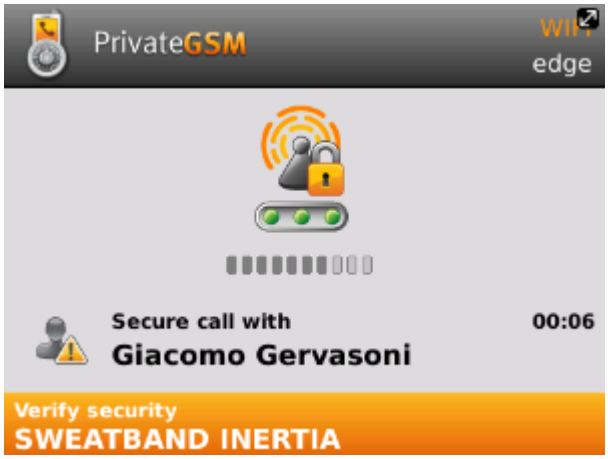
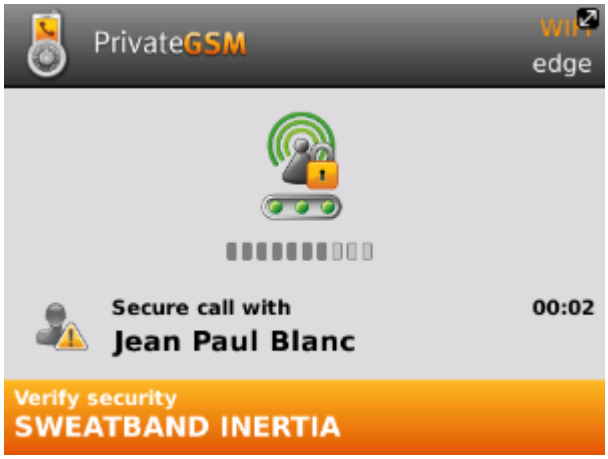
Top Secret Security

The "Top Secret" level applies an End-To-End security model, with audio data encrypted on one end point of the call and decrypted on the other end point without any possibility to intercept it in the middle. PrivateGSM relies on ZRTP protocol so there is no need to deploy a PKI infrastructure, but a human verification is required to exclude the presence of a MITM (Man In The Middle).

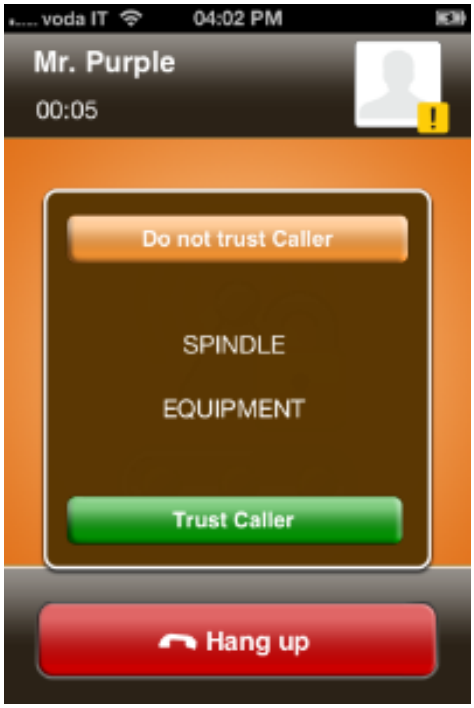
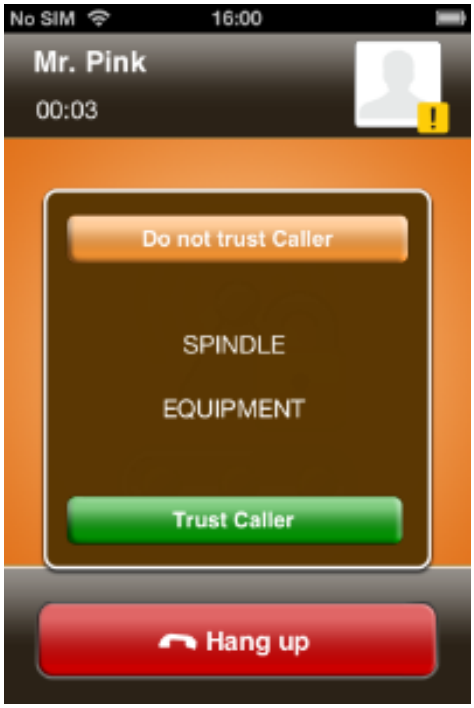
Verifying call security

PrivateGSM Professional and end-to-end encryption enabled version use an encryption and security system based on ZRTP protocol. This protocol is based on "human" verification of two words (called Short Authentication String or SAS) displayed at the beginning of a call. The SAS are made up of two words in English, randomly generated for each call. The same SAS displayed on the two phones must be verbally compared by the two callers to guarantee call security. After the security has been verified the two peers should trust each other.

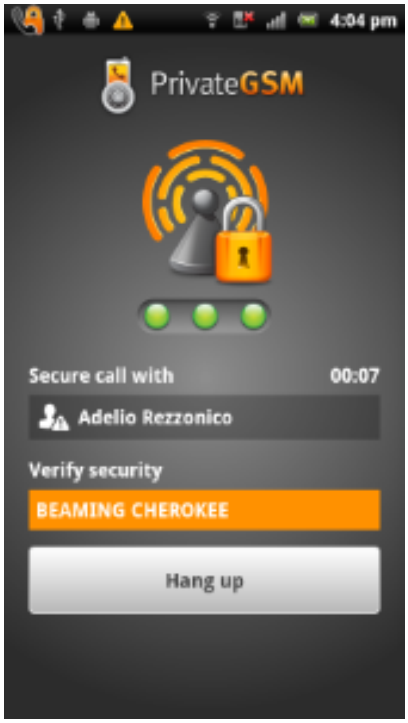
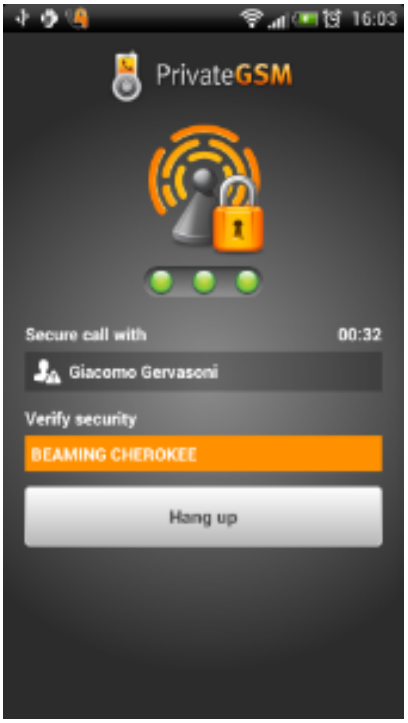
Verify call security on BlackBerry:

		
1. The caller reads his key out loud		**2. The called party makes sure it matches his one**
	Matching key exchanges : the call is secure!	

Verify call security on iPhone:

		
1. The caller reads his key out loud		**2. The called party makes sure it matches his**
	Matching key exchanges:the callis secure!	

Verify call security on Android:

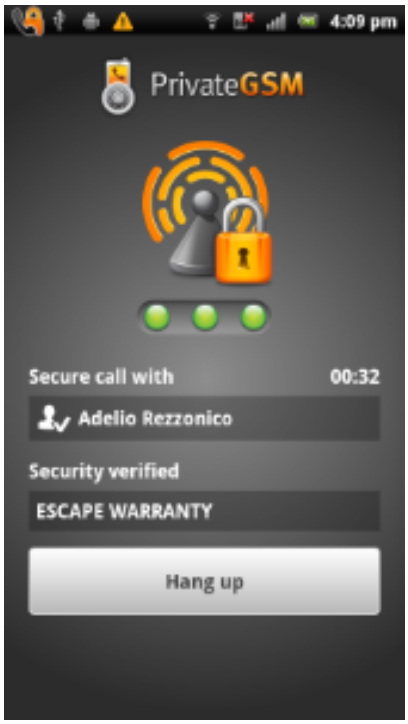
		
1. The caller reads his key out loud		**2. The called party makes sure it matches his**
	Matching key exchanges:the callis secure!	

Suggestion

After making sure the Short Authentication Strings match and that the called party is really the person you are speaking to, save the contact in the phone book as "trusted" by clicking **Trust**. This way you need not verify the key exchange next time you call this (trusted) contact in the future.The Short Authentication Strings will no longer be highlighted in orange. Security is guaranteed by the ZRTP key continuity feature.

In normal conditions subsequent communications with a "trusted" contact can start without the need of verbal verification. Short Authentication Strings background color will be different and SAS should only be verified in the event of wiretapping attempts or change to one of the two phones' configurations. In this case, the keys must be verbally verified or the call immediately interrupted.

Secure call between trusted contacts



1. Trusted contacts

Warning

If the SAS does not match with your peer's one you should immediately hang up the call as this might be a sign of a Man in the Middle interception attack.

Identifying a wiretapping attempt

Attempt to wiretap a call to a "trusted" contact

If a third party attempts to wiretap a call to a contact previously "trusted" by you PrivateGSM automatically detects the wiretapping attempt, interrupts the call and displays the following security alert.

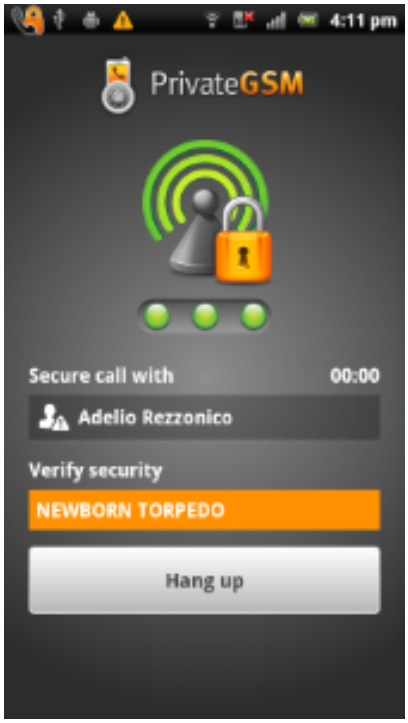
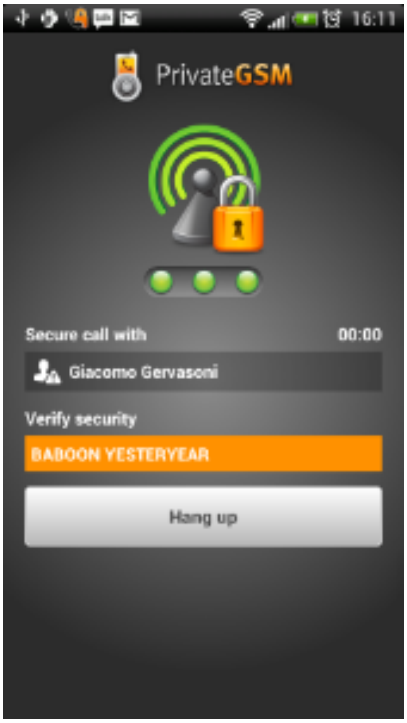
WARNING
PrivateGSM detected a possible security breach. You must call again and check the authentication string with your partner. Current call is automatically terminated to let you read this warning. Please note that this warning may happen also if your partner changed the mobile phone or reinstalled/restored PrivateGSM.

The security alert may even be displayed when there is no wiretapping attempt but your contact changes his phone number or phone. It may also be displayed when the software is re-installed on one of your trusted contact's phones. You must always re-verify contact security after a security alert.

After receiving a security alert, you must always verbally re-verify the SAS after the cryptographic key exchange and re-trust your contact for future calls (see chapter Verifying call security).

Attempt to wiretap a call to a contact not yet saved as "trusted"

In the event of a third party attempts to wiretap a call to a contact not yet saved as trusted, PrivateGSM displays two different Short Authentication String on the two phones. The callers should verbally verify the differences between the two key exchanges and interrupt the call.

		
1. The caller reads his key out loud		**2. The called party verifies that keys do NOT match and interrupts the call!**
	NON matching key exchanges: wiretapping attempt in progress!	