

# ENTERPRISE WIDE SECURE & TRUSTED SMS MESSAGING



## XMS MANAGER

Besides social communications between users, SMS Messaging is increasingly being used in innovative ways: –

- to contact employees (as notification pagers)
- to schedule appointments (as a tool for scheduling)
- for having non invasive communication in meetings (one way message)
- for sending short reports in field operations (confirmation, findings)
- internal organizational notifications (bulk message notification to employees)
- for requesting and passing brief urgently required business information (sales quotes etc.)
- for communicating sale purchase decisions with agent / broker while in meetings (sell / buy stock)

80% of the 1 billion mobile users worldwide do not leave home without their phones as the desire to communicate more easily and have more timely access to information is universal.

Mobile usage is soaring as businesses increasingly turn to the mobile phone to “get the message across” anywhere anytime.

The mobile phone today is being adopted in diverse and innovative ways to enhance business productivity and SMS is playing a leading role in this adoption.

**How secure** is the SMS messaging medium? Can you trust this medium to send in a sales quote or sensitive information? It is possible to get a sneak preview of messages on a colleague’s handset left on the desk during a coffee break.

In the past, social engineering attacks on servers at the SMS gateway left SMS messages vulnerable to theft and espionage.

## YOU NEED

### Confidentiality

Through key based encryption

How do I know the message from the boss (or the Cabinet Secretary) to me (or to the Under Secretary) is in fact **authentic**? Today, it is possible to spoof the identity of the sender of an SMS message using free software on the internet. The message ostensibly from your boss could actually be maliciously sent to you by a prankster.

### Non Repudiation

Signed & Secure messages

Digital signatures built into the product enable Government officials or business users to trust the **source** of their SMS messages.

### Integrity

Messages are tamper proof

Strong hashing algorithms serve to preserve the **integrity of the data** contained in the SMS message.

*“The mobile phone is no longer confined to the world of telecoms, or even entertainment. The mobile phone is now truly open for business – for all companies who understand how being on the mobile will provide an important part of their future growth and productivity gains.”*

“The Mobile is open for business” Netsize Guide 2005 sponsored by Mobile Data Association and 3GSM Association



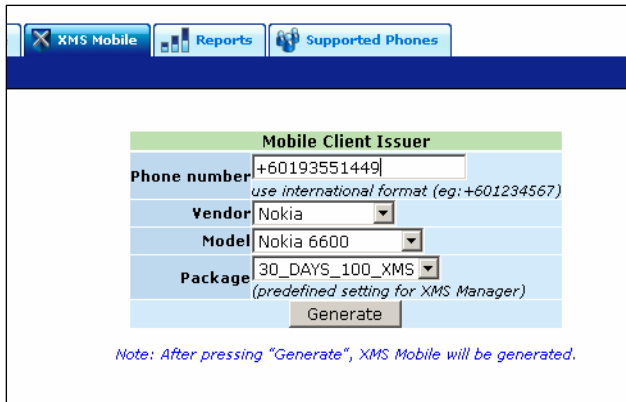
**XMS Manager** is a Web based management interface which will enable an organization to issue XMS Mobile applications.

Be they government departments, Small Medium Enterprises (SMEs) or large multinational corporations, XMS Manager allows the organization to issue and manage XMS Mobile application to any number of their staff across locations worldwide.

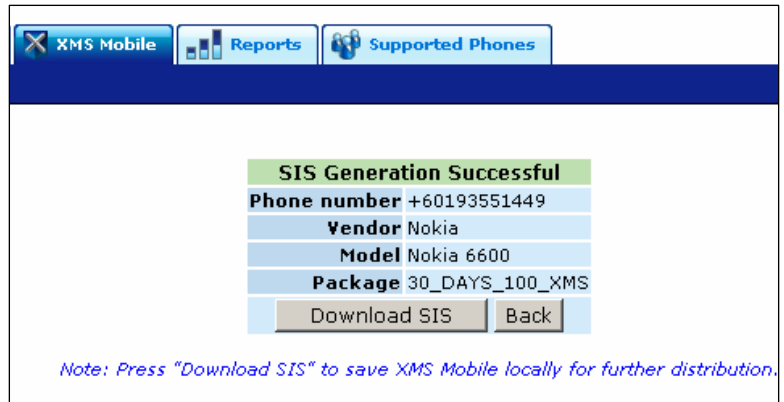
These secure messaging applications can be installed on supported mobile handsets and works across countries, different cellular providers and diverse technologies (GSM, CDMA etc).

It provides a truly autonomous and scalable means of rolling out XMS Mobile applications to a selected, closed user group to ensure true end to end secure mobile messaging.

Businesses can protect against industrial espionage & prevent information leakage by using XMS for business communications and enabling and trust within closed user groups. This technology will truly change the way we live and do business.



**Step 1 – Generation XMS Mobile**



**Step 2 – Download XMS Mobile**

The XMS Manager is a Software based application that is installed on the administrator's computer (any Windows Workstation). The administrator uses simple, intuitive steps (as shown below) to select the handset model of the users and feed in the employee's phone number. The name of the user or the phone number does not need to be shared with the cellular provider or with any other agency. This provides the organization complete privacy and control in the deployment of the XMS solution.

Having completed the Mobile Client Issuer (Ref Step 1 & 2) an installable .sis file would be generated and saved by the administrator on his computer. This file can then be transferred to the user's handset via infrared, Blue tooth or data cable. It can also be sent to the employees via email for them to download and install onto their phones via infrared, Bluetooth or data cable.



**How to use Xecure Message Services™**  
Every mobile user who requires secure communication with another mobile user needs to:

**Step 1: Both peers Download XMS**

**Step 2: Users install XMS Application**

**Step 3: Exchange XMS messages.**

<p><b>Corporate Office</b></p> <p><b>NSS MSC Sdn Bhd (624307-K)</b> Suite E-07-21, Plaza Mont Kiara, 2, Jln Kiara, 50480 Kuala Lumpur Malaysia Tel: +603 6203 5303 Fax: +603 6203 5302 Email: malaysia@mynetsec.com Website: www.mynetsec.com</p>	<p><b>Branch Offices</b></p> <p><b>India</b> Network Security Solutions (I) Ltd. <b>Pune</b> Tel: +91 20 2614 1596 / 97 Fax: +91 20 2613 6471 Email: india@mynetsec.com</p> <p><b>Delhi</b> Tel: +91 120 251 3586 Fax: +91 120 251 3345 Email: india@mynetsec.com</p>	<p><b>Singapore</b> Network Security Solutions Pte Ltd Tel: +65 6835 7139 Fax: +65 6835 7145 Email: singapore@mynetsec.com</p> <p><b>USA</b> Network Security Solutions Americas LLC Tel: +1 800 697 1884 Fax: +1 888 274 1689 Email: usa@mynetsec.com</p>
---	---	--