

- **Fundamental requirements**
- **Application Activation**
- **Secret Menu**
- **GeneralKey entry**
- **Normal Message Create**
- **Private Message Create**
- **Normal Message Read**
- **Private Message Read**
- **Configuration**



Fundamental requirements

EmoSEC is a state of the art SIM ToolKit application, running on TG48 silicon, a GSM certified secure silicon device produced by Emosyn an ATMI company.

EmoSEC is a derivative of Silcom Technologies SIMToolkit enabled GSM11.11 Phase 2+ SIM operating system. EmoSec will run on any Phase2+ SIMToolkit enabled Mobile Equipment conforming to the minimum terminal profile of `0B 01 05 23', for reliable PINCode support the terminal profile must be at least `0B 03 05 23' and for full support of all current functions the following profile must be met or exceeded `0B 83 17 23 00 00 00 18 01'.

It should be noted that an ME must not only report the profile, but also fully support the profile !. Your attention is drawn to this fact, because in testing we have discovered many mobiles that report profiles that are NOT fully supported or are « buggy », in these cases the application will perform unreliably.

For the purposes of this document we will explain the operation of the application based on use of the popular low cost mobile equipment supplied by Alcatel, model 311. Other models that we have determined to support the application are Alcatel 501 and 511. Siemens models SL45 and S45 also meet the minimum requirements, but not the full requirement. Notably the Siemens Models do not fully support Cover mode operation.

The EmoSEC application is large and pushes the mobile close to the limit of functionality, small changes in software revisions of the mobile equipment can severely affect the functionality of the terminal profile. Care should be taken to fully test the equipment before deployment.



Application Activation

We recommend that in all cases the SIM card PIN is enabled. The application can run in Covert or Overt mode :

Overt mode : Upon switch on and after entry of the SIM PIN, the application is invoked from the user menu on the mobile equipment. Viewing the menu the user will see a menu option

EMOSIM, selection this option will activate the Secure SMS application in Overt Mode.

Covert mode : upon switch on and after entry of the SIM PIN, the application is invoked by dialling the application PIN Code - default 987654321. Pressing the send key after dialling the application PIN will activate the Secure SMS application.



Successful entry into the application is indicated by the message « service activ » momentarily before the application menu is displayed.

General key

Successful entry into the application is indicated by the message « service activ » momentarily before the application menu is displayed.

The application menu shows « SMS secure », pressing OK will prompt the user for the GeneralKey, default - aaaaaaaaa, this key is case sensitive, on the Alcatel 311 lower case is selected by pressing the # key before entry of the alpha character. The Alcatel 311 will prompt the user for confirmation of input after pressing OK, press OK again to confirm your entry.

Normal Message Create

A normal message can be received and decrypted only by other EmoSEC users with the same GeneralKey, this can be considered as a Group message

After entry of the GeneralKey, the menu will show « Create », « Read », « Setup ». To create a Normal message :

Action	Option	Prompt
Select	« create »	
Press	« OK »	
Select	« normal »	« Enter Text » text entry is via the keypad with the option of T9 if required.
Press	« OK »	« mobile number » enter the mobile number via the keypad.
Press	« OK »	« send », « store », « Exit » The message can be sent, stored or discarded as required

Private Message Create

A Private message can be received by any EmoSEC user using the same GeneralKey, but can only be decrypted by an EmoSEC user with the same GroupKey and knowledge of the passphrase. This can be considered as a private message within the EmoSEC group.

After entry of the GeneralKey, the menu will show « Create », « Read », « Setup ». To create a Private message :

Action	Option	Prompt
Select	« create »	
Press	« OK »	
Select	« Private »	« PassPhrase », enter at least 8 characters. The PassPhrase must be agreed between the sending and receiving party.
Press	« OK »	« Enter Text » text entry is via the keypad with the option of T9 if required.
Press	« OK »	« mobile number » enter the mobile number via the keypad.
Press	« OK »	« send », « store », « Exit » The message can be sent, stored or discarded as required

General Message Read

After entry of the GeneralKey, the menu will show « Create », « Read », « Setup ». To read a General message :

Action	Option	Prompt
Select	« read »	MSISDN's will be shown, 1 for message received. Select the message to be read and if that message is a general message, it will be decrypted and displayed.
Press	« OK »	« Done » « Delete » « Forward », select the option of your choice. If selecting « Forward », you will be prompted with « Private » or « Normal » message creation.

Private Message Read

After entry of the GeneralKey, the menu will show « Create », « Read », « Setup ». To read a Private message :

Action	Option	Prompt
Select	« read »	
Press	« OK »	MSISDN's will be shown, 1 for message received. Select the message to be read.
Select	« MSISDN »	« PassPhrase » the correct PassPhrase must be entered to decrypt and display the message.
Press	« OK »	« Done » « Delete » « Forward », select the option of your choice. If selecting « Forward », you will be prompted with « Private » or « Normal » message creation.

Configuration

After entry of the GeneralKey, the menu will show « Create », « Read », « Setup ». To configure the system :

Action	Option	Prompt
Select	« setup »	« SMS SCenter » « Validation » « Announcement » « Multilingual » « ReRouter » « PINCode » « KEY »
Select	« SMS Sceneter »	Enter your secure SMSC
Select	« Validation»	Select the time to live for undelivered SMS messages
Select	« announcement »	The mobile can indicate the receipt of a secure message, even when in covert mode. Select the options most suited to the situation.
Select	« Multilingual»	Language support
Select	« ReRouter »	Enter the MSISDN of the EmoSEC equipped mobile to route the message via. To disguise the senders address.(* network / mobile limitations mean that this option may not be successful, test before use)
Select	« PINCode »	Modify the the activation PINCode. This is the number dialled to activate the covert menu. Selecting « OFF », will deactivate covert operation and move the application to Overt mode. Entry into the system will be via the standard mobile menu, under « EMOSIM » Selecting « change », will allow the PINCode to be changed. Note- this PINCode will be dialled to enter the covert menu, DO NOT select a valid mobile number, the number WILL BE dialled, if the call is answered, the security of the application may be compromised.
Select	« KEY »	You may « change » the GeneralKey. You may create a new GeneralKey. If a new general key is created, stored messages using the old Generalkey will be rendered unreadable. All users in a Group MUST use the same generalKey. For added security the Group should operate a policy of regular KeyChanges. The GeneralKey is case sensitive, as with all crypto keys, names and readable text should be avoided. Select a Key containing Upper and lower case characters and include numbers. The Key MUST be at least 8 charaters in length.

EmoSEC Function Guide

PINCode :	<p>Used to activate the Covert menu system.</p> <p>The PINCode is entered via the keypad, the send button is pressed to enter the PinCode. (as if dialling a telephone number). Once dialed, the PINCode will activate a covert menu, allowing access to the secure SMS system.</p> <p>The PINCode is user definable and can be changed only after entry into the system. The user may change the PINCode only after entering the existing PINCode or the transport PINCode if the system is new.</p> <p>The user may define the PINCode to be one of two conditions :</p> <p>(OFF) - If set to OFF, the secure SMS system becomes Overt. The secure SMS system no longer requires the entry of the PINCode. The secure SMS system will be viewable and accessible from the standard mobile menu under the heading EMOSIM, a user key will still be required before use of the system will be granted</p> <p>(ON) - If set to ON, the secure SMS system becomes Covert. The secure SMS system required entry of PINCode to activate the covert menu.</p> <p>User defination of the Covert/Overt function can be disabled by the manufacturer during card personalisation, locking the system in Covert or Overt mode.</p>
Transport PINCode :	<p>When delivered the system will be enabled with a Transport PINCode, this should be changed to a secure PINCode before deployment of the system.</p>
GeneralKey :	<p>To enable communications between users. To define user groups and to encrypt and decrypt messages.</p> <p>Each user group MUST use the same GeneralKey. A group may consist of one or more users entering the same key to access the secure message base in the SIM card.</p> <p>A user may belong to more than one group, but may only have one GeneralKey active in the SIM card at any one time. Recollection of additional GeneralKeys is the responsibility of the user.</p>

Passphrase :	<p>Used to encrypt and decrypt Private messages between the users in a group. A Passphrase is only valid between users operating with the same GeneralKey.</p> <p>When creating a secure message, the user has two options :</p> <p>Normal : The user enters the message text and recipient mobile number. The system uses the GeneralKey for encryption, thus any user with the same GeneralKey can decrypt the message. This can be considered a Group message.</p> <p>Private : The user is prompted for a Passphrase. The message is then encrypted using Passphrase and Generalkey. Only a user in the same group using the Passphrase can decrypt the message. This can be considered a Private message between users in the same Group.</p> <p>A user receiving a Private message, will be required to know the Passphrase in addition to the GeneralKey. The user will be prompted to load the Passphrase when trying to read a Private message.</p> <p>A user may receive messages from many other users in the Group, each user in the group may use an unlimited number of Passphrases when creating Private messages.</p> <p>It is not possible to decrypt a Private message without the matching Passphrase, even if the user has entered the GeneralKey. The Passphrase never stored inside the system.</p>
SMS Center :	The MSISDN of the SMS center in international notation. This allows either the default mobile account SMSC to be used, or an alternative SMSC for secure messaging.
Validation :	Time to live for undelivered SMS Messages, see GSM specifications for more info.
Announcement :	<p>The notification received when a secure SMS is received, Can be set to :</p> <p>SOUND-ON, ICON-ON SOUND-OFF, ICON-ON SOUND-ON, ICON-OFF SOUND-OFF, ICON-OFF</p> <p>For covert operation, SOUND-OFF, ICON-OFF, is recommended. Receipt of messages should be periodically to prevent attention being drawn to the application up on receipt of a secure message.</p>
Multilingual :	Language options
ReRouter :	Messages can be routed via other EmoSEC equipped mobiles to disguise the origin of the sender.