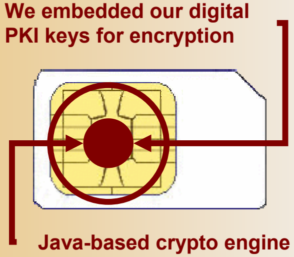
IPCS Group

SECURING m-COMMERCE
FOR EVERY MOBILE PHONE



We embedded our digital PKI keys for encryption

Java-based crypto engine

IPCryptSIM™

SMS encryption

a secure platform for
SMS-Banking
and
m-Commerce

User Manual

Content

Welcome to the IPCryptSIM™

The **IPCryptSIM**™ offers a range of highly desirable security tools for your mobile phone to secure your SMS communication through the strongest commercially available encryption technology.

Your mobile phone is today possibly the closest of all electronic devices in your daily life, and almost never out of your reach. Even though your mobile operator has made all attempts to secure your mobile phone, your SMS communication thus far has had some security issues with sending clear text via the public domain. Many users have turned to SMS communication in public places to avoid that they can be overheard by other persons nearby. This means that worldwide more than 1 trillion SMS are sent a year today and this vast number of SMS is growing daily.

The only security flaw of sending an SMS is that it is being sent over the public domain and may be stored at your mobile operator for some time. Although the chances are slim, this could mean that somebody could have access to the content of your SMS.

Using **IPCryptSIM**™ encrypted SMS as a means to communicate with your friends, family or bank no longer exposes your SMS to any security threat. Encrypting the text of your SMS renders it completely unreadable and guarantees that only the recipient of your choice can decrypt it and read it.

In fact the **IPCryptSIM**™ is so strong protecting your SMS that more and more banks have decided to deploy it for their banking clients and to allow banking transaction to be made via secure SMS.

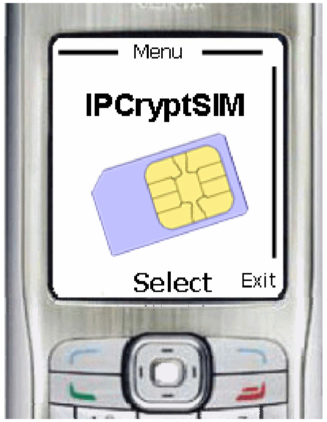
Whereas today there are a number of SMS encryption applications available for mobile phones, each only works with a selected number of mobile phone brands and then often with specific models, only.

IPCryptSIM™ has been developed to work with ever mobile phone that uses a SIM card, that little chip you receive from your mobile operator to install in your mobile phone before you can use it. This allows you to change you mobile phone whenever you like. Since you most likely do not want to change your mobile number when getting a new mobile phone, using the same SIM allows you to have the same secure SMS functions on your new mobile phone!

Thank you for purchasing **IPCryptSIM**™ and enjoy the freedom of secure SMS communication!

IPCS Ltd.

Introduction to your IPCryptSIM$^{\text{TM}}$

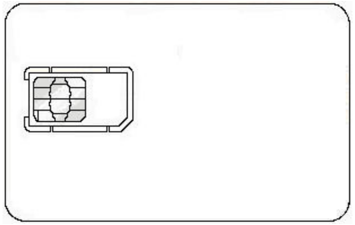


IPCryptSIM$^{\text{TM}}$ is a SIM card based encryption technology of according to International Standards and offers you absolute privacy and confidentiality in all your SMS text message communication and future mobile-Commerce and mobile-Banking transactions.

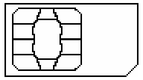
IPCryptSIM$^{\text{TM}}$ is the global choice due to its unsurpassed security yet complete ease of use and is the only known mobile security application that is SIM card based. It is, therefore, offering the same benefits to any type, brand or model of mobile phones.

IPCryptSIM$^{\text{TM}}$ SMS text messages are sent / received via the standard Short Message Service mechanisms. As a consequence, they are billed at the usual Telco’s SMS rate and will appear on the monthly service statements as regular text messages. **IPCryptSIM**$^{\text{TM}}$ supports "larger" content (also known as *LMS*,) allowing to send messages up to 1000 characters in length. This is done by segmenting over multiple messages and will therefore increase in cost proportionally (at the rate of about 1 extra SMS per 117 characters).

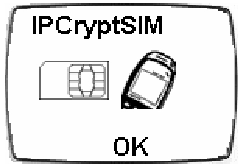
Installing your SIM card

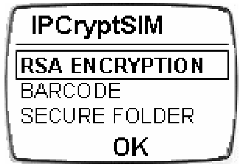


If your mobile phone has not been supplied with the SIM card already installed, you may receive the SIM card as part of a credit card size plastic carrier card, similar to the image on the left side hereto. You will be required to break out the SIM card from its carrier card. This is easy.



This is how your SIM card will look like after you have removed it from its plastic carrier card. To mount it into you mobile phone switch off your mobile phone, remove its back cover and battery. Slide your SIM card with its chip face downwards into the allocated space, ensuring that the diagonally cut corner fits neatly in the dedicated space allocation.



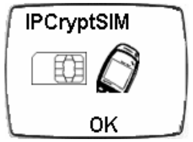


Remount the battery and the phone back cover. Switch on your phone and enter the personal identification number (PIN) that was supplied with your **IPCryptSIM**^{TM}. You now can scroll through your phone's menu until you find the **IPCrytSIM**^{TM} menu. Press ***OK**** to access the **IPCryptSIM**^{TM} functions. You are now ready to operate the **IPCryptSIM**^{TM} and to prepare your mobile phone to become you most secure means of SMS text message communication.

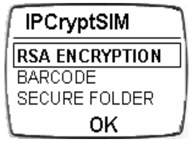
We like to congratulate you for your choice and foresight to make your SMS message communication completely safe, private and confidential!

* Some mobile phone models use the command ***Select*** instead of ***OK***.

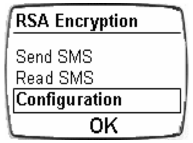
Change your IPCryptSIM^{TM} PIN



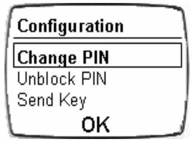
The first time you access your **IPCryptSIM**^{TM} secured mobile phone your PIN you will be asked to access your mobile phone is ***1234***. It is recommended that the first task you should do is to change your PIN.



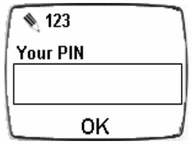
Select the **IPCryptSIM**^{TM} menu and press ***OK****.*



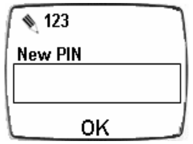
Select ***RSA ENCRYPTION*** tap and press ***OK****.*



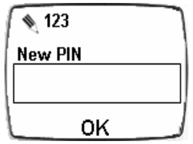
Select the ***Configuration*** tap and press ***OK****.



Select the ***Change PIN*** tap and press ***OK****.

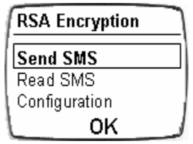


Tap ***1234*** and press ***OK****.



You will be prompted on the ***New PIN*** screen to enter your chosen, personalized PIN. Once done click ***OK****. A screen ***Please Wait*** will appear for a second while the **IPCryptSIM**TM registers your new PIN.

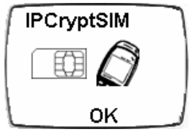
You will be prompted on reconfirm your chosen, personalized PIN. Once done click ***OK****. A screen ***Please Wait*** will appear for a second while the **IPCryptSIM**TM confirms its new settings.



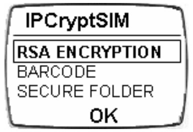
This will return you to the ***RSA Encryption*** menu and your mobile phone is now ready for use.

* Some mobile phone models use the command ***Select*** instead of ***OK***.

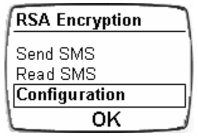
Send your IPCryptSIM^{TM} Key



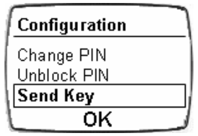
Sending secure / encrypted SMS text messages requires an exchange of encryption keys with the persons or corporations you want to communicate securely with.
Your **IPCryptSIM**^{TM} *was* equipped with your own digital keys. Whereas one, which we call *Private Key*, is securely stored in your **IPCryptSIM**^{TM} chip and can not be moved, the second key, which we call *Public Key*, has to be exchanged with those you want to communicate with. To do this, select the **IPCryptSIM** menu of your mobile phone and press ***OK****.



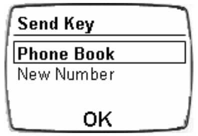
Select ***RSA ENCRYPTION*** tap and press ***OK****.*

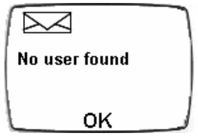


Select the ***Configuration*** tap and press ***OK****.

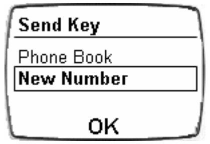


Select the ***Send Key*** tap and press ***OK****.

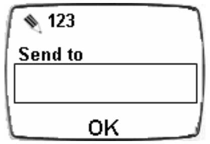




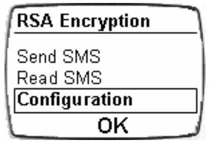
You will now be asked to select the ***Phone Book*** (Key Store) or ***New Number***. For the first time, your **IPCryptSIM**^{TM} phone book will be empty. If you select it and press ***OK****, you most likely will be receive a screen showing ***No user found***.



Select the ***New Number*** tap and press ***OK****.



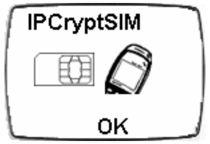
Enter the mobile phone number of the person you want to send your *Public Key* to and press ***OK****. Automatically an encrypted SMS text message will be sent to the selected person, who, then can start sending you encrypted SMS text messages. However, since you might want to send encrypted SMS text messages to this person as well, ask this person to send you his Public Key as well.



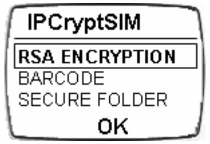
Pressing ***OK**** will return you to the ***RSA Encryption*** menu.

* Some mobile phone models use the command ***Select*** instead of ***OK***.

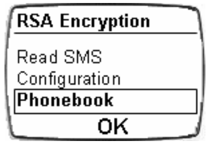
Receive and save a IPCryptSIM^{TM} Key



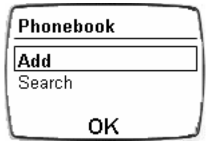
As mentioned before, sending secure / encrypted SMS text messages requires an exchange of encryption keys with the persons or corporations you want to communicate securely with. You will receive the *Public Key* from the person(s) who want to communicate securely with you. This key exchange is a one-time function and you need to store these keys in you **IPCryptSIM**^{TM} *phone book*. When you receive an encrypted message with the Public Key from a person select the **IPCryptSIM** menu of your mobile phone and press ***OK****.



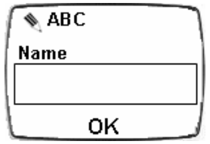
Select ***RSA ENCRYPTION*** tap and press ***OK****.*



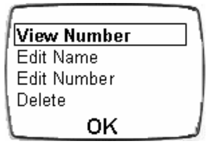
Select the ***Phonebook*** tap and press ***OK****.



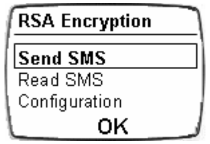
Select the ***Add*** tap and press ***OK****.



You will now be asked to enter the name of the person who sent you his/her *Public Key*. Tap in the name and press ***OK****.
Select the ***New Number*** tap and press ***OK*****.



At any time thereafter you can administer your Phonebook / Key Store, view or change numbers and names, or delete a selected one.

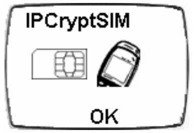


Pressing ***OK**** will return you to the ***RSA Encryption*** menu.

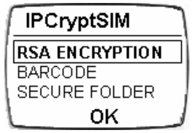
You are now ready to exchange (send and receive) encrypted SMS text messages with the other person.!

* Some mobile phone models use the command ***Select*** instead of ***OK***.

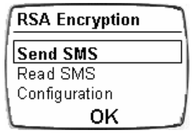
Write and Send a secure SMS



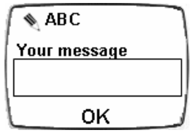
To write or to reply to a previously received secure SMS is easy.
Select the **IPCryptSIM**^{TM} menu and press ***OK*****.*



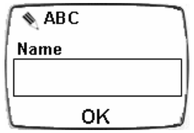
Select ***RSA ENCRYPTION*** tap and press ***OK****.



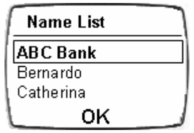
Select ***Send SMS*** tap and press ***OK****.



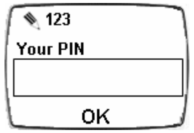
Tap in the message body you want to send. You can write like in a normal SMS up to 160 characters. For added security your SMS will be sent in 2 parts and only the receiving mobile device during decryption will assemble the 2 parts to one SMS text body. Once you fnished composing your SMS click ***OK****.



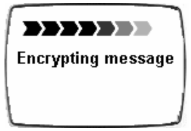
The Phone Book / Key Store opens and you have to stored name of the recipient. This name is linked to the recipient's mobile number and his/her encryption key.

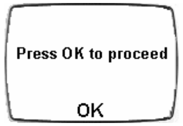


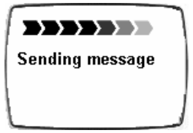
Select the name of the recipient and press ***OK****.



As and added security feature you will be prompted to enter y**our PIN** which is your personal identification number and is required before the written text is encrypted. Only this way you can ensure that only you can send encrypted SMS from your mobile phone. Press → ***OK***.







You will see a confirmation box that the SMS has been encrypted. You will be prompted to press ***OK*** and the SMS will be sent.

* Some mobile phone models use the command ***Select*** instead of ***OK***.

What happens hen you encrypt you SMS?

Your **IPCryptSIM**^{TM} enabled SIM card offers you the security of a 128bit RSA algorithm, to encrypt your SMS text message. This is a military grade security algorithm that turns your SMS text message in something similar to this:

```
0
Mj4*L@UlyTOØ&7oæ*æ.HxQB0s!oKF$oA%N>ö,Lu,
8ΘiKOöuäβØléiul*d$A,3òVt28Ξhl'xΔβh7+ròWCÆæ
;
----------------------------------------------------------------------
0
Mj4JL@u Δ%1gNØV cää0éL|S§6Ň:Cxtlc@a)#y7
héΦ%!ki(zΦfu5b5ÆÆ0-*&d/y^æ-ΞΣ£?dia)A*zo£
;
```

This is the encryption of the word *Hello* alone. As mentioned afore, your encrypted SMS will be sent in 2 parts and can only be assembled on the recipient's mobile phone.

With today's technological advancement, it would require the world's largest super-computer in the excess of 3,000 years to break you personal encryption key. Imagine your **IPCryptSIM**^{TM} key of 128bit has a combination of 10^{128} possibilities, that is equal to 10 followed by 128 "0"!

To make it even more difficult, in the unlikely event that you have your mobile phone stolen, while in the active mode, your **IPCryptSIM**^{TM} is secured with your personal identification number (PIN) which is programmed to block access after 10 tries. Once blocked, it will require your 8-digit personal unblocking key (PUK) to unblock it. Your 8-digit PUK has a number combination of 10^8 or 1,000,000,000 (1 billion) combinations!

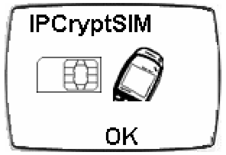
It is no wonder that with this type of strongest SMS security even the financial institutions / banks worldwide are excited to offer mobile banking services. Can you imagine you to be sitting in a traffic jam or standing in front of a sales counter and wanting to know your latest bank balance? With **IPCryptSIM**^{TM}, this is just a short encrypted SMS away. Within seconds your bank could respond to you with a secure SMS letting you know the answer to this.

IPCryptSIM^{TM} assures you the privacy and confidentiality to communicate any time and from any where. Its principal security function is based on an exchange of digital keys required to encrypt and decrypt SMS text messages. In the previous pages we asked you to exchange (send and receive) a Public Key with the mobile phone of the other person you want to communicate with in utmost security. With these simple steps you now set your mobile phone to one of the most secure personal devices you use in your daily active life!

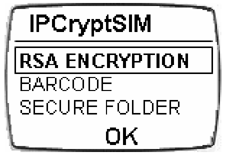
* Some mobile phone models use the command ***Select*** instead of ***OK***.

Receive and Read a secure SMS

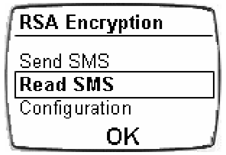
When an incoming **IPCryptSIM**TM encrypted SMS text message arrives, it will appear in the standard mobile phone ***Message*** list.



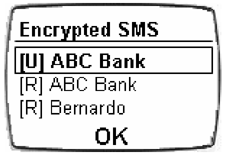
You can view messages in the list by tapping them. They will, however, show up in their encrypted form and are completely meaningless. This is to ensure that unauthorized access to your mobile phone does not allow reading these secure SMS text messages.



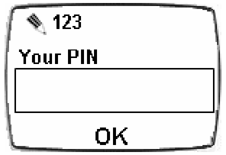
To decrypt them, select the ***IPCryptSIM*** menu followed by ***RSA ENCRYPTION*** menu. Press ***OK****.



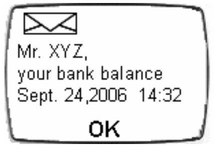
Select ***Read SMS*** and press ***OK****.



Select the SMS text message you want to access. All unread message show a ***[U]*** "unread" indicator in front of the message sender's name. Already read messages show a ***[R]*** indicator in front of the sender's name. Press ***OK****.

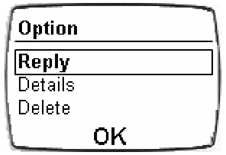


You will be prompted to tab in your PIN (personal identification number) in the ***Your PIN*** field, then press ***OK****, and the message will decrypt. This may take a split second and you may see a Please Wait screen, which automatically clears after the **IPCryptSIM**TM has decrypted the secure SMS text message.



Mr. XYZ,
your bank balance
Sept. 24,2006 14:32

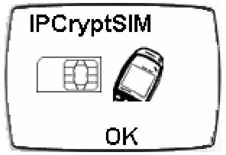
After you have read the decrypted message press ***OK****.



The ***Option*** menu allows you to either ***Reply***, check for message ***Details*** (date and time), ***Delete*** the message. If you want to keep the message select ***Back*** and press ***OK****. The SMS text message will then be stored in its secure, encrypted form on your mobile phone.

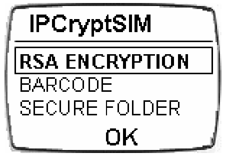
* Some mobile phone models use the command ***Select*** instead of ***OK***.

Unblock your IPCryptSIM™ PIN

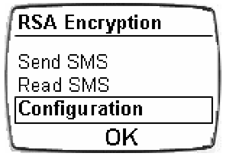


Your **IPCryptSIM**™ has an added security feature that will block access to encrypted messages if you tap in a wrong PIN 10 times. This is to ensure that nobody but you have access to your secure SMS text messages.

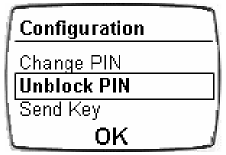
If your PIN is blocked, select the **IPCryptSIM**™ menu and press ***OK****.*



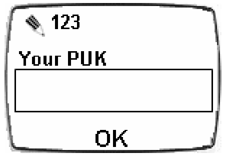
Select ***RSA ENCRYPTION*** tap and press ***OK****.*



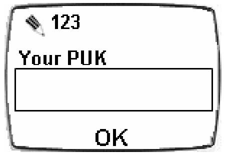
Select the ***Configuration*** tap and press ***OK****.



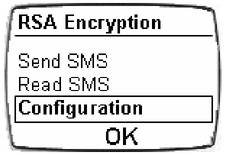
Select the ***Unblock PIN*** tap and press ***OK****.



You then will be prompted to enter your 8-digit PUK (personal unblocking key), which was given to you with your SIM card. Press ***OK****. A short ***Please Wait*** screen will show up while your SIM card processes the request



This procedure will be repeated a second time. Tap in your 8-digit PUK once more and press ***OK****.



As your access to your secure SMS text messages will be unblocked the menu returns to RSA Encryption and is ready for sending or reading secure SMS. If you want to exit from the menu press ***OK****.

* Some mobile phone models use the command ***Select*** instead of ***OK***.

IPCS Group

SECURING m-COMMERCE
FOR EVERY MOBILE PHONE

THANK YU FOR CHOOSING IPCryptSIM™

Should you have any questions or comments, we would love to hear from you!

Kindly contact the nearest office of IPCS Group. We guarantee your satisfaction!

IPCS Group

IPCS Ltd.

13/F, Silver Fortune Plaza
1 Wellington Street, Central, Hong Kong
Tel: (852) 2525 7718 Fax: (852) 2140 6833

IPCS Group, Inc.

Unit 12C, 12/F, Goldland Tower, 10, Eisenhower St.,
Greenhills, San Juan, 1503 Metro Manila, Philippines
Tel: (63 2) 7235771, 3961061 Fax: (63 2) 6473499

BICS Sdn. Bhd.

8.01, Level 8, AMODA Building,
22, Jalan Imbi, 55100 Kuala Lumpur, Malaysia
Tel.: 60 3 2144 7000 Fax.: 60 3 2144 8959

MSC-Status Company