



Safe

1.0.12

User Manual

v1.0 -27/03/2006
Copyright © 2005-2006 By Ugo Chirico. All rights reserved

Disclaimer of Liability

The content of this manual has been checked for agreement with the software described. Since deviations cannot be precluded entirely, full agreement is not guaranteed. However, the data in this manual are reviewed regularly and any necessary corrections will be included in subsequent versions. Suggestions for improvement are welcomed.

Java (TM) and all Java related trademarks and logos are trademarks of Sun Microsystems, Inc. Other company products and service names may be the trademark or service marks of others.

Thanks

Many thanks to Ornella Simeoli for her good suggestions and her kind patience during the nights I spent to develop Safe.

Content:

Abbreviations and Acronyms 4

About this manual..... 4

1 Introduction 5

1.1 How it works5

1.2 Supported Platforms5

1.3 Technical details.....5

2 Installation 6

2.1 Installation from mobile phone via internet/WAP browser:6

2.2 Installation via Infrared port or Bluetooth connection:.....6

2.3 First activation6

3 Using the Main Menu 7

3.1 Create a new secret8

3.2 Read a secret9

3.3 Registering the program 10

Abbreviations and Acronyms

J2ME	Java 2 Micro Edition
MIDP	Mobile Information Device Profile
CLDC	Connected Limited Device Configuration
CDC	Connected Device Configuration
JVM	Java Virtual Machine
AES	Advanced Encryption Standard

About this manual

Safe User Manual is designed for experienced mobile phone users having good familiarity with encryption. An updated electronic copy of this manual is available at the following URL:

<http://www.ugosweb.com/safe>

1 Introduction

Safe is an application for Java enabled mobile phone for storing securely secrets into mobile phone's memory (or data card plugged into the mobile phone)

Safe allows encrypting secrets and any kind of confidential information, such as passwords, credit card numbers, phone numbers, etc., in the mobile phone's memory by supplying a secure, encrypted notebook where the user can encrypt and store all sensible information using a strong cryptographic algorithm such as AES256.

1.1 How it works

Safe encrypts secrets using the user PIN as the encryption key for AES256. The user can access to *Safe* only after typing the correct PIN (if the PIN typed is incorrect the decryption doesn't work). After that he can see all stored secrets or can add new secrets to the encrypted store.

1.2 Supported Platforms

Safe can be installed on any Java enabled mobile phone compliant with J2ME - MIDP1.0 or MIDP2.0 platform. The list (not completed) of all compliant devices is reported at the following url:

<http://www.ugosweb.com/safe/devicelist.html>

If your mobile phone is not in this list please download and try *Safe* and, write me to this address ugo.chirico@ugosweb.com, specifying the result of your test and the model of your mobile phone, so that I can update such a list.

1.3 Technical details

Safe uses AES256 for encrypting the secrets using the hash (SHA-1) of the PIN as encryption key.

2 Installation

Safe is available for downloading as shareware version for MIDP1.0 and for MIDP2.0 platforms. See the url <http://www.ugosweb.com/safe/devicelist.html> for the platform supported by your mobile phone. If your phone is not in this list please download and try MIDP1.0 version and, write me to this address ugo.chirico@ugosweb.com, specifying the result of your test and the model of your mobile phone, in order that I can update such a list (as reward you will receive a license for free)

2.1 Installation from mobile phone via internet/WAP browser:

- 1) open the browser on your mobile phone and point to: <http://www.ugosweb.com/safe/download.asp>
- 2) select MIDP1.0 or MIDP2.0 and follow the instruction on your mobile phone to complete the installation.

2.2 Installation via Infrared port or Bluetooth connection:

- 1) download the version for your mobile phone from:
<http://www.ugosweb.com/safe>
- 2) send the downloaded file .jar to you mobile device via infrared or Bluetooth connection
- 3) select the message with .jar attached or the file .jar itself (depends on your mobile device)
- 4) follow the instruction on your mobile phone to complete the installation.

2.3 First activation

Once installed, when you start the application for the first time, *Safe* asks you to type a special PIN code (and the confirmation of such a PIN) by which the internal secret store will be encrypted. Next time you start *Safe* you should enter such a PIN correctly to gain access to SMS repository.



3 Using the Main Menu

The main menu is shown in the picture at right.

The main operations are:

- *Create* creates a new secret.
- *Stored* shows the list of stored secrets
- *About* shows information about the program and license information
- *Registration* allows to register Safe
- *Exit* exits the application and returns to the phone's menu



3.1 Create a new secret

Select "New" from the main menu. The following are the steps to create a new secret:



Step 2 – type your secret



Step 3 – give a name to your secret

3.2 Read a secret

Select "Stored" from the main menu. The following are the steps to read a secret:



Step 2 – Select a secret from the store by name



Step 3 – Read the secret

3.3 Register the program

The registration of *Safe* is subject to a license fee.

See <http://www.ugosweb.com/safe> for more information about licensing and fee.

To register the program select *About* from the main menu and annotate the value of identification pass-phrase. The registration procedure will ask you such a value because is needed to generate your own registration code. The received registration code must be inserted selecting "Registration" from the main menu.



Step 1 – annotate the Identification Phrase



Step 2 – put here the registration phase