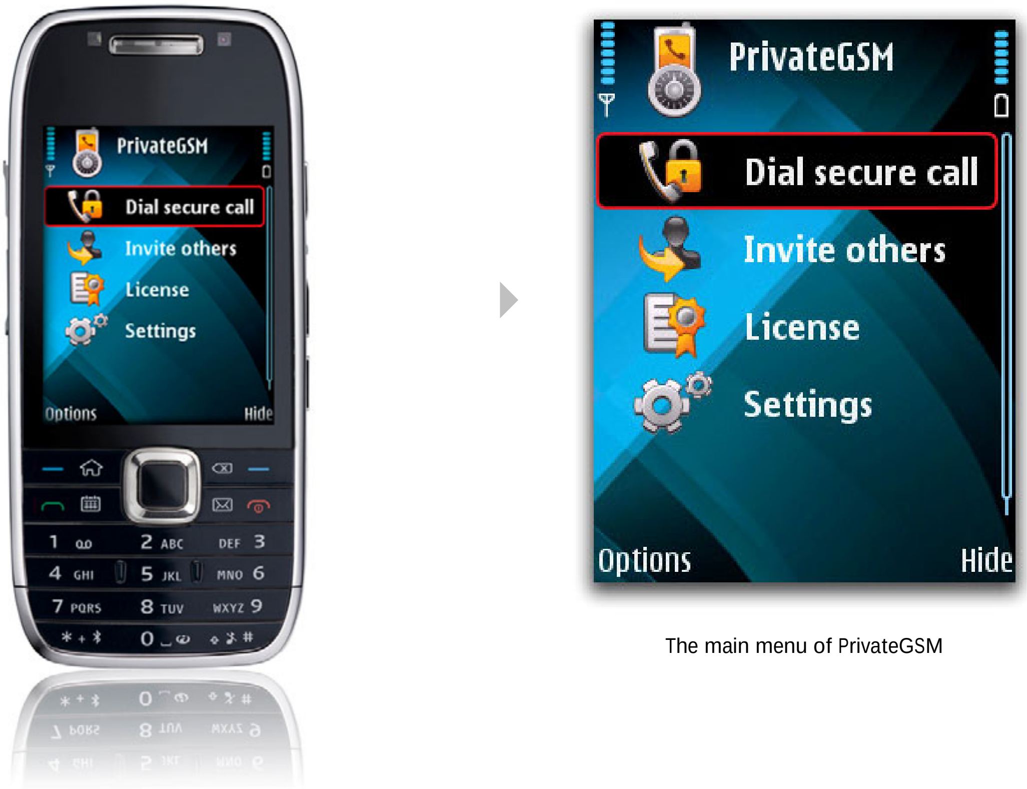
Privatewave

PrivateGSM CSD

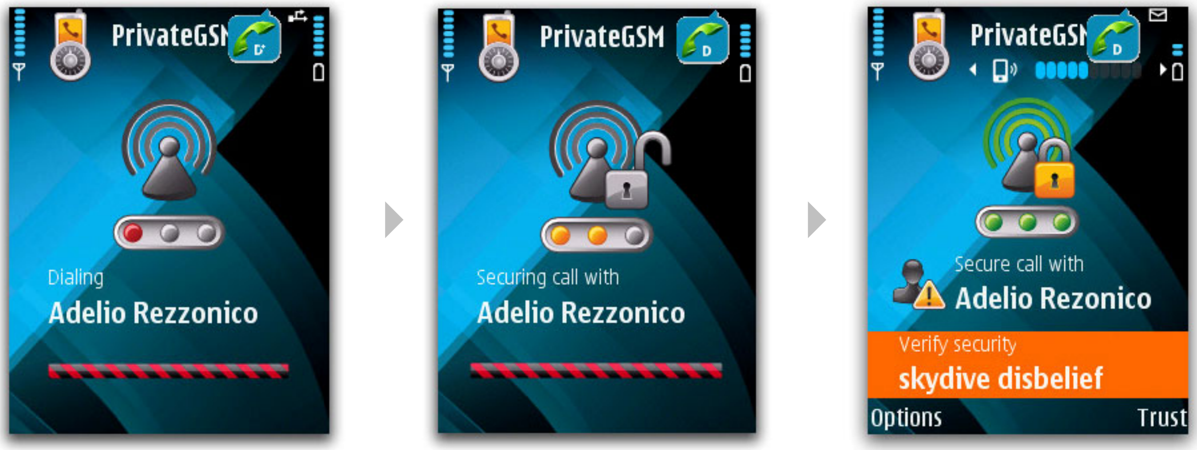
User manual

Index

1. The PrivateGSM software



The main menu of PrivateGSM



Secure phone call in action

2. Software installation

In order to install PrivateGSM it is necessary to run the software installer on a compatible telephone and follow the installation process.

Precondition: it is necessary to verify that the cellular telephone is compatible with the software. The phone models supported by PrivateGSM belong to the Nokia series S60 third edition.
A complete list of compatible cellular phones is available on the "**Support**" section of the website: **http://www.privatewave.com**

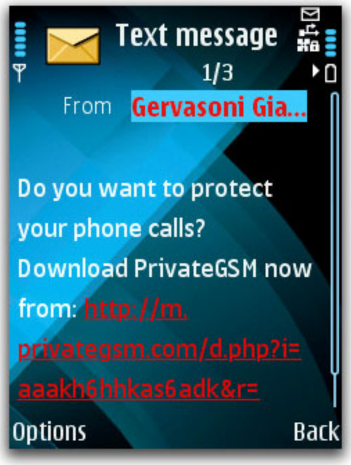
The simplest method of installing PrivateGSM is downloading it through the "**Products**" section of the website **http://www.privatewave.com**
It is sufficient to insert the proper personal data, the phone number and the model of the mobile phone on which you wish to use the software, and then click on the command "**Download PrivateGSM**".

SMS
SMS
3G
1/1
Options
Back

Do you want to protect your phone calls? Download PrivateGSM now from: http://www.privategsm.com/d.php?i=aaakh6hhkas6adk&r=hhb6bn6nddhkl

Software download

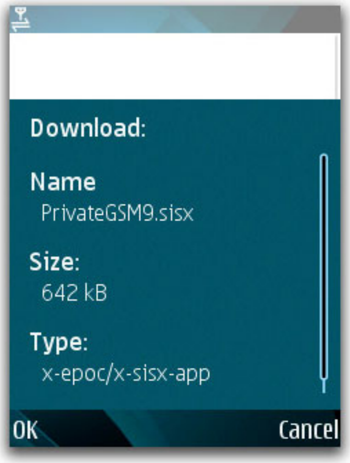
You will then receive an **installation SMS** from which you can download and install the software directly on your cellular phone, using the internet connection supplied by the phone operator:



Text message
1/3
From Gervasoni Gia...

Do you want to protect your phone calls? Download PrivateGSM now from: http://m.privategsm.com/d.php?i=aaakh6hhkas6adk&r=

1. Installation SMS



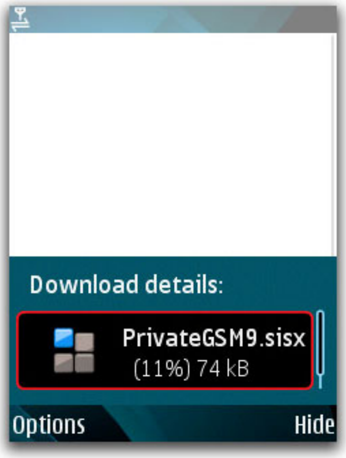
Download:

Name
PrivateGSM9.sisx

Size:
642 kB

Type:
x-epoc/x-sisx-app

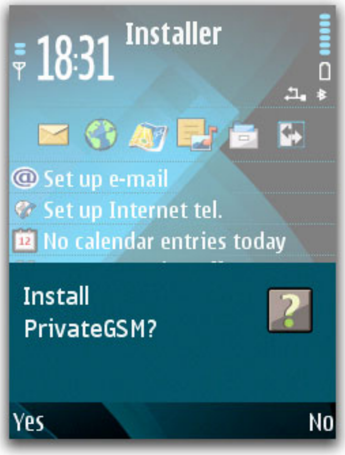
2. Confirm software download



Download details:

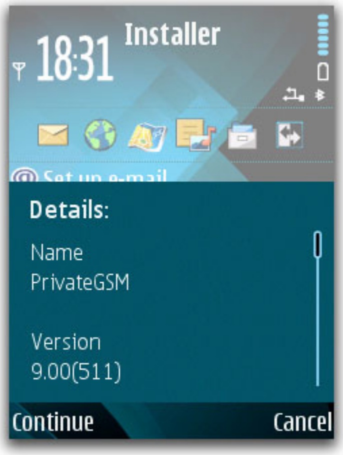
PrivateGSM9.sisx
(11%) 74 kB

3. Download in action with indication progress



Install PrivateGSM?

4. Confirm installation

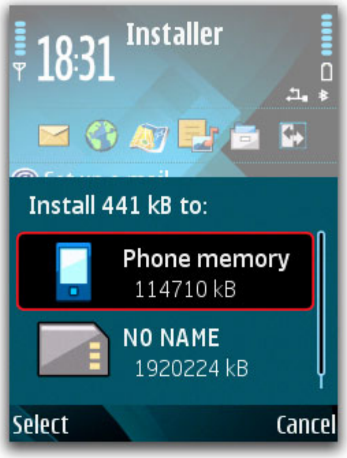


Details:

Name
PrivateGSM

Version
9.00(511)

5. Confirm software installation

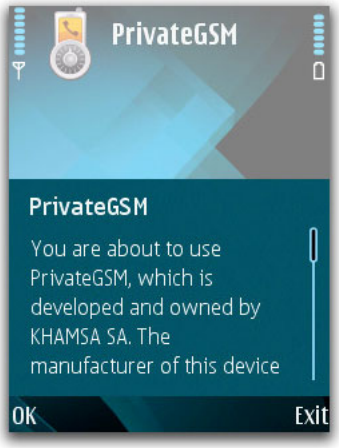


Install 441 kB to:

Phone memory
114710 kB

NO NAME
1920224 kB

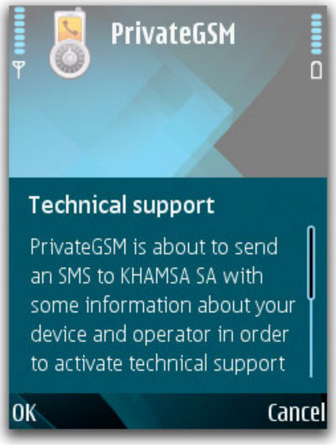
6. Choose the memory on which to install the software



PrivateGSM

You are about to use PrivateGSM, which is developed and owned by KHAMSA SA. The manufacturer of this device

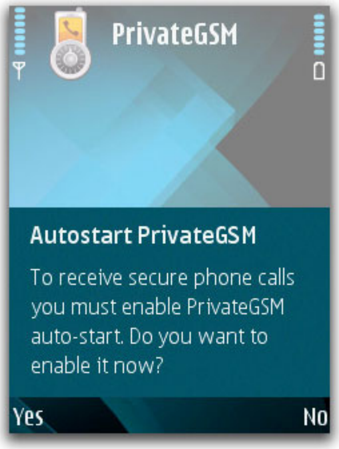
7. Accept licence agreement



Technical support

PrivateGSM is about to send an SMS to KHAMSA SA with some information about your device and operator in order to activate technical support

8. Activate technical support



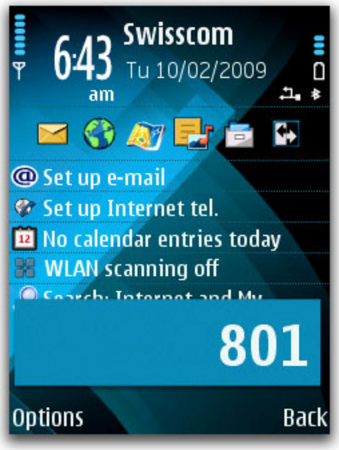
Autostart PrivateGSM

To receive secure phone calls you must enable PrivateGSM auto-start. Do you want to enable it now?

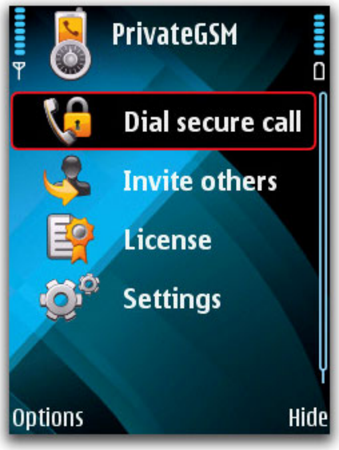
9. Restart the software

2.1 Start the software

Starting the PrivateGSM software is easy: it is sufficient to enter the number **801** as if you were starting a normal phone call. After pressing dial, the principle screen of the PrivateGSM menu will immediately appear.



1. Enter the number 801 and press the dial button



2. Principle screen of the PrivateGSM software

3. Activation of network services

PrivateGSM works on **GSM 2G** (850 / 900 / 1800 / 1900MHz) networks and requires a **data line CSD** (Circuit Switched Data).

3.1 Activation of data line CSD

PrivateGSM transmits the voice securely through a data type call, different from the traditional voice call which we are used to.

Because of this, the use of PrivateGSM requests the participants of the secure phone call to be in possession of a data line on their phone SIM card; that is the users' phone operator assigns an additional number to the original SIM card, exclusively dedicated to receiving **data CSD phone calls**.

Once the CSD data line has been activated by a phone operator, the functions of the phone will seem identical to those we are used to.

Consult the section "**Additional data number to receive secure phone calls**" for additional information.

!

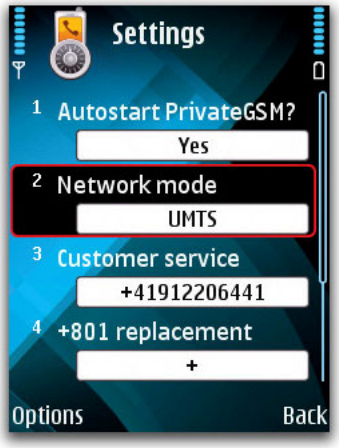
ATTENTION!
In absence of the necessary ability to make and receive data CSD calls, it may not be possible to make secure phone calls.

Consult the section "**Typical network problems for secure phone calls GSM CSD**" to resolve eventual connection problems.

3.2 Connect to the GSM network

In order to make a secure phone call correctly, the mobile phone needs to be connected to the **GSM** network (2G, second generation). The UMTS networks (3G, third generation) does not generally support data calls although it can work with some operators.

It is possible to change the network settings of the operator from the PrivateGSM settings menu, selecting GSM as **network mode**.



Settings

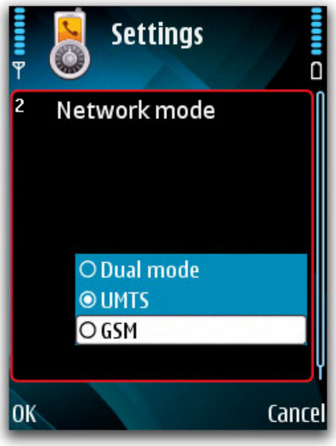
1 Autostart PrivateGSM?
Yes

2 Network mode
UMTS

3 Customer service
+41912206441

4 +801 replacement
+

1. After having entered "settings" from the principle menu, choose "network mode"

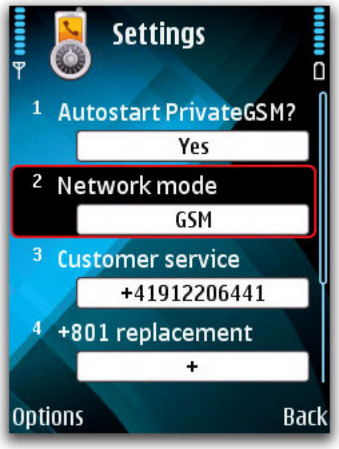


Settings

2 Network mode

○ Dual mode
● UMTS
○ GSM

2. Select the preferred network mode



Settings

1 Autostart PrivateGSM?
Yes

2 Network mode
GSM

3 Customer service
+41912206441

4 +801 replacement
+

3. The type of network has been modified

From PrivateGSM version 9.06, variations of network mode will be suggested automatically in the installation phase.

Please notice:
If you select a setting of network mode 2G, settings remain valid also for making normal phone calls without using PrivateGSM.

4. License mode: Full and Receive Only

PrivateGSM offers **two different user options**, depending on if you wish to have complete rights to both making and receiving secure phone calls (**Full**) or if you only need to be able to receive secure phone calls (**Receive Only**).

From the moment of installation, PrivateGSM will be in Full mode for **15 days**, without the need to insert any license.
After this period, which is useful for testing the software and arranging all settings, PrivateGSM will switch mode to **Receive Only** (for unlimited time until the user decides to uninstall PrivateGSM from the mobile phone). Inserting a valid **license code** permits the software to continue in Full mode and thereby making all software functions available (until the license expires).

In every secure communication network, it is sufficient to have only one cellular phone with PrivateGSM functioning in **Full** user mode. For the other users it is sufficient to have the **Receive Only** user mode.

To expand the network of persons with whom you wish to have secured conversations, you can easily use the Invite function – consult the section "**Inviting other users**".

To activate the PrivateGSM license consult the section "**Licences and activation codes**".

5. Secure phone calls with PrivateGSM

Making phone calls with PrivateGSM is very easy, but it is useful to be aware of the fundamental differences compared to traditional phone calls.

- **Time needed to begin a call**
  To begin a secure conversation, PrivateGSM needs between 15 and 45 seconds depending on the conditions of the available network. This limitation is dependent on the GSM CSD technology used by the mobile phone operator.

- **Delay of the voice**
  Secure phone calls have the characteristics of a voice delay of approximately **1 second**, similar to satellite communications. This characteristics depends on the transmitting technology GSM CSD used by the phone operator. In a secure conversation it is therefore useful to create some **small breaks** in the communication, allowing voices to be transmitted before continuing the conversation.

- **Dial tone**
  When calling another PrivateGSM user it will **not always be possible to hear the dial tone** (depending on the type of phone) which normally indicates that the other persons' phone is ringing. However, it will always be possible to follow the progress of the communication on the display of the phone.

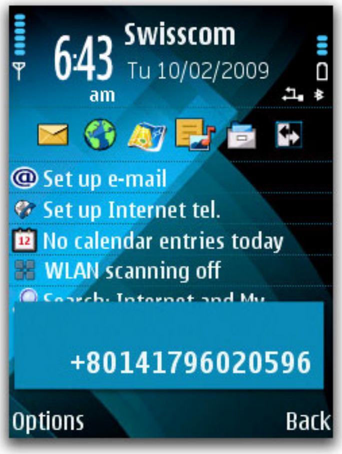
5.1 Making secure phone calls

To make a secure phone call with PrivateGSM it is sufficient to digit the secure prefix **+801** before the actual phone number, including the international prefix of the country you intend to call.

The called phone number **can either be inserted** at every new communication **or saved** in the phonebook including the secure prefix. For example, to call the phone number +39796020596 it is sufficient **to insert the prefix +801** followed by the number, transforming the dialed number to **+801**39796020596.

It is important that the dialed number includes both **the secure prefix** and **the country prefix** but **without including the initial 00** (e.g.: for Italy who has the country prefix 0039, a secure phone call should be initiated as +80139…. And not +8010039...).

To make a secure phone call using a number from the telephone phonebook, it works exactly like with a normal phone call. **Choose the contact** you want to call from your personal list and press **the green dial button**.



6:43 am Swisscom
Tu 10/02/2009

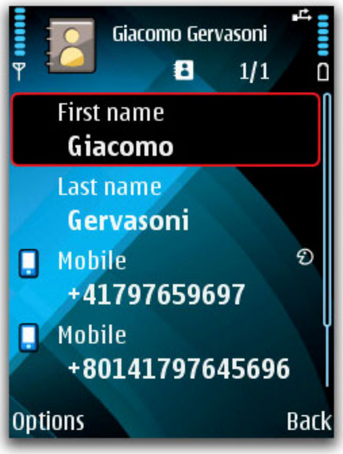
Set up e-mail
Set up Internet tel.
No calendar entries today
WLAN scanning off
Search: Internet and My

+80141796020596

Options Back

Call with the secure prefix +801

Secure prefix
+801



Giacomo Gervasoni
1/1

First name
Giacomo
Last name
Gervasoni
Mobile
+41797659697
Mobile
+80141797645696

Options Back

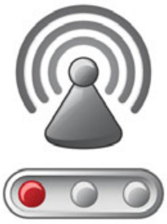
Save the number including the secure prefix in the phonebook

It is also possible to call directly from the principle menu of the application: select the section “**Other methods for calling**”.

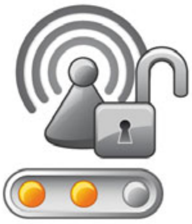
For some countries who does not accept the “+” in front of the prefix (e.g. Brazil) the secure prefix +801 **needs a configuration**: consult the section “**Particular user cases of the secure prefix**”.

5.2 Stabilizing the communication

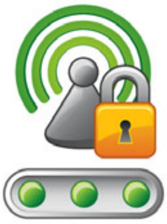
The connection of a secure phone call has **more phases** than that of a normal call. Every phase is shown on the display with three icons of different colors:



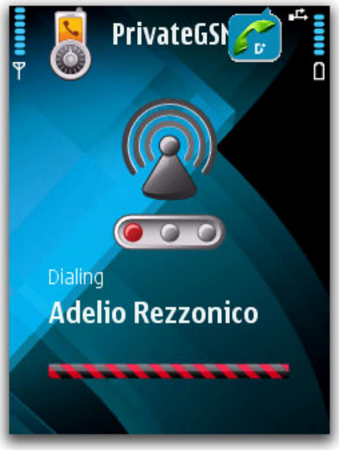
Red: the communication **is not yet stabilized**. This phase of the phone call can have a duration of 6 to 36 seconds.



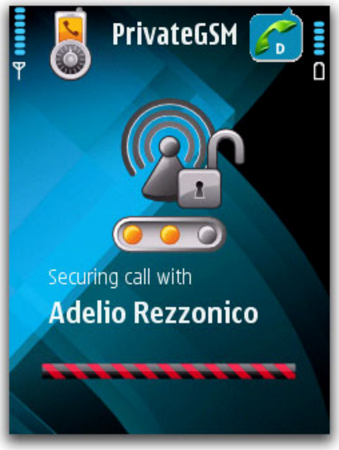
Yellow: the communication has been stabilized and **security is being established** with the ZRTP protocol. This phase lasts approximately 9 seconds.



Green: the communication has been stabilized and secured. **It is now possible to speak**.



1. Call in progress



2. Exchange of ZRTP keys in progress

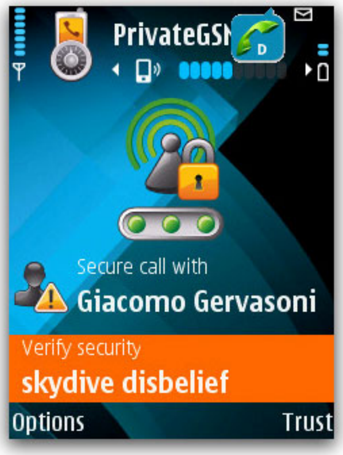
Following the phase of security key exchange, **it is possible to verify that the phone call is secure** and, once confirmed, you can begin your conversation.

5.3 Verify the security of the phone call

Once the phone call has been successfully established, it is necessary to **verify that the connection is secure**.

In order to verify the security of the phone call, PrivateGSM displays two “**secret words**” which are used as **security codes** between the conversation partners, identifying the security key of the on-going phone call.

To exclude the possibility of a third person intercepting the phone call, the two conversation partners **must verbally compare the two words**: if the words correspond, the phone call is secure and the conversation can begin without any risk.

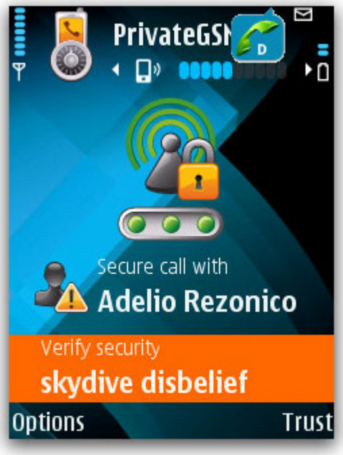


Secure call with
Giacomo Gervasoni

Verify security
skydive disbelief

Stabilized secure call

Security code which must be verified



Secure call with
Adelio Rezonico

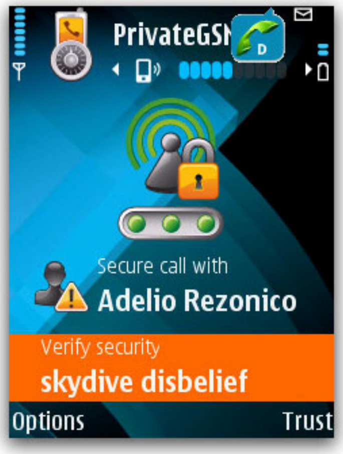
Verify security
skydive disbelief

Stabilized secure call

!

ATTENTION!
In case of the two words not corresponding, immediately interrupt the communication: this is evidence of an attempt to intercept your phone call and manipulation of either one of the phones or between the phone lines.

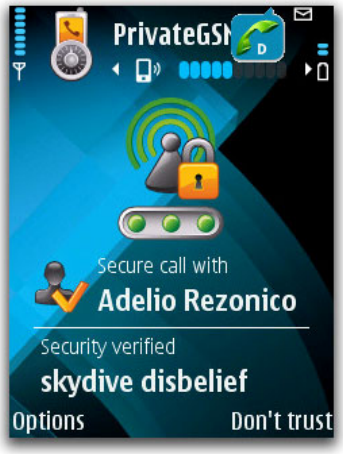
Once the correspondence of the security codes has been verified verbally, **from the PrivateGSM 9.06 version**, it is possible **to declare a contact as “trusted”** during a secure phone call. In this way it will not be necessary to verify the security of every phone call with the contacts you have already declared as trusted. Also the necessary time to stabilize the communication will decrease of some seconds.



Secure call with
Adelio Rezonico
Verify security
skydive disbelief

Trust not yet stabilized

Stabilizing trust by verifying correspondence of security codes



Secure call with
Adelio Rezonico
Security verified
skydive disbelief

Trust established

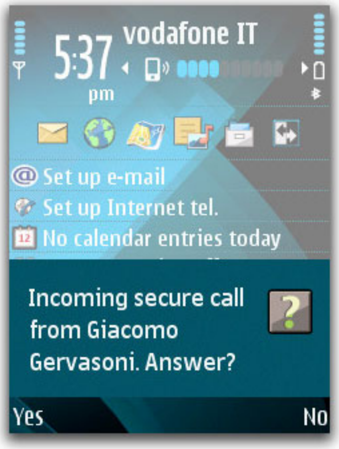
Information note

The two “**secret words**” are two english words generated from a well-known list like the **PGP Word List** which are distinguished by their phonetic diversity and defined as “**Short authentication string**”, a fundamental part of the encrypted vocal standard technology **ZRTP**. The Short Authentication String **changes at each new phone call**.

5.4 Responding to a secure phone call

When receiving a secure phone call, PrivateGSM displays an incoming secure phone call and proposes the **classic options of responding or refusing the call**.

Please note
The ringing tone of a secure call **is different** from that of a normal not-secure call, making it easy to distinguish between the two types.



Incoming secure call from Giacomo Gervasoni. Answer?

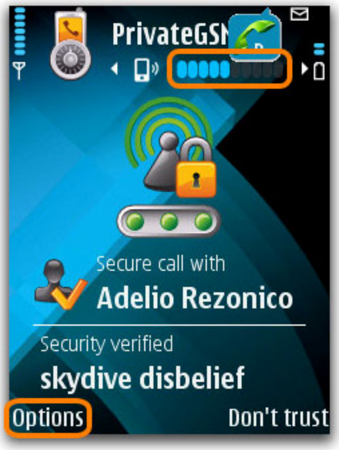
Receiving a secure phone call

5.5 Regulating the volume

During a secure phone call PrivateGSM permits the user to set and regulate all the **audio options** of the call, exactly like during a normal phone call.

To regulate the volume it is possible to use the proper buttons on the mobile phone (if available on the model) or you can use the central cursor of the phone **pushing to the left to reduce** the volume or **to the right to increase the volume**. A volume indication bar helps recognize the level of settings.

To activate or deactivate the loudspeaker of the phone it is sufficient to press the “**Options**” button followed by the “**Loudspeaker**” or “**Mute**” during the call.

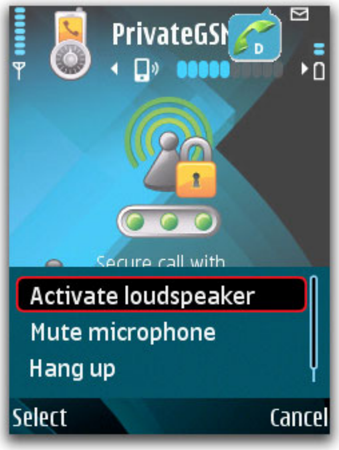


Secure call with
Adelio Rezonico

Security verified
skydive disbelief

Volume indicator

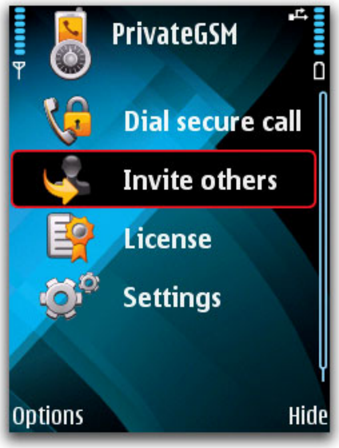
Activation
Mute/
Loudspeaker



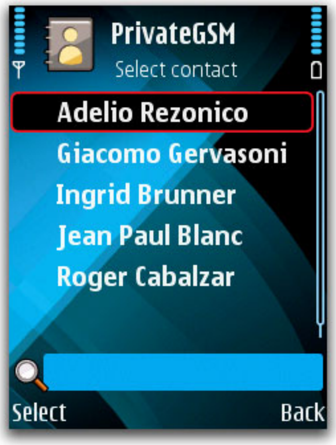
6. Inviting other users

It is possible **to invite other users** to use PrivateGSM directly from your cellular phone: simply enter the application menu, press **801** followed by the dial button, select “**Invite**”, and then choose the contact you wish to invite from the phonebook.

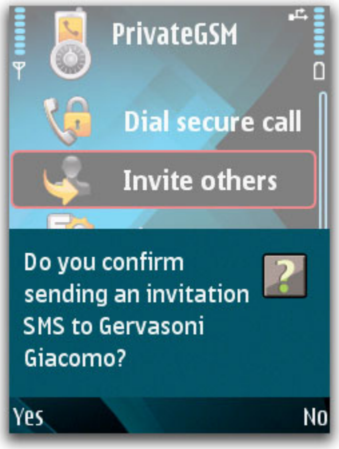
Then your contact will receive an **SMS with an installation link**.



1. Select “Invite”



2. Select a contact from your phonebook



Do you confirm sending an invitation SMS to Gervasoni Giacomo?

3. Confirm the sending of an invite to your contact

As an alternative, you can invite a user to run the installation directly from the website, following the directions of the section “**Installation of the software**”.

7. Additional data number to receive secure phone calls

To receive secure phone calls with PrivateGSM, especially with **communications between different phone operators** and in **Roaming** conditions, it is necessary to have an **additional phone number** dedicated to the reception of data calls on the same SIM card.

This is needed by the mobile phone operator to correctly generate transmissions from one cellular phone to another, avoiding potential frequent network errors.

All operators supply the additional data number, however often in different ways and with different conditions; to ease the interaction between user and phone operator, PrivateWave supplies a constantly up to date list of the **activation procedure** on the "**Support**" section of the website **http://www.privatewave.com**

! **ATTENTION!**
The phone operators, who assist clients with these issues, often confuse the "additional CSD data number" with the internet connection. PrivateGSM DOES NOT use internet connection.

We suggest explaining the phone operator that the issue is to receive faxes directly on the mobile phone and that you wish to have a number dedicated to receiving these faxes. Often this explanation helps the phone operator to better understand the request and identify the correct service to activate.

In rare cases mobile phone operators **do not provide** additional phone numbers on the same SIM card (multi-numbering scheme) for voice management, although the receiving of data and fax guarantee the availability of receiving CSD data calls (single numbering scheme). In these cases, network errors especially in Roaming and between different phone operators can be bigger: therefore we suggest finding **another phone operator** in order to make PrivateGSM function properly.

Please notice
The major part of phone operators only offer the additional data number to **SIM card subscriptions** and not to rechargeable SIM cards, dedicating this service mostly to business users.

8. Secure phone calls in movement

Use of PrivateGSM while moving, especially in **high speed cars or trains**, can cause a decrease of conversation quality like **increased delay** and **small interruptions**.

This is a result of the so-called **cell exchange** operation (handover) that occurs when you move between zones which are covered by different GSM cells.

During the **handover**, the transmission of the encrypted data will be interrupted - even though for only some milliseconds.

PrivateGSM has been tested with speeds up to 150km/h.

The possibility of losing signal quality depends on **the density of cells** on the road where you move in high speed. Generally, in city peripheral zones the GSM network is composed by **a reduced number of very powerful cells**, which leads to less operations of “cell exchange” (e.g. the highway). Opposite, in zones with a high population density the number of cells is bigger but each is less powerful, and therefore there will be a higher number of “cell exchanges” when in movement (e.g.: orbital roads and big city streets).

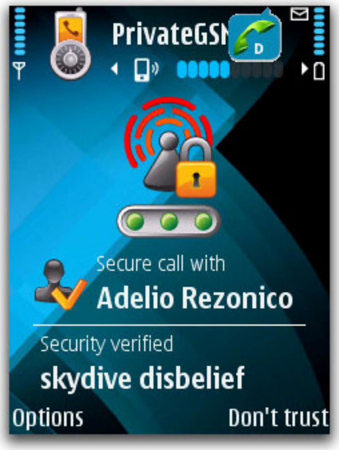
Please notice
In many countries use of mobile phones while driving is against the law. In these countries we suggest to use the loudspeaker of the mobile phone.

9. Control the quality of the phone call

In difficult network conditions of low signal, frequent change of network/cells, intercontinental communication and Roaming, the quality of the call can decrease with the effect of an **increased voice delay**.

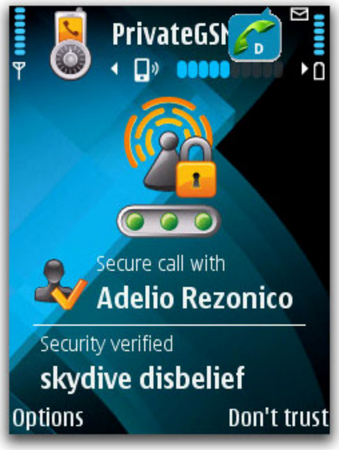
The increased voice delay is created by PrivateGSM in order to avoid holes and interruptions in the conversation, which could cause loss of information.

An eventual decrease of calling quality will be displayed on the mobile phone:



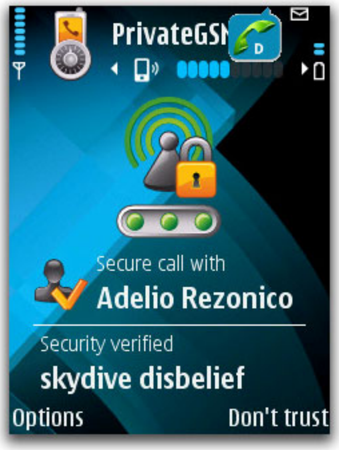
Secure call with
Adelio Rezonico
Security verified
skydive disbelief

Very bad connection



Secure call with
Adelio Rezonico
Security verified
skydive disbelief

Connection of medium quality



Secure call with
Adelio Rezonico
Security verified
skydive disbelief

Great connection

If the quality of the phone call is always bad, we advise you to consider **changing your SIM card operator or Roaming operator**.

Please notice

The function of increasing the voice delay in order to avoid interruptions in the conversation is available from PrivateGSM version 9.06.

10. Secure calls in Roaming

When using PrivateGSM in a foreign country in Roaming, you can encounter **network problems** due to the local mobile phone operators not properly managing GSM CSD data calls.

In particular, you can experience that a secure call **will not be stabilized** (the phone call does not start or arrive to the receiver like a normal GSM VOICE call and not as a CSD call), or that the data containing the encrypted voice **will not be transmitted** correctly (there will be no audio).

In these cases, provided that all other requirements are satisfied (CSD data line and 2G configuration of the mobile phone) there are two possible solutions to the problem:

1. **Change the Roaming operator**
   Some operators do not manage the CSD data calls correctly. Change the roaming operator from the menu of the mobile phone:

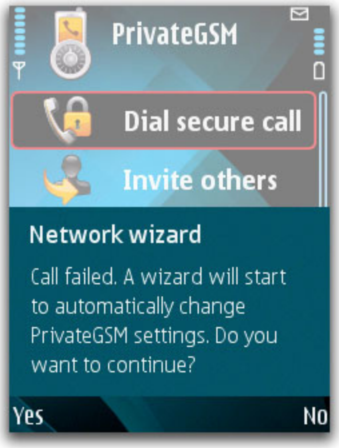
   Tools -> Settings -> Phone -> Network -> Operator selection

   Change operator and retry the call.

2. **Change calling mode**
   Some operators do not support the call mode CSD data digital V.110 and it is necessary to choose the call mode analog V.32 from the menu:

   Settings -> Advanced settings -> Outbound CSD settings -> Data Protocol

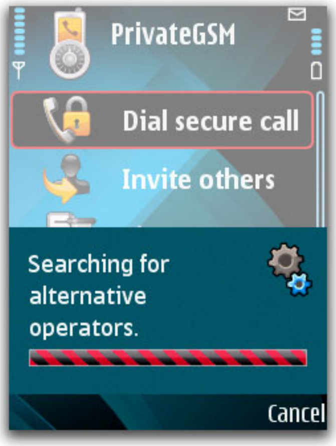
To make the use of PrivateGSM in Roaming easier, from version 9.06 of the software, there will be an **automatic function** available for these problems. When using PrivateGSM in Roaming, if a problem occurs with the communication, **PrivateGSM will automatically try all Roaming operators and all modes of CSD calls** in order to quickly and easily identify the best performing configuration for your specific context of use.



Network wizard

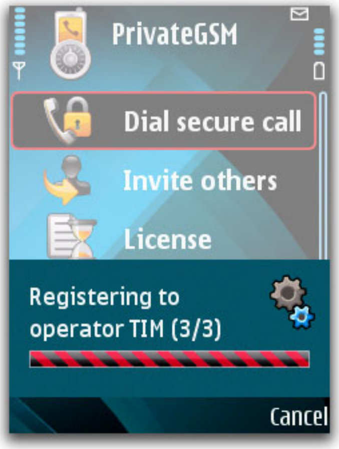
Call failed. A wizard will start to automatically change PrivateGSM settings. Do you want to continue?

1. Begin the process of Auto Roaming



Searching for alternative operators.

2. Searching for Roaming operators



Registering to operator TIM (3/3)

3. Process of connecting to a new operator

For further information and a better understanding of typical network problems that cause a decrease of communication quality for GSM CSD, please consult the section "**Typical network problems with secure GSM CSD data calls**".

11. Calling customer support

In case of necessary assistance related to the use of PrivateGSM it is possible to contact the customer support directly, by calling the number **+801801**. This way you come in contact with the **PrivateWave customer support**.

It is possible **to change the phone number of whom you wish to ask for assistance** from the menu:

Settings -> Customer Support

In case you wish to replace the PrivateWave customer support number with the number of your reseller or the technical assistance.

Please notice
Calling the phone number +801801 is a normal voice GSM communication and **not a secure call**.

12. License and Activation code

PrivateGSM has a very advanced user license management system based on **activation codes**, which, once inserted, gives the right to use the software for a temporary period of time defined by the code.

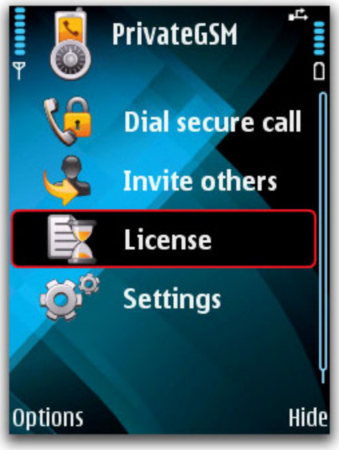
A PrivateGSM license represents the **right to use the software** which is not bound to one specific mobile phone or SIM card, therefore no details of the mobile phone need to be communicated.

However, **specific procedures** exist to manage changes of SIM cards and mobile phones while a user license is already activated on the device.

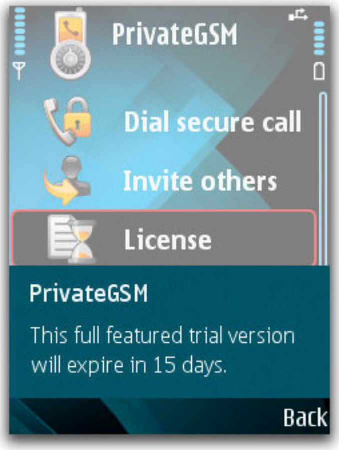
Please notice
When inserting the license code, the period of a Full license begins, thereby ending the trial period.

12.1 Verify the license

To check **the status of the PrivateGSM license,** it is sufficient to access the main screen of the software and click on “**License**”.



1. Select “License”

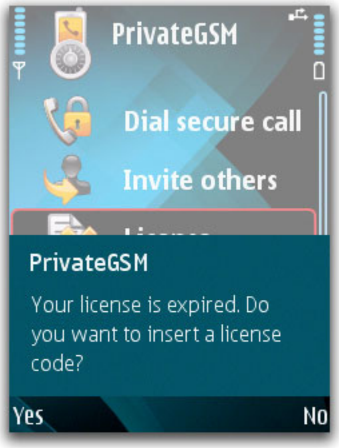


PrivateGSM
This full featured trial version will expire in 15 days.

2. View the status of the license

12.2 Inserting the activation code

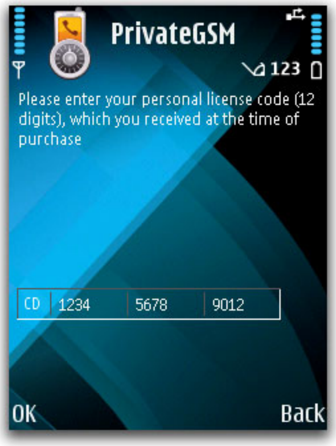
To activate a user license, it’s required to insert a code which will be verified and **authorized by SMS** from the server of the licensing partner of PrivateWave.



PrivateGSM

Your license is expired. Do you want to insert a license code?

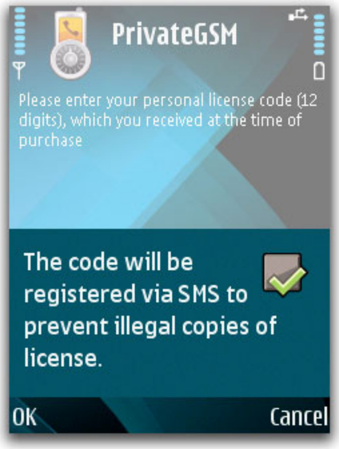
1. License expired: request to insert a license code



Please enter your personal license code (12 digits), which you received at the time of purchase

1234 5678 9012

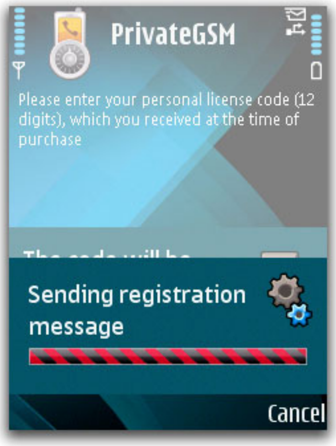
2. Inserting the license code



Please enter your personal license code (12 digits), which you received at the time of purchase

The code will be registered via SMS to prevent illegal copies of license.

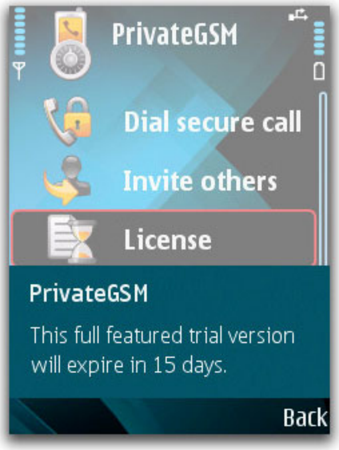
3. Authorization of license code via SMS



Please enter your personal license code (12 digits), which you received at the time of purchase

Sending registration message

4. Sending registration message



PrivateGSM

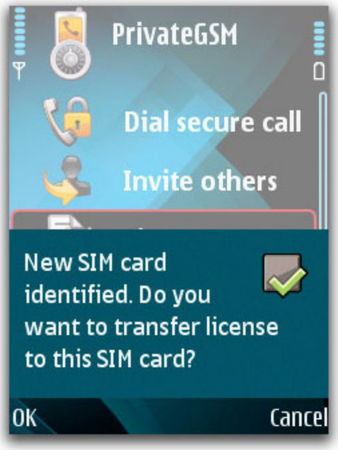
This full featured trial version will expire in 15 days.

5. License status after the activation process

Please notice
Activation of a license by SMS can take from a couple of seconds to a couple of minutes depending on network conditions.

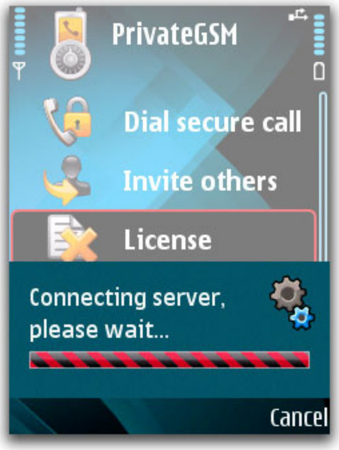
12.3 Change of SIM

In case of **SIM card change** on a phone which is already installed with a Full PrivateGSM license, the license will **automatically be transferred** to the new SIM card. PrivateGSM will notice the new SIM card and propose a **guided process** to verify and update the license.
The automatic guided process needs an **internet connection** (it is therefore necessary to have a valid internet access).



New SIM card identified. Do you want to transfer license to this SIM card?

1. Identification of a new SIM card



Connecting server, please wait...

2. Updating the license on the new SIM card

12.4 Change of phone

If you wish to change your phone but keep the same SIM card, once PrivateGSM is reinstalled (consult the section “**Installation of software**”), it will be sufficient to **reinsert the license code** supplied by the time of software acquisition.

The system will automatically be transferred to the new SIM card authorized by a valid license code, and the license will be inserted on the new mobile phone.

12.5 Change of SIM and phone

In the case of **simultaneously change of SIM card and telephone** (for example in case of loss or theft), it is necessary to **contact the customer support** in order to block the old license and renew it on a new telephone with a new SIM card.

Please notice

This type of service is considered **extraordinary assistance**. For this reason the user who asks for this service can be requested an eventual extra costs due to the management of the operation. However PrivateWave reserves the right to only perform this type of service a limited number of times for the same client during the period of subscription to PrivateGSM.

13. Typical network problems with secure GSM CSD (data) calls

With GSM and UMTS telephony, there exist different types of calls - **voice**, **data** (often referred to as FAX or CSD) and **Internet** (GPRS, EDGE, UMTS, HDSPA).

PrivateGSM uses the **GSM** as transmission technology; calls are therefore not the well-known “voice calls”, but “data calls” which permit direct exchange (and not intermediate) of data between two mobile phones.

Technically speaking you can compare data calls to making a phone call through a digital modem.

The technical definition of the used transmission of PrivateGSM is **CSD** (Circuit Switched Data), not transparent (Using RLP, Radio Link Protocol), asynchronous, at a speed of 9600bps.

It is NOT Internet, NOT IP, NOT GPRS, UMTS or EDGE and it has nothing to do with internet, however most mobile operators customer support confuse the request of a CSD data line with a request for an internet connection.

The GSM network manages data calls in another way than those of voice calls and there is no uniform way for mobile operators to manage the connection of data calls; for this reason user problems can occur.

PrivateGSM however has been noted to function in most of the Western World, Far- and Middle East and in South America in different GSM networks. However, it is always a good idea to verify the services supplied by local phone operators, especially in the activation phase when moving in countries in Roaming.

Use in Roaming can in fact provoke specific user problems which solutions can be found by following the instructions of this user manual.

There are two principle types of CSD calls:

- **v.32** - **Analog**
- **V.110** - **Digital**

The default mode of PrivateGSM is **V.110 digital**, which needs approximately **10-15 seconds** to stabilize a call and further is **the most supported in the Western Countries**.

However, in some countries (generally in Roaming) to make a secure phone call it can be necessary to change the mode to **V.32 analog**, which by the telephone network will be treated as an analog modem needing approximately **30-35 seconds** to stabilize a phone call (please consult the section “**Secure phone calls**”).

13.1 The number called receives a mechanical voice and hear a sound similar to a fax

Problem
The caller never reaches the phase of “key exchange” and the called receives a normal voice call to which responses are similar to the noise from a fax.

- **Diagnostic 1**
  In these cases it is very probable that the called phone does not have a dedicated CSD data line or the caller has not used the data number to make the secure call.

  Solution
  - Verify that the two phones (caller and called) are in GSM network mode;
  - Verify that on the called number there is an activated CSD data line;
  - Verify that the number called is actually the data number and not the normal voice number.

- **Diagnostic 2**
  The caller or the called is in Roaming near an operator who does not properly manage CSD data line calls.

  Solution
  Follow the instructions in the section “**Secure phone calls in Roaming**”.

13.2 The call does not start but is ended with error “Impossible to stabilize the call”

Problem
It is not possible to start a call due to an immediate interruption with the error: “**Impossible to stabilize the call**”.

- **Diagnostic 1**
  In these cases the problem can be due to the device configuration or an operator issue both for the caller and the called.

  Solution
  - Verify that the two phones (caller and called) are in GSM network mode;
  - Verify that on the called number there is an activated CSD data line;
  - Verify that the callers SIM card is allowing outgoing CSD traffic (rare case);
  - Try to move to an area with less phone density, the network can be overfilled;
  - Verify that the number called is actually the data number and not the normal voice number.

- **Diagnostic 2**
  The caller or the called is in Roaming near an operator who does not properly manage CSD data line calls.

  Solution
  Follow the instructions in the section “**Secure phone calls in Roaming**”.

13.3 The call falls through after 30/60 seconds ending with “Exchange of keys”

It can happen that a secure call does not begin even though it was able to establish the CSD data call. PrivateGSM will then stay in the phase “Exchange of keys” for 30 seconds after which the call will be interrupted by the software.

This type of problem can happen when one of the two parties is in Roaming and the Roaming operator does not support CSD calls correctly. The technical problem depends on the phone operator to whom you are connected, even though data calls arrive at the destination, the transmitted data is not being transmitted correctly from one dispositive to the other

.

In these cases you can try to **manually change the Roaming operator** and the mode of call from V.110 digital to V.32 analog (please consult the section “**Secure calls in Roaming**”).
The guided process of resolving Roaming problems unfortunately does not cover this particular disfunction caused by the GSM network.

13.4 Only the caller or the receiver of the call can hear a voice

It can happen that after a secure call has been connected, the encrypted voice data begin to flow in only one direction, therefore **making only one part of the conversation able to hear the voice**.

This type of problem can happen when one of the two conversation partners are in Roaming or one of the Roaming operators does not support CSD calls correctly.

In these cases you can try to **manually change the Roaming operator** and the mode of call from V.110 digital to V.32 analog (view the section “**Secure calls in Roaming**”)

The guided process of resolving Roaming problems unfortunately does not cover this particular disfunction caused by the GSM network.

14. Particular user cases of the secure prefix (Brazil)

To make an international call it is always necessary to compose the number with the country prefix, e.g.: "+ 39 347 0123456". The structure of the number is composed as follows:

- "+": **country exit prefix**
- "39": **country prefix** (e.g.: Italy)
- "347": **area code**
- "0123456": **number**

The major part of countries use "00" as the exit prefix, but it is not a general rule: in North America, for example, you use "011" as the exit prefix. Other countries has prefixes even more different. A list can be viewed on **http://en.wikipedia.org/wiki/List_of_international_call_prefixes**

In order to avoid confusion, the use of "+" instead of the exit prefix has been spread around the world for years. This helps remembering the International format of contact numbers and you can without difficulties call from both France and the United States without having to manually change the exit prefix from "00" to "011". While most parts of the world support numbers with a prefix of "+" at the moment Brazil does not.

The secure prefix "+801" is not a real country prefix but a prefix exclusively used by PrivateGSM. When the software calls the number "+801 39 347 0123456", instead of making a voice call to the number +801 39 347 0123456, it makes a secure call to the number +39 347 0123456. As seen by this example, the prefix "+801" substitutes the prefix "+".
The Brazilian network does not allow calls with "+" but only with the old country exit prefix. Therefore in Brazil it is necessary also to specify **the selection code** of the operator that you wish to use to make the call.

!

WARNING!
When you are in Brazil it's requied to modify the PrivateGSM settings in order to substitute "+801" with "00xx", where "00" is the old numeric prefix and "xx" is the prefix of the operator used to route long distance calls. It will not be requied to modify the numbers already saved in your phonebook. and you can continue using +801 prefix.

To change the configuration select:

Settings -> +801 replacement.

15. Other methods for calling

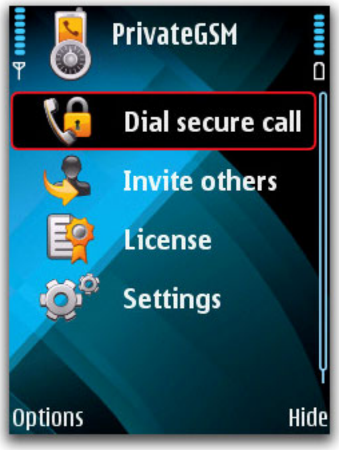
It is possible to make secure calls in other ways than those shown in the previous pages.

15.1 Selecting a contact from the application

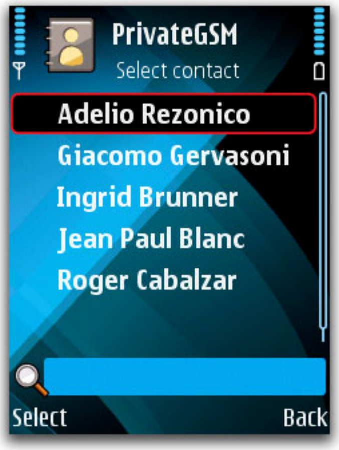
It is possible to make secure calls from the main menu of the software, selecting a **contact** from the phonebook.

Pressing the selection “**Secure call**” opens the **phonebook** and it is immediately possible to make a secure phone call.

Please notice
Using this method will not leave any indication of a secure call being made in your phone register.



1. Main menu

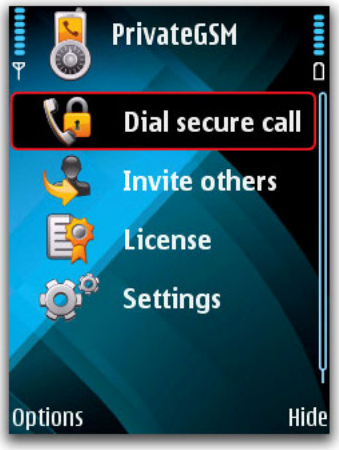


2. Telephone book

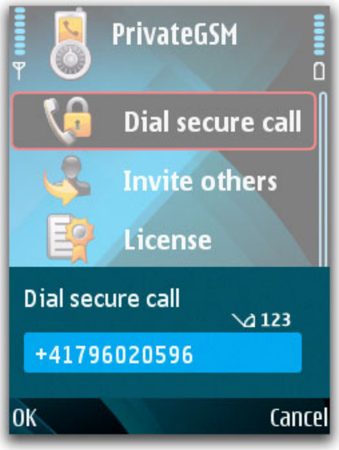
15.2 Dialing a number from the application

It is possible to make a secure phone call **from the software**, inserting the phone number you wish to call directly (after having entered into the main menu).

Please notice
Using this method will not leave any indication of a secure call being made in your phone logs.



1. Main menu



Dial secure call
+41796020596

2. Inserting the phone number

16. Other methods of installation

Besides the OTA methods (over the air) through SMS and internet, it is possible to install PrivateGSM through a computer connected by cable or by Bluetooth.

16.1 Installation from a computer via Bluetooth (PC)

In order to install PrivateGSM via Bluetooth, it’s required to download **the installation file** on the computer from the “**Products**” section of the website **http://www.privatewave.com** and then send it to the phone using Bluetooth.

The phone will display PrivateGSM as a message **in the message inbox list**. By opening the message you begin installation.

16.2 Installation from a computer via cable connection USB (PC)

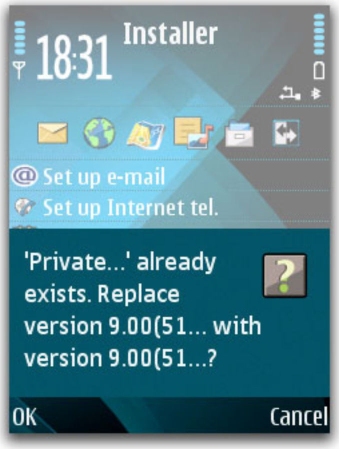
In order to install PrivateGSM via a USB cable, it’s required to download the installation file from the “**Products**” section of the website **http://www.privatewave.com** and then proceed simply by clicking on **the installation file**.

You must ensure to have a version of the **Nokia PC Suite** software compatible with your phone and be sure that the phone and the computer are properly connected with the cable.

17. Software updates

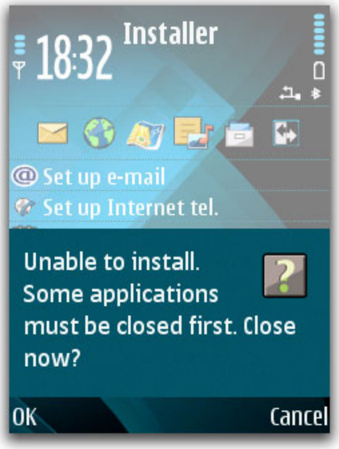
To update the Private GSM software it's required to follow the installation process.

The only supplementary step consists of the request **to replace an already existing version** of the application, followed by **closing the running PrivateGSM application**. It's required to **confirm** both requests



'Private...' already exists. Replace version 9.00(51... with version 9.00(51...?

1. Confirm the updates and substitute the software



Unable to install. Some applications must be closed first. Close now?

2. Confirm termination of running applications

18. Notes on secure phone calls

PrivateGSM guarantees complete security of your communications: proper use of the software makes it mathematically impossible to intercept and understand the content of a secure phone call.

Following are some important security notes about proper use of secure phone calls.

18.1 If someone intercepts a secure phone call

If someone intercepts a secure phone call protected by PrivateGSM they will come into possession of **two digital files** representative of the data flow exchanged during the communication, **protected with ZRTP, ECDH key exchange** and encrypted with **AES256**.

These files are impossible to decipher not even with high technological decipher mechanisms as those used by the top secret services of the western countries, and, considering the technological evolution of today, they are evaluated to remain protected for many tens of years into the future.

18.2 If someone steals an encrypted phone

If someone intercepts the communications which are protected by PrivateGSM and eventually comes into possession of the phones from which the communication has been made, **the content of the phone calls will however remain intact**.

In fact, in contrary to many encryption technologies, PrivateGSM supplies the encryption feature called **PFS (Perfect Forward Secrecy)**.

Thanks to the feature of PFS from the encryption technology ZRTP, it is in fact **impossible to decode** eventually intercepted phone calls, **even if the interceptor later comes in possession of the two devices** on which the communication has been made.

Even if the encryption keys are stolen there’s no chance for an attacker to recover phone calls contents by intercepting it.

18.3 If someone carries on an attack on the encryption technology ZRTP (Man in the middle)

If someone carries on a very sophisticated attack on the ZRTP encryption, the **SAS** (short authentication string), **the two secret words** described earlier, will show **different words** on the phone of the caller and the called.

For this reason **it is important to verify that the two words on the display of the phones are the same** for both conversation partners.

18.4 If a cell phone is lost and later found again

In case the phone on which you have done encrypted phone calls had been lost and later refound, it is better to do a complete reinitialisation before continuing to use the PrivateGSM software.

PrivateGSM has to be considered secure on the phone on which is installed on as long as it is **always in control and possession of the proper user.**

Even temporary possession of the mobile phone by an intelligence agency (or other third party) may no longer guarantee you secure calls, because of the fact that a backdoor, a digital spyware or other attack tools can be installed on your mobile phone, thus have an external access to your calls.

If your risk context includes opponents as intelligence agencies or military organization, we suggest you to always carry your PrivateGSM phone with you, even to the toilet, and close to the bed when you sleep and never to leave the phone unattended in a hotel room or an office.

In the case of the phone being unattended for several hours or rather lost and later found again, before using it, it is necessary to do a **complete reinitialize** (format) and **reinstallation** of PrivateGSM by downloading from a trusted source.

18.5 What is not protected by PrivateGSM

PrivateGSM protects cellular phone communication when properly used according to your particular context of risk.

It is important to know that PrivateGSM obviously does not protect against environmental interception such as microspy placed in your house, office or car.

In the same way PrivateGSM does not protect from environmental interception such as long distance microphones and microphone lasers.

PrivateGSM does not protect from geographical tracking devices based on GPS devices or geographical localization from SIM GSM.

Always make reference to a security expert to receive proper measures of protection from wiretapping attacks based on the above mentioned environmental interception devices.

19. Note on PrivateGSM compatibility with other telephone softwares

PrivateGSM integrates technological elements as the **Nokia Audio Proxy Server** (APS) and the **VoIP Audio Services** (VAS) which, if already installed from other applications (for example Fring), can make PrivateGSM not function in a correct way.

In this case it is a good idea to uninstall the application associated with the version of Nokia APS or VAS in conflict and reinstall PrivateGSM.

20. Note on the costs of secure calls

Generally the cost of a data call **is the same of a normal phone call**. However the cost of a call made on a CSD line can vary from operator to operator.

We suggest verifying the cost rates with your phone operator before activating/verifying the data and FAX line.

Contacts

For any need you can consult our website:

http://www.privatewave.com

To contact our technical staff:

Tel: **+39 02 911 930 891**
E-mail: **support@privatewave.com**

Office hours: Monday to Friday, from 10 am to 12 am and from 2.30 pm to 4.30 pm (GMT +1)

To give us your opinion or suggestion:

Tel: **+39 02 911 930 890**
E-mail: **customercare@privatewave.com**

Office hours: Monday to Friday, from 9.30 am to 12.30 pm and from 2.30 pm to 5.30 pm

PrivateWave Italia SpA
via Sansovino 13/A - 20133 Milano - Italy

www.privatewave.com