERE IS NO GREEN DOT IN THE UPPER LEFT CORNER, ONLY RED. WHAT SHALL I DO?

The Internet access of the phone is prevented by either exceeding the data limit of the subscription package or by the lack of credit in case of prepaid cards.

THERE IS NO GREEN DOT IN THE UPPER LEFT CORNER, ONLY GREY. WHAT SHALL I DO?

The phone has no Internet access. Please make sure that the phone has Internet access, which can be WIFI, 3G or any other type of proper quality Internet access.

CAN THE ENCRYPTING BY VIOLATED OR BROKEN THROUGH THE ANDROID OPERATION SYSTEM?

ANDROID is an open source code system which means that anyone can access it. So if a security gap is placed in it, anyone can check, uncover or publish it at any time. This way the probability of identifying such gaps is much higher than in closed source code systems. This makes any open source code systems, for example LINUX, much more reliable than a closed source code system that, as it is well known, may contain security gaps.
To sum it up, the probability of breaking or bypassing the interception protection of SECFONE through the ANDROID operation system is much smaller than it would be using a closed source code system.

HOW CAN I RECORD THE CONVERSATIONS?

There is no way to record conversations on the mobile itself as the SECFONE solution does not allow such applications to run parallel with SECFONE. But there are solutions for recording SECFONE conversations using the own products of NICOpro Kft. (www.nicopro.hu), as official distributor, after reviewing requirements and possibilities. The recording of conversations can be done at the speakers' phones and/or in the centre of the group, in case of a group subscription. Of course, for regular GSM calls voice recording softwares may continue to be used on the phone.

WHAT IS SECBOX?

The Secbox is an intelligent network communication device using MVCN-technology capable of building a private, closed and secure virtual network over the Internet. The endpoints of this network are the Secbox-devices, which use the Internet as transmission media.
A virtual network built from Secboxes can be used to send and receive data, voice, video files or any other digital data stream. You can make Internet phone calls (VOIP) **SECURELY**, without being afraid that someone taps the line; build a worldwide private intranet, and connect securely and instantly to this intranet anywhere in the world.

The Secbox uses a **PEER-TO-PEER CONNECTION** for communicating between the devices, there is no central network hub allowing potential eavesdroppers to aim a single point of attack. The secure communication is subject to using Secbox devices at all ends of the communication.

Users can be identified with their fingerprint to prevent unauthorized access to Secbox devices.

In order to meet the different users' demands Secbox devices are manufactured in **different types, with using different bandwidths.**

WHICH EUROPEAN UNION LAW IS SECFONE SUBJECT TO?

The hardware and software service is partly classified as a product of dual use and as such its trading is subject to EU Council Regulation 428/2009.

NICOpro Kft. official reseller
website: **www.secfone.nicopro.eu; www.nicopro.eu**
email: nicopro@nicopro.hu; phone/fax:+36-79-326581