End-to-End Security

End-To-End security model encrypts audio data on one end of the call and it decrypts audio stream on the other one without any middle point exchange. When using End-to-End Security model, PrivateWave relies on **ZRTP** protocol so there is no need to deploy any PKI infrastructure, but it's required human verification on each call, so to exclude possible MITM (Man In The Middle) attacker.

Verifying call security

PrivateWave Professional uses 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 was verified the two peers could trust each other.

Verify call security: matching keys means the call is secure!

figure 1. caller' SAS must match callee's one

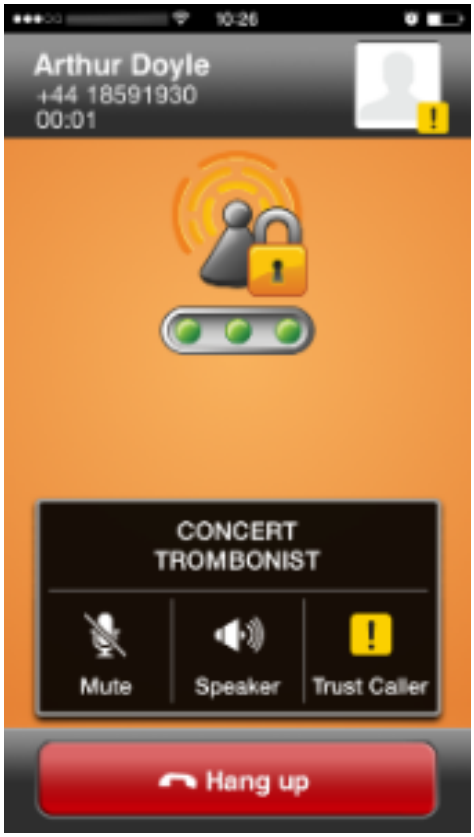

figure 2. caller' SAS must match callee's one

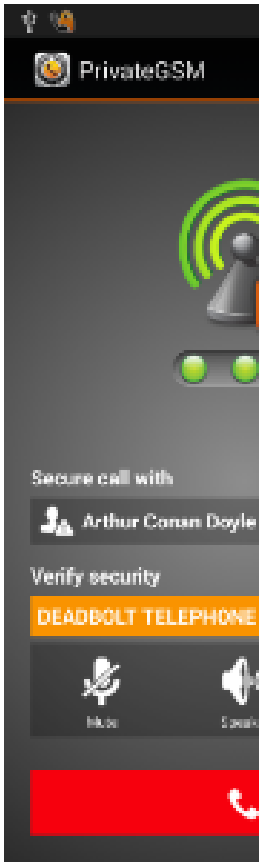

figure 3. caller' callee&#3

Caller reads his key out loud and callee checks they match his owns.

> **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

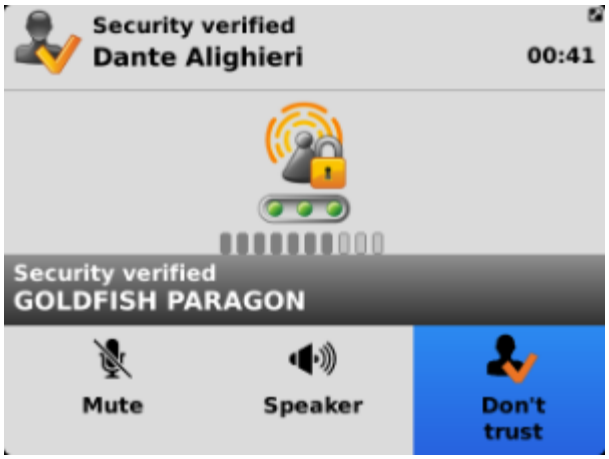

figure 4. Trusted contacts

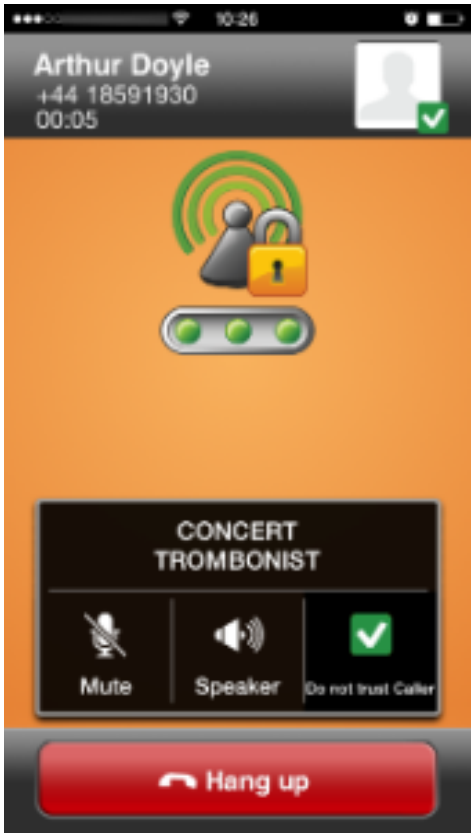

figure 5. Trusted contacts

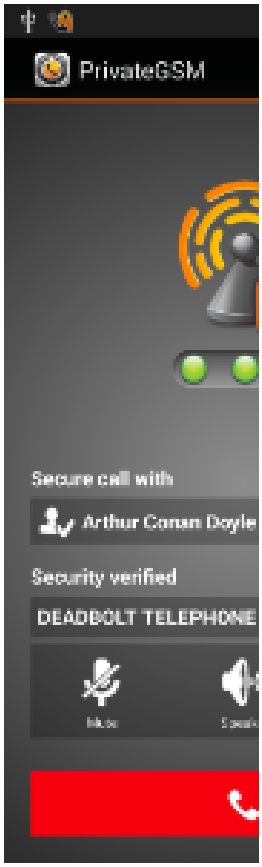

figure 6. Trust

> **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 PrivateWave automatically detects the wiretapping attempt, interrupts the call and displays the following security alert.

WARNING
PrivateWave 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 PrivateWave .

> 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 when you're speaking to a contact not trusted, PrivateWave displays **different Short Authentication String** on the two phones. The caller should verbally verify the differences between the two key and interrupt the call.

End-to-Site Security

Checking in progress calls