What you should know before using PrivateGSM

Interactions with standard GSM voice calls

If you receive a standard voice call during a secure call (VoIP), you may:

1. **Accept the voice call**: since this channel takes priority over VoIP, the secure call will be automatically hung up.
2. **Refuse the voice call**: the VoIP call remains connected and you can continue the secure conversation.

Limits of protection provided by PrivateGSM

PrivateGSM can not protect your conversations against eavesdropping in your local physical environmental, for example:

1. Eavesdropping by surveillance bugs placed in your home, in the office or in your car.
2. Eavesdropping by long distance directional microphones or laser microphones.

PrivateGSM cannot protect your location information from the following location tracking systems:

1. GSM mobile phone locators
2. GPS locators

We suggest you to consult a security expert to protect yourself against these type of threats.

Call quality on the move

It may take longer time to establish a connection or you may experience short interruptions in the audio when traveling by car or high speed train. This is because you are switching from one GSM network radio cell to another. Call quality depends on the local infrastructure of the mobile operator.

For example while driving on a highway in the countryside the GSM network is usually made up of less cells with higher coverage so switching from one cell to another is less frequent. Contrarily, in the center of metropolitan areas the GSM network is made up of more cells with lower coverage: switching from one cell to another is more frequent (for example on expressways and ring roads).

Note

No perceivable audio problems of a PrivateGSM secure call were demonstrated in tests conducted driving on a highways at 150 km/h.

Network type and call quality

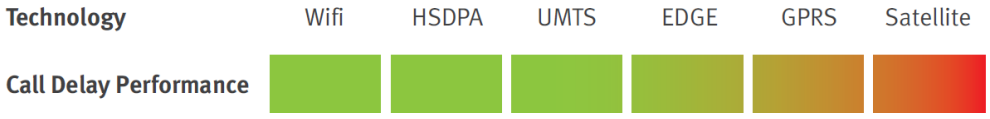
Secure calls with PrivateGSM use VoIP technology that utilizes an Internet connection establish the audio flow via TCP/IP and UDP packets. The data packets containing the voice in encoded and encrypted form are routed on the network during a call.

PrivateGSM secure calls require an open Internet connection without any firewall or other restriction by the caller or called party.

Mobile phone operators typically offer two type of Internet access with two different Access Points:

- **Full Internet access**: supports all transmission protocols and *required by PrivateGSM*
- **WAP/MMS access**: *not appropriate* for PrivateGSM.

The following figure demonstrates different network types, ordered by quality and bandwidth. Bandwidth determines the amount of data transmitted per second. Latency determines the time required for the data to reach its destination.**:**



To check your mobile phone network, check the symbol next to the signal bar:



figure 1. EDGE network

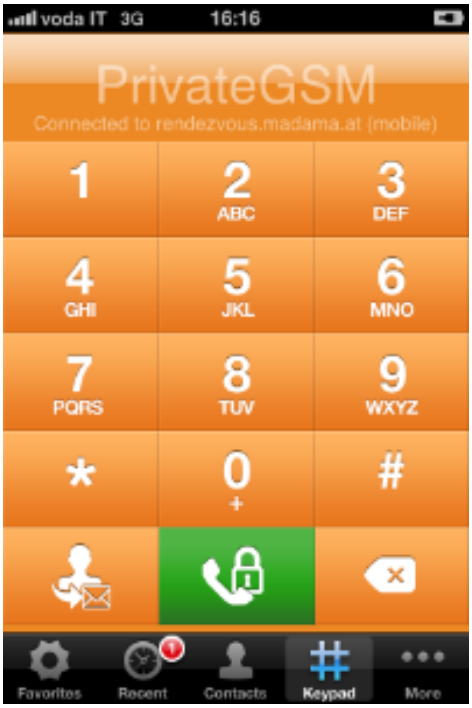


figure 2. 3G network

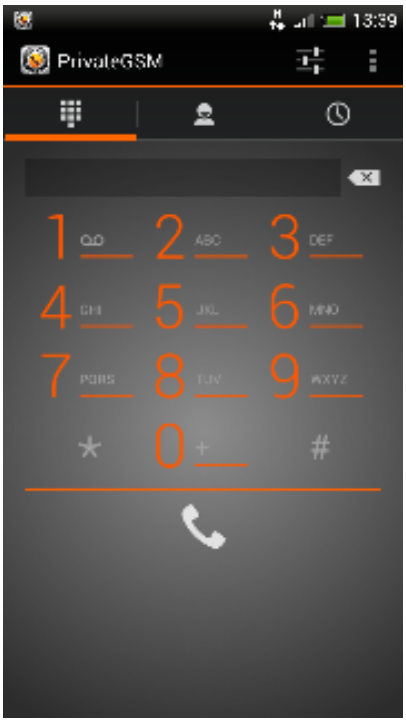


figure 3. 3.5 G network (HSDPA)

Use Wi-Fi when available. There are no additional costs and call quality will be definitely better.

Data plan rates

PrivateGSM secure calls use an Internet connection and data traffic will be charged by your mobile service provider. The exact costs depend on the contract with your mobile service provider. To receive secure calls, PrivateGSM has to keep an Internet connection open. You should therefore choose a rate that lets you **stay online as long as you need** to receive and make secure calls (i.e.: 24/7, or business hours).

We suggest you consult your operator to set a flat rate tied to your connection needs.

Note

When using PrivateGSM abroad, be sure to have a data traffic plan that allows you to control your costs.

Disadvantages of a limited traffic plan

Traffic plan limited in data	When PrivateGSM is running but no secure call is active, it still keeps alive a connection to the server. On average, PrivateGSM uses a total of 2MB per month even when you do not call securely. A secure call uses data traffic between 100kbyte and 200kbyte per minute. So 1MB of Internet traffic is enough for a minimum of 5 to a maximum of 10 minutes of secure conversation.
Traffic plan limited in time	As PrivateGSM has to maintain a continuous connection to the server and these type of data plans are billed based on the connection time, these plans can create unaffordable costs and they are not recommended for PrivateGSM.

Differences between secure and standard calls

Delays in establishing a connection	To establish a connection with the called party, PrivateGSM needs from 5 to 60 seconds based on the Internet connection quality of the caller and called parties.

Audio delay	Unlike standard calls VoIP secure calls may be subject to an audio delays from 1/5 of a second to a maximum of two seconds. This depends on the underlying technology of the data transmission network. The better the connection, the smaller will be the audio delay.
Different ringing tone	PrivateGSM secure calls use different ringing tone than standard calls (not customizable).
Battery life	Internet connection may lower the battery life of the mobile device. Average battery consumption may increase from a minimum of 5% to a maximum of 35% based on the type of network used by the Internet connection. **Note** A Wi-Fi network consumes more than a 3G network. A 3G network consumes more than a 2G network.

Other functions and settings

User license and license code