

Sending and receiving Secure Messages

What is a "Secure Message"?

A Secure Message is a Short Text Message that can be sent and received securely using PrivateGSM. Secure Messages share the same communication infrastructure provided used for secure voice. EVSS do not relay at all on Apple Push Notification or Google Cloud Messaging, in order to protect users' security:

- Server Authentication by SSL certificate.
- HTTPS and SIP over TLS protocols to exchange data in encrypted way.

Secure Messages are text only, thus no attachments are provided. Maximum length of a Secure Message is 160 characters.

How does Secure Messages work?

When a user chooses to send a Secure Message, it triggers an HTTPS POST request in his client towards PrivateServer which plays a "store-and-forward" role. If recipient is online, Secure Message is immediately delivered. Otherwise it is stored temporarily in PrivateServer up to 3 days before expiring: as soon as the recipient pops up online, PrivateServer delivers the Secure Message.



Security model provided is end-to-site: message are protected during transport from wiretapping by TLS. Local temporary storage is encrypted with server key.

Delivery is performed by SIP over TLS protocol, so as you can see the whole end-to-end path is encrypted and the message is stored after a local encryption on the server.

Send Secure Messages

It's possible to write Secure Messages to other parties both **by answering** them or **by writing for your own initiative**. In the first case you would probably **use the Contact's History view**, in the latter you would **use the Contact's details view** instead.



Since the "History" lists all the communication attempted or happened on your PrivateGSM, it's possible to start a conversation using "History" as well, eg: answering to a missed call by a Secure Message or just using one event conveniently.

Sending Secure Messages from "History" view

As you can see in [History](#) when you look at the screenshots presented as "Example of contact's history event" at the bottom of the Contact's History view, there's a text field you can use to type a new message, like the ones shown below:

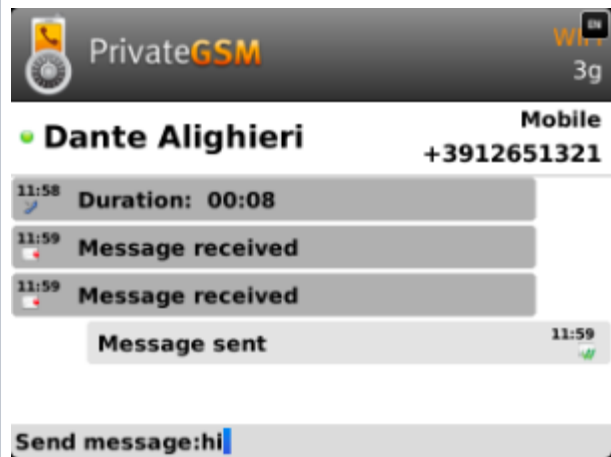


figure 1. BlackBerry



figure 2. iPhone

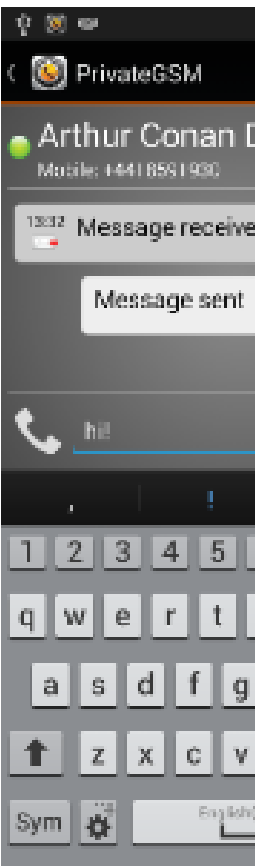




figure 3. Android

Please note that by convention, your outgoing communications are placed on the right side of the screen, while the incoming ones by the chosen contact are placed on the left of the screen.



 Unknown Attachment figure 4. send button (iPhone)	iPhone
 figure 5. send button (Android)	Android

You can send your new message pressing the proper "Send" button in the User interface if you're on Android or iPhone, else on BlackBerry you just use the "Enter" key in your keyboard.

Sending Secure Messages from "Contact's Detail"


As stated before, Secure Messages are also available from "Contacts" view which is probably the best way to start a conversation via text messages. Obviously first thing it to reach the contact you want to write to. Please refer to [Performing a secure call with PrivateGSM](#).

Central button on BlackBerry keyboard	"info" icon in iPhone	"info" icon in Android
---------------------------------------	-----------------------	------------------------

<p>? Unknown Attachment</p> <p>figure 6.</p>	 <p>figure 7.</p>	 <p>figure 8.</p>
---	--	--

Once you reached the specific number of your peer contact, then you can open his contact's history by pressing the "info" icon in Android and iPhone or just pressing the central button on the keyboard in BlackBerry (please check [figure 6.](#), [figure 7.](#) and [figure 8.](#)).


You'll get exactly the same view shown in [History](#) (detailed event view).

 Please note that by convention your outgoing communications are placed on the right side of the screen, while the incoming ones by the chosen contact are placed on the left of the screen.

So you can now type your message, just as in [figure 1. BlackBerry](#), [figure 2. iPhone](#) and [figure 3. Android](#).




Receive Secure Messages

Obviously Secure Messages can be received. When this is the case, then one specific notification is raised by PrivateGSM using system's notifications.

iPhone locked	PrivateGSM in background	Once you open the application
new Secure Message notification is shown	PrivateGSM shows an event notification on its icon	"Recent" icon shows how many events occurred. Clicking on "Recent" shows "History" list with event item in bold.
<p>? Unknown Attachment</p>		<p>? Unknown Attachment</p>

BlackBerry locked	Click on system's notification area	Click on PrivateGSM item
Sound and vibration notify a new event. Once unlocked "new message" icon is shown in notification area	When you drop down the event list, PrivateGSM item shows the "new message" icon and you can click on it.	You got redirected directly to "History" view where "Message received" event is bolded.
<p>? Unknown Attachment</p>	<p>? Unknown Attachment</p>	<p>? Unknown Attachment</p>

Android locked	Click on system's notification area	Click on PrivateGSM item
----------------	-------------------------------------	--------------------------

<p>Sound and vibration notify a new event. If you had a model equipped with coloured led, then it would lit.</p> <p>Once unlocked, "new message" icon is shown in notification area</p>	<p>When you drop down the event list, PrivateGSM item shows the "new message" icon and some details about the sender.</p>	<p>Once you clicked on PrivateGSM item in event list, you got redirected directly to "History" view where the "received message" event is bolded.</p>
 Unknown Attachment	 Unknown Attachment	 Unknown Attachment



If just one message has been received, then clicking on the notification would lead you directly to the event detail where you'll be able to read the message.

As shown above each platform shows the event notification differently, according to the underlying operating system behaviour.

Secure Messages compared to SMSs

Secure Messages provide a user experience very similar to SMS, adding security and with some minor differences. Some current constraints will be relaxed in next versions.

Secure Messages look just like clear text messages but they are not. Instead they are a sophisticated way for writing each other and their complex architecture implies some **bounds**:

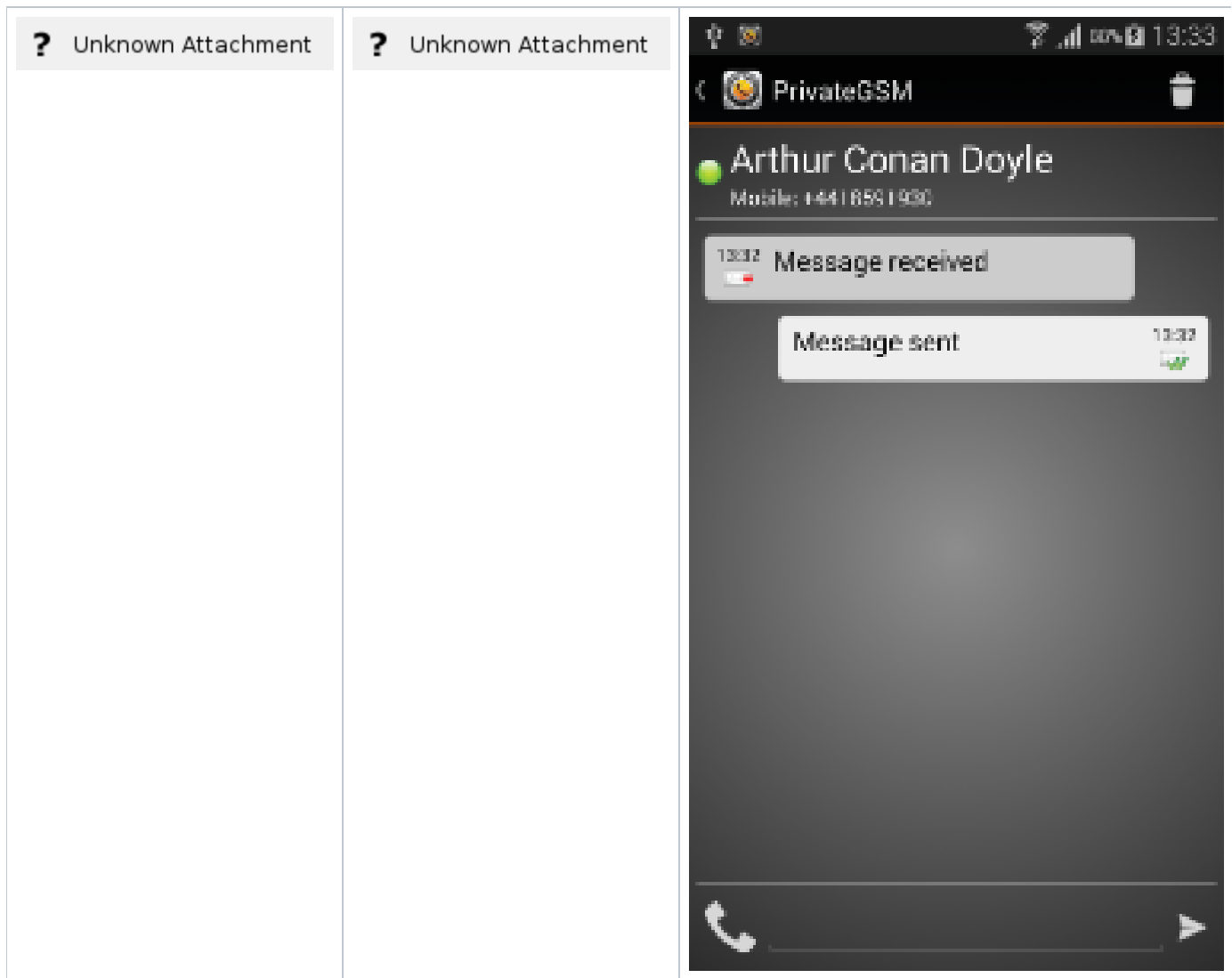
- There's **no chat group** / **no chat room** feature: you can send Secure Messages only to one peer at the time.
- Exception made for BlackBerry, **you can use Emoji** characters to spice up your messages



To use Emoji set it's mandatory to enable this character set on your device. This is an Operating System option thus please refer to your device manual.


- You **cannot attach anything to a Secure Message**: Secure Messages are actually text only.
- Secure Message **length** is **fixed** to a **maximum** of **160 characters**.
- Each Secure Message has a **time validity**, after which it **expires**. Expiration means that the Secure Message content is **no longer readable** and it's gone for good. Instead of message content you'd rather read "Message received" or "Message sent".

BlackBerry expired Secure Message	iPhone expired Secure Message	Android expired Secure Message
-----------------------------------	-------------------------------	--------------------------------



Each time you send a Secure Message you can see a status icon appearing on its side. Here follows an explanation of each icon along with its status name and meaning:

Icon	Description	Meaning	Timeouts and general behaviour
	Sending Message	PrivateGSM is actually trying to send the Secure Message to its recipient via PrivateServer	<p>If there is some network issue, then PrivateGSM starts the retry procedure: it tries to send 5 times the message to PrivateServer. If it fails at the fifth try (5 * TLSTimeout = 60 secs), then the message remains in the client queue waiting for one of the following triggers:</p> <ul style="list-style-type: none"> ◦ The user can connect to Sip Server ◦ The client sends a SIP KeepAlive to the server ◦ The user sends another message <p>If more than 12 hours passed and the message is still in client queue waiting to be sent, then the message expires: a "Send error" notification is fired by PrivateGSM and the message is removed from local queue</p>
? Unknown Attachment	Message Enqueued	Secure Message has been enqueued in PrivateServer encrypted storage and will be delivered to recipient as soon as possible.	If delivery is not possible because the peer is offline, PrivateServer retries as soon as recipient registers for up to an expiration period (72h), before removing them definitely from the database.
	Message Delivered	Secure Message has been delivered to recipient's device, who could have read it or not.	None

	Error sending Message	This status is a fall back for any other one and it's triggered both by timeouts and error responses.	None
---	--------------------------	---	------

History	Other functions and settings
-------------------------	--