"PrivateWave detected a possible security breach. You must call again...": what does it mean?

Question: I got this error message while trying to dial a ZRTP secure call. What does it mean?

Answer: Each device is identified by ZRTP-ID (a auto generated identifier, generated once at install time) and also by mobile phone number (CLI). When you mark the other peer as "trusted" you are marking the couple <ZRTP-ID, CLI> as trusted in your device memory.

Upon secure call, ZRTP-ID and CLI are checked for trustiness. If only one of this two changed (e.g.: SIM exchange, uninstall/install PrivateWave -> a new ZRTP-ID is generated) we face a situation similar to what an MiTM attacker could try. For security reason, PrivateWave warns that this situation, could be both valid and legal or a MiTM attack. So, secure call is hanged and you are forced to re-check SAS (Short Authentication Strings) to validate the other peer trust.