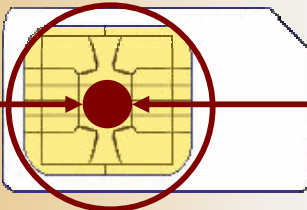


Secure Mobile Banking through SMS encryption



We embedded our digital
PKI keys for encryption



Java-based crypto engine

Financial services organizations face a new strategic challenge, m-commerce. The wireless channels being created by the collision of the mobile and Internet technologies, are opening up a new landscape of threats and opportunities. Mobile payment is using the mobile phone at the point-of-sale instead of using credit or debit cards. This provides an unparalleled shopping experience combining ease with flexibility.

The future of m-commerce will be determined by m-payments success

Before mobile commerce is taken up by the mass market, three pivotal components must be in place.

1. A robust infrastructure must be developed to allow transactions between the buyer and seller in return for goods and services.
2. To reach the widest consumer group requires to enable all types of mobile phones the traditional GSM phones as well as the newer Java / Smart phones (GPRS, 3G, Edge, ...).
3. Security is critical to consumer confidence, as e-commerce experience confirmed. Without secure payments systems, customers stay away. Creating security standards is therefore key to the development of m-commerce. Digital signatures can also boost customer confidence by making transactions secure, helping to stem the rising tide of fraud on the net.

IPCryptSIM™ is the answer to secure mobile banking

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.

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™ facilitates the exchange of private, secure SMS text messages. 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.

Given the success of recent mobile banking deployments world-wide, it is evident that consumers have a strong 'appetite' for being able to interact with their banks via their mobile phone provided that strong authentication and SMS encryption ensure privacy/confidentiality and integrity of the text communication.

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 mobile banking.

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



CryptSIM™ combines the discretion and mobility of "texting" with the privacy and security of modern cryptography.



IPCryptSIM™ messages are sent / received via the standard Short Message Service mechanisms. As a consequence, they are billed at the usual 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.

Mobile banking from the customer's perspective

As a mobile banking customer, you can link your mobile device to any of your financial accounts. With just a few clicks on your cell phone, you can pay for purchases at stores, shop online, pay monthly bills - even transfer money from one account (or person) to another. Mobile banking is a simple, secure, and convenient way to handle your finances.

Mobile Payments

Writing checks and buying stamps was once considered novel. Now mobile banking opens the next page into the future. With your mobile device you can pay your monthly bills, anywhere, any time.

Account Selection

Link yourself instantly to multiple financial accounts. Credit card accounts (Visa, MasterCard, American Express, and more), debit card accounts, checking accounts... it's up to you. Mobile banking services of your bank can handle them all. All you need to do at checkout time is select which account to charge, send an encrypted SMS instruction to your bank and authorize the payment.

IPCryptSIM™ use-cases in m-banking

- | | |
|---|---|
| <p>Use case 1:
Request of account balance.</p> | <p>The user is in a mobile situation (e.g. in a department store) and intends to know his account balance, e.g. to verify his account before realizing a spontaneous purchase.
Resulting need: <u>Quick obtainment of account balance.</u></p> |
| <p>Use case 2:
Control of account movements.</p> | <p>The user is waiting for an important cash receipt on his account. He intends to have the exact details of the cash receipt.
Resulting need: <u>Continuous control over movements on the account.</u></p> |
| <p>Use case 3:
Instant payment.</p> | <p>The user is in a mobile situation and intends to make a payment by bank transfer from his account.
Resulting need: <u>Instant execution of a bank transfer.</u></p> |
| <p>Use case 4:
2nd factor authentication for e-banking Internet access.</p> | <p>The user accesses the bank's Web site via a PC. For security purpose, the bank requires a 2nd factor authentication before user can access account details.
Resulting need: <u>Bank sends an encrypted SMS containing the TAN to user's mobile, who then copies the TAN into the log in Web page.</u></p> |

CryptSIM™ Highlights

1. **Consolidated Identity:** A user's private keys, passwords, and profiles for access to network services are contained in a SIM card;
2. **Ease-of-Use:** User simply installs the SIM card into the mobile device and selects "IPCryptSIM" functionality to send a secure SMS;
3. **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);
4. **Strong Authentication:** RSA algorithm, 128bit encryption strength based on 1,024bit key length;
5. **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.

