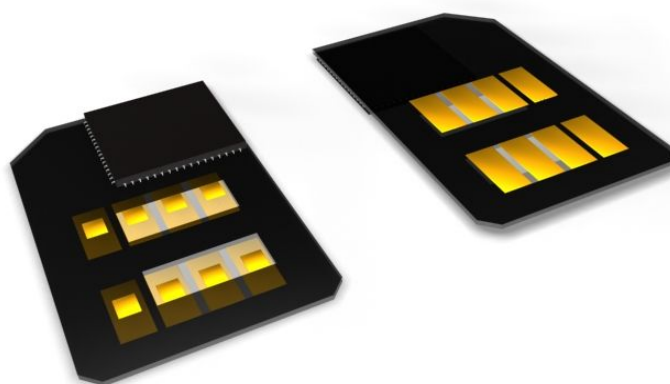


## Introduction

**Turbo SIM – Security Edition** is a device with a set of pre-installed applications targeted at SMS encryption and privacy protection. Inserted in the SIM Lock together with the operator SIM card, the device can be used in any GSM SIM Toolkit enabled mobile phone, i.e. almost every mobile phone produced since 1998.



**Turbo SIM - Security Edition** has been developed to be used by financial institutions, security organizations, businesses and every other area that uses SMS for critical communications with a need for protection against eavesdropping and message spoofing (sender faking). Furthermore, it can be used for general mobile phone protection and as a secure store of private information.

Being independent of the mobile phone used makes it ideal for deployment in the heterogeneous environments of governments, large organizations or any establishment with a high mobile phone turn over rate.



**Turbo SIM – Security Edition** contains following applications:

- **Secure SMS** – SMS communications are protected against eavesdropping and message spoofing by the employment of the strong Twofish<sup>1</sup> symmetric cipher. To simplify the usage of Secure SMS, secret keys can be assigned to individual phone numbers. It is possible to have dozens of keys for communication in large enterprises – including secret keys that can be hidden against a user (users then do not know the keys and cannot view them).
- **Killing SMS** – it is possible to define a special “Killing SMS” that blocks or resets the mobile phone in the event that it is lost or stolen. This makes it impossible to make calls, or otherwise manipulate the phone, when used together with the SIM card PIN and phone locking.
- **Flash SMS** – messages sent using this application appear directly on the recipient's mobile phone display. No more wasting precious seconds going into the SMS Inbox – the message are instantly displayed on the screen.
- **Secrets** – an application for the secure storage of private information, e.g. passwords, bank accounts, credit card numbers, etc. A very handy way of keeping that critical data conveniently in your phone, yet safe from possible discovery.

## User Interface

After inserting the **Turbo SIM – Security Edition**, a new menu item called **Secure** appears on the mobile phone – containing the following applications:

**Secure SMS**  
**Flash SMS**  
**Secrets**  
***SIM Applications\****

*The item **SIM Applications** is optional and is offered only when there are other SIM Toolkit applications available on the SIM card. The label of this item depends on the SIM card provider (operator).*

**Note on phone number selection.**


*Whenever phone number is inserted user can either: select number from SIM phone book, enter it directly, select it by position in SIM phone book or search by the first letter.*

## Secure SMS

Secure messages can be used for protecting SMS communication against interception.

When the application is locked there are two options in **Secure** -> **Secure SMS**:

- **Send secure SMS**
- **Unlock application**



Send Secure  
Unlock

It is possible to send secure SMS even if application is locked but user needs to enter secret key for encryption, even if it is already associated to given phone number (see *Key Management* section on page 5).

Incoming secure messages can only be read if application is unlocked.


### **Unlocking application**

After **unlocking** the application user can:

- **send** secure messages without entering secret key for message encryption (when the recipients phone number has an assigned key (see *Key Management* section on page 5))
- **view, reply and delete** secure **messages**
- **manage secret keys** used for message protection and assigning keys to phone numbers
- **change main key** for unlocking
- **define and send Killing SMS**

*The default key for application unlocking is 1234*

The application locks automatically when the user exits the **Secure** menu or if not used for a short period of time (usually 30 seconds, but this depends on the mobile phone used).

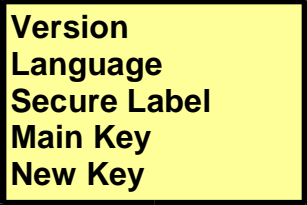


Send Secure  
Setup  
Killing SMS  
+12345678  
John

If there are any secure messages stored on the SIM card they are listed below the menu options. Messages are labelled by the sender (either phone number or name if known) and are ordered by time of arrival with the newest messages on top. In the example above, **+12345678** and **John** are secure messages.

*Due to the limitations of most SIM cards, the maximum number of secure SMS stored is set to 10. Application warns user whenever the SIM card is full or this number is reached.*

## Setup



Version  
Language  
Secure Label  
Main Key  
New Key

**Version** contains serial number and information about the application and firmware versions.

**Language** option allows the preferred language to be set. The user interface is localized to **English**, **French**, **German**, **Danish** and **Czech** languages.

**Secure Label** allows the user to set what message should appear when read via standard phone interface for messages – i.e. SMS Inbox. The default is “**Secure Message**” but sometimes it is desirable to display alternative text to make the secure message delivery less obvious to possible reader, e.g. “Message delivered”.

*This feature is not supported on every mobile phone due to problematic standard compliancy by some vendors.*

## Key management

The secure messages are protected by secret keys negotiated between communicating parties. These keys are used for enciphering the text with the strong 128 bit Twofish cipher in CBC mode (i.e. two messages of the same text, encrypted with the same key, appear different).

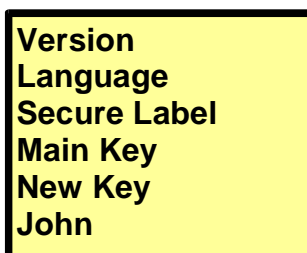
To simplify the secure SMS communication the application provides management of the secret keys. These keys are stored encrypted internally and can only be accessed by the unlock key (main key).

The **Main Key** item allows to change the application unlock key.

The **New Key** item is used for creation of a new secret communication key associated to an individual phone number. It is inserted in two steps:

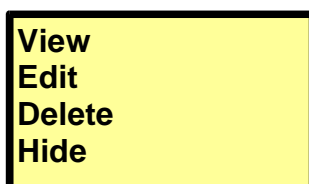
1. **Phone number**
2. **Secret key**

The result is the new menu item, e.g. **John**:



Version  
Language  
Secure Label  
Main Key  
New Key  
John

Every secret key can be **Viewed**, **Edited**, **Deleted** or **Hidden**.



View  
Edit  
Delete  
Hide

If the secret key is hidden it cannot be viewed nor edited, only deleted. This allows a higher authority to set secret keys and keep them unknown to users.

## **Sending secure message**

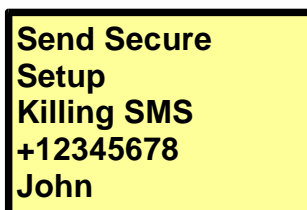
The sending of secure message is similar to sending of a standard text message. Simply select **Secure** -> **Secure SMS** -> **Send Secure** and do two or three steps:

1. **Enter message text**
2. **Select recipient**
3. **Enter key for message encryption.** This step is omitted when the application is unlocked and there exists a secret key associated to given recipient.

Note: The secure message is limited to 136 characters in length.

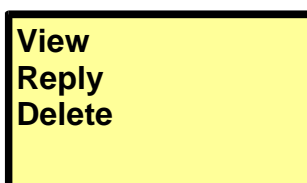
## **Answering secure message**

To reply to the secure message with a secure answer, select the message in the main menu:



Send Secure  
Setup  
Killing SMS  
+12345678  
John

By selecting the message, e.g. John, there appear three options:



View  
Reply  
Delete

Selecting **Reply** leads to entering the answer text. If there is no secret key available for the given phone number the user is prompted for the key at this time.

## **Deleting message**

To delete the message it is possible to use the option available for every secure message, but, we recommend using the standard message interface for message deletion and use this only in the event of the mobile phone failing to delete the message the standard way. Some mobile phones have firmware issues with deleting SMS messages on SIM card.

## **Answering plain text**

The secure messages are stored on the SIM card as any other text messages. To answer

with plain text (unsecure) use the standard mobile phone interface for messages.

## **Killing SMS**

**Killing SMS** is a special SMS that blocks or resets the mobile phone in the event that it is lost or stolen. This makes it impossible to make calls, or otherwise manipulate the phone, when used together with the SIM card PIN and phone locking.

To define “**killing**” text use **Secure SMS->Killing SMS->Edit**.



**Killing SMS** is sent by **Secure SMS->Killing SMS->Send**.



## Flash SMS

**Flash SMS** is an application to make a message appear directly on the recipient's mobile phone display. The usage is simple, just enter desired text and select phone number.

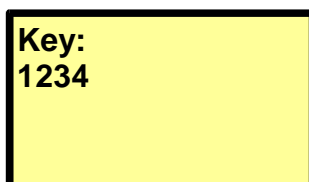
## Secrets

The **Secrets** application can be used for storing private/sensitive information (passwords, PINs, bank accounts, etc.) in secure manner. The information is stored in the internal memory of **Turbo SIM** encrypted by strong 128 bit Twofish cipher in CBC mode.

The access to the information is protected by alphanumeric password that can be 17 characters long.

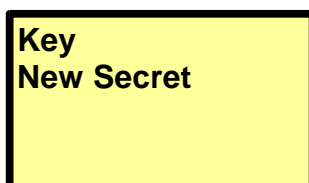
### Unlock

The first step is to enter the key (password):



*The default key is set to 1234*

If the correct key is entered, the following menu appears:



The access key can be changed by selecting the item **Key**.

## New secret

A new secret is created with the help of **New Secret** item in two steps:

- Enter name (label):

Name:  
My weight

- Content of the secret:

Enter Text:  
70 kg

The result is the new secret **My weight** in the main menu:

Key  
New Secret  
My weight

### **Security note**

*In the internal memory, only the content of the secret is encrypted (i.e. 70 kg in our example), the name is left in plain text.*

**Every secret can be Viewed, Edited and Deleted.**

## Notes on security mechanisms used

1. **Turbo SIM** – Security Edition uses 128 bit symmetric cipher Twofish, <http://www.schneier.com/twofish.html>
2. Messages and secrets are encrypted in **CBC** mode, i.e. the same text encrypted several times will look different every time.
3. It is used a **unique random number generator** that combines pseudo random generation techniques with **physical behaviour of the mobile network**.
4. For **protection against application manipulation**, the device is **locked** and it is impossible to upload or remove applications without first deleting the pre-installed applications.
5. For **protection against invasive attacks**, all keys and data are stored **encrypted** in memory, with the main unlock keys not being stored at all. In the case of an invasive attack no data is accessible in plain text. All messages stored on the SIM card are also encrypted for added security.