

IPCS Group

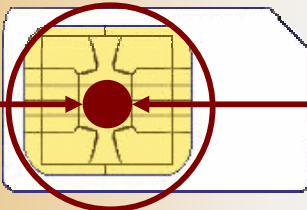
Contending with Today's Leading Data Threats
in Electronic and Mobile Commerce



SMS Encryption



We embedded our digital
PKI keys for encryption



Java-based crypto engine

Encrypted SMS is becoming increasingly important as the examples of SMS intrusion, snooping, and interception multiply.

You probably heard the stories, and may have even read the published transcripts, of intercepted and incriminating mobile phone text messages sent between famous and notorious alike. Everyone loves Short Message Service (SMS). These small email-like notes are discreet, direct, and instantaneous; the required infrastructure has been well established. However the contents of SMS messages are known to the network operator's systems and personnel. Therefore, SMS, at a first glance would not offer an appropriate technology for secure communications. Most users do not realise how easy it may be to intercept.

Encrypting the text body of a SMS is the answer to safeguard confidential information from unauthorized access. SMS encryption is no longer new. However, until now SMS encryption has been developed for the upmarket Java-based Smart Phones and PDAs only, leaving all simpler / cheaper GSM mobile phone users unprotected.

IPCryptSIM™ is the answer to secure communication

All mobile devices, whatever type, brand or model, use a SIM card to operate. Without it you would not be able to switch on your mobile device. The SIM card is the only part of the operator's network that connects and authenticates the subscriber to the network.

IPCryptSIM™ resides on the SIM card of every type of mobile device to allow you to secure SMS messages. Its ease of use interface offers a simplified method of data input to make it a "simple-click operation" with remarkable user friendliness.

Using SMS for secure communication, users are looking for confidentiality and integrity of the message. Authentication is achieved by simply looking at the message itself, which includes the sender's phone number. Encrypting the message provides confidentiality, and the integrity of a non-tampered with SMS is guaranteed since no one else but the SMS recipient's mobile device has the digital key to decrypt the message. Even if a secure SMS is intercepted (or stored in the telco's database servers and can be accessed by the telco), no one can make sense of the SMS message as it is displayed in encrypted form thus no one can make changes to its text contents.

The required Public Key Infrastructure (PKI) can be uploaded through a normal SMS transmission over-the-air (OTA), is self-extracting and generates the digital keys on board of the Java-based SIM card. Key security meets the most stringent demands.

IPCryptSIM™ facilitated the exchange of private, snooper-free text. IPCryptSIM™ can keep eavesdroppers, intruders, paparazzi, stalkers, and other "monitors" out of your business. IPCryptSIM™ combines the discretion and mobility of "texting" with the privacy and security of modern cryptography.

IPCryptSIM™ uses an asymmetric RSA encryption algorithm and offers a 1,024-bit key length with a 128-bit encryption.

With these highest security standards, an all social levels reach and ease-of-use for a use anytime-anywhere, IPCryptSIM™ is today's single answer for completely secure communication between all types of mobile devices.

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

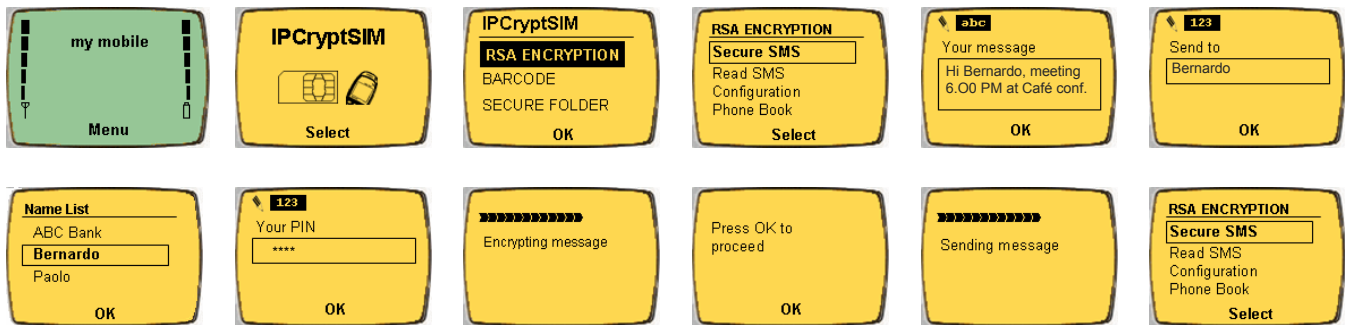
BICS Sdn. Bhd.

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



Secure SMS Communication

IPCryptSIM™ combines the discretion and mobility of "texting" with the privacy and security of modern cryptography. Even operating your bank account using IPCryptSIM™ is quickly turning into the only secure platform for mobile banking.



IPCryptSIM™ 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.

When using the IPCryptSIM™ m-banking service, the customer sends an encrypted text message (SMS), requesting the bank that he wishes to view his account balance, control account movements, make a payment or simply administer his account. He receives an encrypted text message on his/her mobile phone with the requested details. The SMS is sent from the bank's GSM Mobile Payment server. After this, the customer uses his personal password, which is chosen when registering as service user to decrypt the message. In case of a payment, the chosen account is charged and payment transferred to the merchant.

IPCryptSIM™ Highlights

Consolidated Identity: A user's private keys, passwords, and profiles for access to network services are contained in a SIM card;

Ease-of-Use: User simply installs the SIM card into the mobile device and selects 'CryptSIM™' functionality to send a secure SMS;

Chip-Based Technology: Offers the functionality and security of a multi-application smart card. PKI keys are generated on board the SIM card (Java-enabled hardware token);

Strong Authentication: RSA algorithm with 128bit encryption strength based on 1,024bit key length;

Enhanced PKI: Secure digital certificate management and key storage occur in the protected environment of the mobile device itself for increased security, mobility, and confidence.

Receive/Decrypt a IPCryptSIM™

When an incoming IPCryptSIM™ arrives, it will appear in the message list. You can view messages in the list by tapping them. If they have not been decrypted yet, the password field will become active. Tap in your personal identification number (**PIN**) then hit OK, and the message will decrypt.

Replying to a IPCryptSIM™

To reply to a previously received IPCryptSIM™, select the message you want to respond to, then tap **Message > Reply**. The CryptSIM™ form will appear. Tap in the message body you want to send, then click **OK**. The Phone Book / Key Store opens and you select the digital key of the recipient. Click **Select**. You will be prompted to enter your PIN. As described above, you will see a confirmation box when the message has been sent.

Saving the IPCryptSIM™ list

In normal operation, messages are saved in transient memory, and the message list is changed with a prefix **R** (read). The SMS is saved as an encrypted file. This file encapsulates the current message, and can be decrypted later using the same password. This is the preferred method for saving IPCryptSIM™ messages.

Be that as it may, there are times when you want to leave something behind, when you need to save a conversation or pass some info to another program. You can save a plain text copy of the current message as an unencrypted text file.

Since this procedure saves a visible copy of the IPCryptSIM™ messages, it should normally be avoided and used only when absolutely necessary.



IPCryptSIM™ is a trademark of IPCS Ltd.
© IPCS Ltd. 2006 - All rights reserved -

Short Message Service (SMS) has grown in popularity over the years and it has become a common way of communication. SMS is usually used to transport unclassified information, but with the rise of mobile commerce it has become a popular tool for transmitting sensitive information between mobile users. By default SMS does not guarantee confidentiality and integrity to the message content. Therefore SMS is not totally secure and reliable. IPCryptSIM™ is today's single answer for completely secure communication between all types of mobile devices combining the discretion and mobility of "texting" with the privacy and security of modern cryptography