

# SECURE CALL



## OVERVIEW

# 1. Product Description

A 100% software solution that enables two users from anywhere in the world to talk and send SMS over an encrypted Line using any GSM network that supports Data call (CSD) facility. The software, “Secure Call” requires to be installed on user’s handsets, along with a Secret Key entered by all users. If the key is not entered correctly the secure calls will not be established.

After installation the user can access the software from the Main Menu of the phone to place secure calls to other users. To place the call the user needs to enter the normal phone number of the caller from the dialer screen. To send secure SMS, the user needs to send an SMS from within the application that will be encrypted and send over the GSM network.

When an encrypted call or SMS is sent to the other handset, the software checks for the correct keys on both ends and then initiates a 256 bit encrypted call.

## 2. Implementation

### Instant Secure Communication

This application ensures that information can be sent from anywhere in the world to headquarters within a few seconds. Some information requires to be sent instantaneously and requires an instant reaction. With Secure Call, a simple call is to be placed to HQ and a conversation can take place to aid instant decision making.

### Non Tapping Solution

The data transferred over the GSM networks is encrypted, where the users can be assured that no one will be able to listen in. Missions and consultants in foreign countries do not need to be bothered of who is listening into their conversations, as they are over a data line which is heavily encrypted. At no point is any data sent over a voice channel or is in clear text type transfer.

### Security

The Secret Keys can be changed by users at any time, to ensure that keys cannot be hacked by a listening party. The Secret keys can be entered by the users at any time, and it will be reflected on the next call. Even if a key is compromised, changing the key regularly will help in maintaining a high level of security.

## 3. Configuration

The Secure Call Software is simple to configure. Just enter the Secret Key on all phones that wish to communicate with each other and you are done. Simplicity of this software should not be mistaken for its performance. In the background the software uses Data Call facility provided by the network provider to seamlessly auto-adapt itself to any GSM network. The end user does not need to enter the bps, port parity or any other settings to make it operational. Just the Secret key and you are ready to go. An Intelligent plug and play system ensures smooth operations. Software access in the handset is protected by a password to ensure that eligible users can gain access to the main menu. The users can change the access code/password at any time.

## 4. Security

The software runs on a 256 bit encryption, with a 32 alpha numeric Initializing Vector (IV) provided by the end user. This ensures the following:

1. All calls are 256 bit encrypted.
2. The IV or Secret Key can be changed at any time to ensure higher security
3. As the IV or Secret key is entered by the end user there are no back doors, or security lapses. The security is the in the hands of the end users. In other words, harder the Secret Key (or IV), higher the encryption.
  - a. For e.g.: a key 12345678912345678912345678900 can be easily broken as compared to !@3AJ!@#MSn1239!@#1;lOa-AKms\*uA which is harder to crack.
4. Keys are not exchanged at any time during the call set up or handshaking thus ensuring that no one, including the network provider can listen to the calls.
5. The software and call logs are password protected so that no one can view the calling activity when they have access to the handset.
6. Secure call logs are not viewable in the normal call registry of the phone.

# 5. Software:

The software is only available for sale to Law Enforcement or related agencies. The software has the following modules:

## 1. Encryption Layer:

This module ensures the security of the call. The voice data is captured by the encryption layer, encoded into a Voice Codec, encrypted and the rapidly pushed over the data channel. The encryption layer also receives encrypted data, decrypts it and plays it on the speaker of the phone. If the data is not encrypted correctly then it drops that packet. The encryption layer does not exchange keys between phones to ensure the highest possible level of security.

## 2. Auto Configuration Layer:

This layer is activated as soon a call is placed and answered. It auto enumerates the settings of the HSCSD or CSD settings and sets it for this particular call. The layer remains active during the course of the call and ensures dynamic settings if there is a change in the duration of the call. If the user steps out of the network coverage or the software is not able to enumerate the CSD settings, it immediately disconnects the call.

## 3. User Interfaces

This layer only allows users who have validated themselves by entering the correct password to open the operational screens of the application. This layer sends call and answer commands to the core of the application.

## 4. Logging Engine

Ensures that secure call logs are not visible in the call registry of the phone and allows the user to select contacts from the Contacts or Call Logs to place calls.


# 6. Software Operations

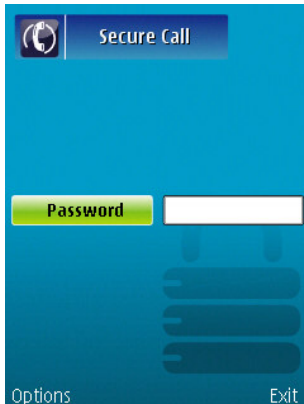
- **Encryption:** 256 bit encryption
- **Delay:** Less than 1 second for the duration of call after first 4 seconds.
- **IV:** Provided by the end user
- **Channel:** CSD, HSCSD or EDGE
- **Requirements:** Compatible Handset (as listed in Appendix A.2.) and a GSM Network that supports CSD or HSCSD
- **Trial:** Available. Expires after one phone restart and allows a 60 second call only.
- **Final Version:** Require IMEI number for final application delivery.
- **Source Code:** Available for review for Law Enforcement only. Additional costs and conditions apply for opening source code to ensure that no back doors are incorporated.

# APPENDIX

## A1. Application Screenshots:

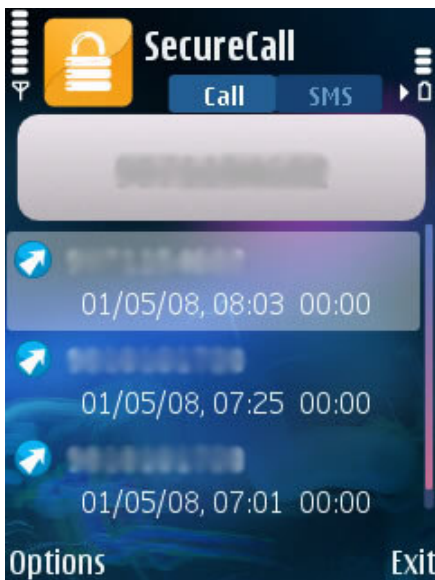


Click on  in the main menu of the phone. Will open main screen which prompts to enter password:

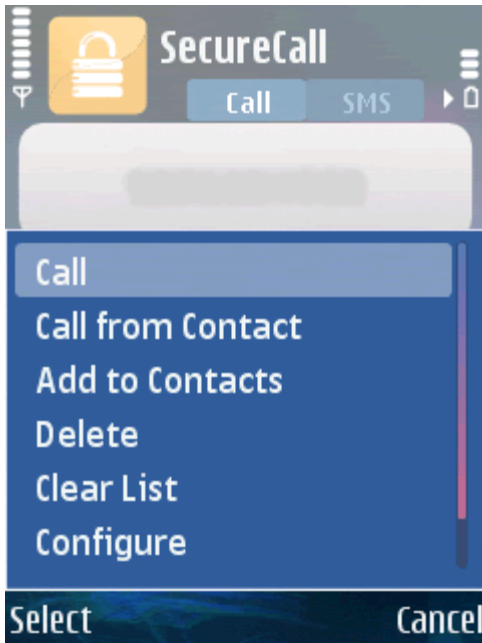


Screen A.1: Enter Password

Success verification will open the dialer screen. Enter the phone or select a number from the call logs below and press the Green Call key or Click **Options** > *Call*.



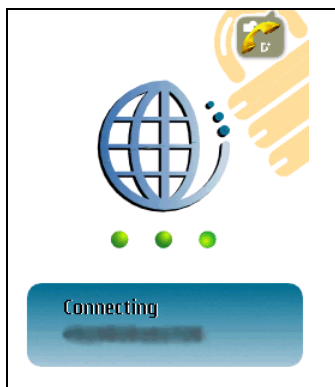
Screen A.2: Dialer Screen



Click Options on the main screen to show the following options:

1. **Call:** Will place a call to the entered/selected phone number
2. **Call from Contacts:** Will open the contacts view of the phone, to select a number to dial
3. **Add to contacts:** Will add a selected contacted to the phone book
4. **Delete:** Will delete the selected call entry
5. **Clear List:** Will remove all call entries
6. **Configure:** Will open the configuration Screen.

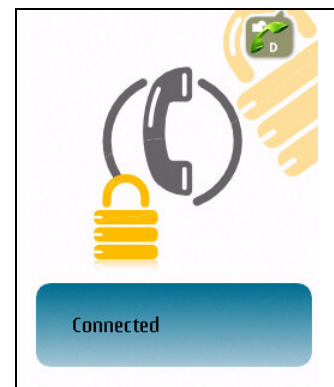
Calling a phone number will trigger the following sequence:



Screen A.3: Calling Screen



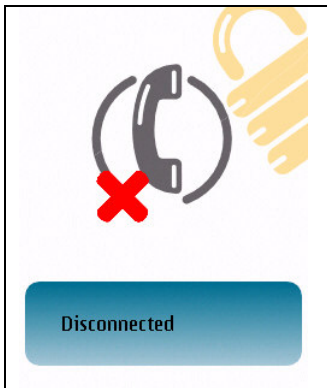
Screen A.4: Handshaking Screen



Screen A.5: Connected Screen



At the **end** of the call, the following screen will appear:

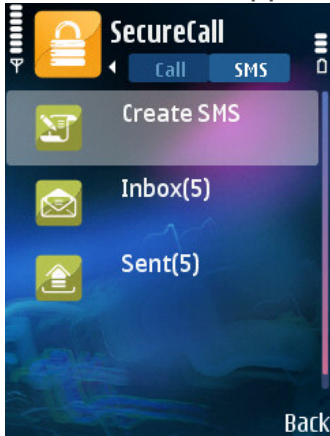


Screen A.6: Disconnected Screen

To Set/Change the IV or Secret Key, press **Options** > *Configure* in the Dialer Screen:



To send an SMS: In the main screen, press the right joystick button and the SMS screen will appear:



Click on *Inbox* to view all incoming Secure SMS

Click on *Sent* to view all Secure SMS sent from the phone.

Please note that none of the incoming or outgoing Secure SMS will appear in the Normal Inbox of the phone.

Click on Create SMS to compose and SMS

