



XMS Manager – WHITE PAPER

Adding trust to your messages





Contents

Preface	4
Purpose of this document	4
Network Security Solutions (NSS MSC SDN BHD)	4
Document history	5
Change history	5
Product overview	6
XMS Manager – A corporate solution	7
Key functions and features	7
XMS Manager: functions and features	7
Simple XMS Mobile issuing interface	8
Executive summary and detailed reports	8
User management	9
Closed group	9
XMS Mobile: functions and features	10
Integrated messaging	10
Integrated address book	10
Intuitive message indicators	11
Resident protection	11
Transit protection	11
Technologies in detail	13
SMS	13
Using SMS scenarios	14
So much more to SMS	14
SMS Architecture	14
SMS Security issues and vulnerabilities	15
Attacks on GSM, the SMS carrier technology	16
Attacks on SMS	17
SMS Security: What is needed?	19
XMS Technology	20
XMS Technology: Specifications	20
XMS Cryptography standards	20
Key pair generation	20
Encryption	21
Digital Signing and verification	21
Hashing	21
Strength of XMS crypto technology	21
XMS Manager Specifications	22



Software Specifications	22
Minimum Hardware Specifications	22
XMS Mobile Specifications.....	22
Supported OS	22
Supported phones	22
Application size	23
XMS – Length of messages	23
Installation options	23
XMS Mobile licensing.....	23
Glossary	24



Preface

Purpose of this document

This White Paper will be published in several revisions as the product is enhanced. Therefore, some of the headings and tables below may be updated with more information. Additional information and facts will be forthcoming in later revisions. The aim of this White Paper is to give the reader an understanding of technology and its main applications, as well as the main functions and features of the product.

Note: This document contains general descriptions for this specific XMS Mobile product from Network Security Solutions (NSS MSC SDN BHD).

People who can benefit from this document include:

- Telecom service providers
- Banks, Financial services enterprise
- Government and Federal agencies
- Mobile phone SMS users

Network Security Solutions (NSS MSC SDN BHD)

The recognized worldwide leader in security consultancy, products and services, NSS MSC SDN BHD develops, markets, and supports products used by a broad installed base of enterprises, businesses, governments, individuals, and cryptography experts to secure proprietary and confidential information. During the past 5 years, NSS technology has built a global reputation for open and trusted security products. NSS recommended and developed solutions are used by hundreds of corporate/government users and millions of individual users worldwide, including many of the world's largest and most security-sensitive enterprises, government agencies, individuals, and cryptography experts. Contact NSS MSC SDN BHD at www.mynetsec.com.



Document history

Change history

15-Sept-2005	Version 1.0	First Edition
--------------	-------------	---------------

This White Paper is published by:

Network Security Solutions,

NSS MSC Sdn Bhd (624307-K),
Suite E-07-21, Plaza Mont' Kiara,
No.2 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia

Phone: +603.6203 5303

Fax: +603.6203 5302

E-mail: sales.xms@mynetsec.com

www.mynetsec.com

© Network Security Solutions, 2005. All rights reserved. You are hereby granted a license to download and/or print a copy of this document.

Any rights not expressly granted herein are reserved.

First edition (Sept 2005)

This document is published by Network Security Solutions (NSS), without any warranty*. Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to programs and/or equipment, may be made by NSS at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Printed versions are to be regarded as temporary reference copies only.

*All implied warranties, including without limitation the implied warranties of merchantability or fitness for a particular purpose, are excluded. In no event shall NSS or its licensors be liable for incidental or consequential damages of any nature, including but not limited to lost profits or commercial loss, arising out of the use of the information in this document.



Product overview

XMS Manager is a corporate solution for issuing and managing 'XMS Mobile' product for a licensed number of users. It enables an organization to manage in-house the distribution of XMS Mobile - a secure SMS messaging product. The XMS Manager comes across as a highly scalable product in terms of client licenses upgrade and 'XMS Mobile' product feature upgrade. Security is best addressed when ownership and control is in-house and XMS Manager gives all of this and more in form of management, distribution and availability of the 'XMS Mobile' product for its enterprise users.

XMS solution may be made available for distribution and sale by other external providers in the region. However, by having ownership of 'XMS Manager', organizations would not even need to share the name, mobile phone number of 'XMS Mobile' product user with a cellular provider or with any other external providers of XMS technology. This in effect provides the organization complete privacy and control in deployment of the XMS solution.

'XMS Mobile' is a software product for bringing confidentiality, integrity and non-repudiation to SMS messages. It enables user to send SMS to peers that are encrypted and optionally may be digitally signed. With the widespread acceptance of SMS as a low cost and effective means of mobile communication, the XMS Mobile product comes as an end-to-end solution for addressing the known vulnerabilities of SMS technology – namely: Spoofing, Snooping, Sniffing and interception. The mobile phone is today being adopted in innovative ways to enhance business productivity and SMS is playing a leading role in this adoption. However communication of plain text SMS over existing GSM specifications make it vulnerable for having any sort of classified information exchange or privacy of content. XMS Mobile is a powerful solution for plugging all gaps in security and trust for SMS messages.

*

Here onwards, any SMS that is composed using XMS Mobile (or XMS Technology) will be referred as XMS.

Confidentiality

Through key based encryption

For the first time a Public Key (**PK**) based encryption has been extended onto SMS.

Integrity

Messages are tamper proof

Source of SMS is ensured. For the first time, be assured of the sender's authenticity.

Non Repudiation

Signed & Secure messages

SMS can be digitally signed by your Private Key. For the first time, be contents are assured to not be tampered in transit or faked.



XMS Manager – A corporate solution

With business driving communication happening more often on the move, mobile communication has become increasingly essential for corporate world. More and more classified and business related information in form of SMS messages and contacts reside in the mobile phones with the management cadre of any Enterprise. More than 80 % of mobile users do not leave home without their phones. Businesses are increasingly turning to the mobile phone to “get the message across” to the employees anywhere anytime. The desire to communicate more easily and have more timely access to information is universal. The mobile phone is today being adopted in innovative ways to enhance business productivity and SMS is playing a leading role in this adoption.

- *How secure is the SMS messaging medium?*
- *Can one trust this medium to send in a sales quote or sensitive information?*
- *It is relatively easy to get a sneak preview of SMS messages sent, received on a colleague's handset left by the desk during a coffee break.*
- *How do I know the message from the boss (or the Cabinet Secretary) to me (or to the Under Secretary) is in fact authentic?*
- *It is very easy to spoof the identity of the sender of an SMS message using simple tools downloaded from the internet. The message apparently from your boss could actually be maliciously sent to you by a prankster!*
- *What to do about the important or classified business contacts and important or private SMS messages if my mobile phone gets stolen or misplaced?*
- *Social engineering attacks on servers at the SMS gateway have in the past left SMS messages vulnerable to theft and espionage. Is there a way I can be assured of the privacy of my SMS messages?*

XMS Manager for the corporate provides a complete solution to all the above concerns and eliminates the security vulnerabilities inherent with SMS technology. The solution not only provides assurance of security and privacy of SMS messages in transit but also protects the SMS messages and contacts resident in the mobile phone.

Key functions and features

XMS Manager: functions and features

Using the XMS manager, businesses from SMEs to large enterprises can autonomously manage and issue 'XMS Mobile' product to their employees across locations worldwide and begin to use the SMS medium for secure and trusted



business communications. Businesses can protect against industrial espionage & prevent information leakage by using XMS for corporate communication.

Summary and detailed reports of 'XMS Manager' license usage, 'XMS Mobile' distribution, license renewal and administrative features of 'XMS Manager' make the issuing and maintenance of 'XMS Mobile' product a very user friendly experience. The XMS Manager is available as a secure web interface and role based user accounts enable privileged and access controlled usage of the product.

The XMS Mobile product issued by 'XMS Manager' provides dual level protection of SMS messages. It protects resident and SMS messages in transit. Resident messages implies to SMS on the mobile phone.

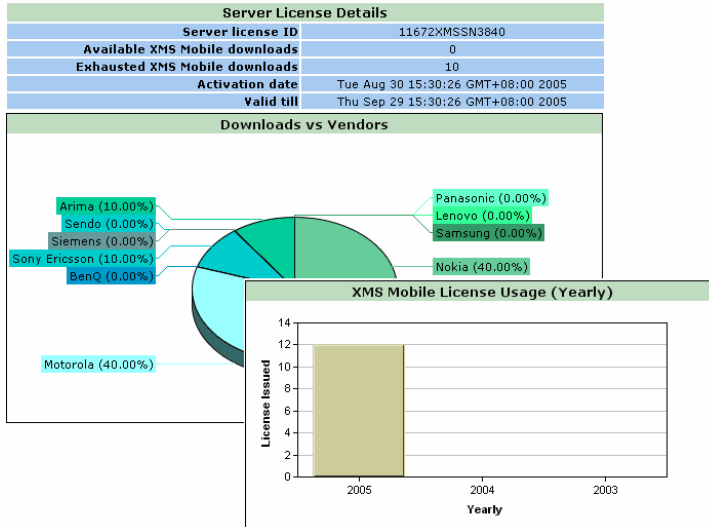
Simple XMS Mobile issuing interface

The administrator uses the simple intuitive steps (as shown below) to select the mobile phone model and input the phone number. 'XMS Mobile' is available for download, which may then be distributed by the Administrator to the end user by whichever means convenient (email, CD, floppy, ftp).

The screenshot shows two side-by-side panels of the XMS Manager web interface. The left panel is titled 'Mobile Client Issuer' and contains a form with the following fields: 'Phone number' (input: +60193551449), 'Vendor' (dropdown: Nokia), 'Model' (dropdown: Nokia 6600), and 'Package' (dropdown: 30_DAYS_100_XMS). A 'Generate' button is at the bottom. The right panel is titled 'SIS Generation Successful' and displays the same information: 'Phone number +60193551449', 'Vendor Nokia', 'Model Nokia 6600', and 'Package 30_DAYS_100_XMS'. It includes 'Download SIS' and 'Back' buttons. A note at the bottom right reads: 'Note: Press "Download SIS" to save XMS Mobile locally for further distribution.'

Executive summary and detailed reports

The administrator of XMS Manager has access to various reports for visualizing the XMS Mobile distribution and usage. It also provides reports on license usage and this can be used for timely renewal of XMS Manager License.

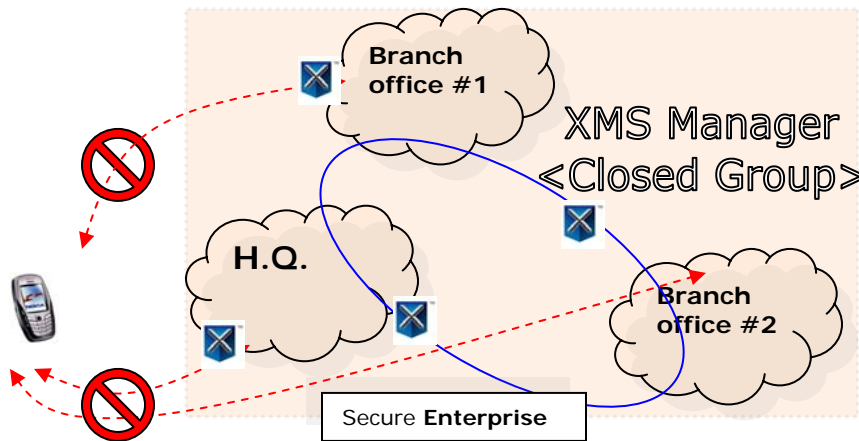


User management

Administrator of 'XMS Manager' may create multiple users accounts in the system. Roles such as 'Report Manager', 'XMS Manager' and 'Administrator' partition various privileged functions and features.

Closed group

One of the salient features of XMS Manager is the availability of a closed group feature. XMS Manager Product may be purchased with closed group capability. XMS Mobile product issued by such closed group XMS Managers will allow XMS peers only within the enterprise to exchange XMS messages. With the strength of encryption and privacy that comes along with XMS Mobile, some enterprise may find it appropriate that its user's only be able to exchange XMS messages within the Enterprise group and not with external XMS peers (not belonging to the Enterprise). This feature particularly may be of interest to federal and government organizations that cannot warrant an intended or inadvertent leakage of classified information as an XMS from an insider to some external XMS peer.



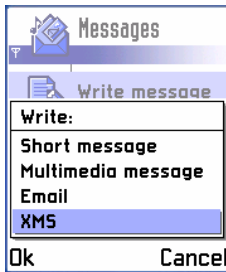
XMS Mobile: functions and features

The XMS Mobile product gets issued by the XMS Manager. The generated XMS Mobile is bound to a mobile number in its license and the product can only be activated if it is installed on mobile phone having the correct MSISDN.

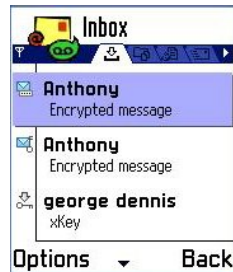
Integrated messaging

Once installed, XMS Mobile gets integrated with the default messaging system of the mobile phone. This way, user gets to see an additional option of composing XMS along with the existing MMS, SMS and E-Mail options available on the mobile phones. This provides better accessibility and easy usage of the product.

The XMS messages are accessed also the same way normal SMS are accessed by using the inbox available in the mobile phone.



Compose XMS just the way you compose SMS



Open XMS just the way you open SMS

Integrated address book

Once installed, XMS gets integrated with the default address book of the mobile phone. This way the existing contacts of the phone user, are extended as XMS contacts and the xKey* management interface is provided over the same set of native contacts.

**xKey*

The public and private key pair generated by XMS Mobile is here onwards referred as xKeys.



Select XMS recipients just the way you do for SMS

Intuitive message indicators

XMS Mobile product comes along with intuitive and descriptive icons, graphics to distinguish and make XMS messaging an easy user experience. Different icons to distinguish between an xKey, password encrypted message an xKey encrypted message and so forth.



See intuitive icons against XMS messages

Resident protection

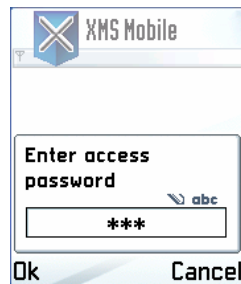
The first defense provided by XMS Mobile is protecting the messages residing on the mobile phone. Once message has reached the phone, it is vulnerable to snooping and loss in case of theft of device. The following features provide protection of the messages and address book information resident on the mobile phone.

Authentication

The authentication feature allows only authorized user to open and read the XMS* messages. This protects the messages in the mobile phone.



Click on XMS



Authenticates user

Data-Wipe

Using the optional *data-wipe* feature of XMS Mobile, in an even of theft or loss of mobile phone the user can erase his plain SMS, XMS from inbox, sent items and also erase his address book of contacts.

Transit protection



Messages leaving the mobile phone through the wireless network onto the wired network to an SMS service server or another mobile phone are protected by the following set of features provided by XMS Mobile.

xKey Encryption

XMS Mobile provides a very simple and easy to use interface to exchange your public key with other XMS peers. Once keys have been exchanged, you can send **PK** encrypted SMS (XMS) to peers.

Password Encryption

In the event that xKeys have not been exchanged by you and your XMS peer, you may optionally send a password encrypted XMS. Your peer will need to know the password to decrypt the XMS.

Digital Signing

This feature allows user to add digital signature to plain SMS. The SMS travels with the digital signature of the XMS Mobile user. The private key of XMS Mobile user is used for signing the plain text SMS message based on accepted international standards.

xKey Encryption an Digital Signing

User will be able to sign the plain text SMS data and then **PK**-encrypt the SMS also.

xKey address book

This address book integrates with default address book of the phone and shows the user a graphical interface of whose xKeys are available and whose xKeys need to be requested.

Multiple XMS recipients

XMS Mobile allows users to send XMS messages simultaneously to multiple recipients. If the message is being sent as xKey encrypted, then xKey of all added recipients should be present otherwise XMS Mobile will prompt to skip recipients whose xKey is not available. In case of password based encryption however, no such lookup of keys is done and hence no prompt whatsoever.

Closed group

An end user may be part of a closed group of XMS Mobile peers as classified during purchase or distribution or download. In this scenario, the XMS Mobile user is restricted to secure messaging only between his closed group peers. XMS Mobile messages from a closed group user to some other closed group or open group (open group XMS Mobile user do not belong to any closed group) XMS Mobile user is restricted.

Internationalization and localization

XMS Mobile supports localization. XMS Mobile can extend its features seamlessly for an international language user interface viz. Chinese, Arabic or any localization supported by the phone.

Utility functions



xKey backup and restore

To be able to change mobile phone and continue communicating with XMS Mobile peers with same xKeys. In the event of a loss of mobile phone, this feature will still enable to restore your old xKeys on new mobile phone XMS Mobile application. This feature prevents resending your new xKey to all existing XMS peers. It uses, built-in Bluetooth and Infra Red to provide the user easy and simple means of xKey backup.

Settings menu

- User gets access to change the 'Authentication' password of XMS Mobile.
- User can enable or disable the 'Data-Wipe' feature. For enabled 'Data-Wipe' feature, the pass phrase for causing the 'Data-Wipe' action can be set and reset by the user.
- User can pre configure if the XMS will be encrypted only or signed only or encrypted and signed.
- User can choose to renew XMS Mobile license if the feature is provided with downloaded copy.
- Security level in form of key lengths to be used during encryption may be set. Low, medium and high – options exist for key lengths 128, 192 and 256-bit.
- The status of current license can also be viewed. This can enable the user to know beforehand if a renewal would be required anytime soon for uninterrupted usage of XMS Mobile.

More in-phone functions

The system integration capability of XMS Mobile seamlessly makes the XMS experience just like SMS. The same SMS message alert tones and ring tones apply to XMS as well. On supporting models, XMS Mobile will extend the phone's personalized themes to its user interface making its look tune in to your moods and your set themes.

Technologies in detail

This chapter offers a detailed description of the technologies built in XMS Mobile product. XMS Mobile has been built over a broad domain of cryptography technology. The underlying wireless, SMS specifications are also detailed in this section.

SMS

Mobile usage is increasing in volume as well as diversity as the mobile phone is already an integral part of the lives of more than 1 billion people worldwide. More than 80 % of mobile users do not leave home without their phones. Businesses are increasingly turning to the mobile phone to "get the message across" to the employees anywhere anytime. The desire to communicate more easily and have more timely access to information is universal. The mobile phone is today being adopted in innovative ways to enhance business productivity and SMS is playing a leading role in this adoption.



Using SMS scenarios

SMS is having enormous popularity as an economical and convenient mode of exchanging information. It not only saves time and cost but in many situations SMS is found to be more convenient than talking on the phone. SMS has changed our working habits and social lives in many ways. SMS has simplified exchange of important short messages and also lead to creation of services that are just fun to use. People can easily share a private moment with their friends, family and work in other geographical sites in a cost effective and instant manner. SMS is further being used in business tasks such as simplifying grocery shopping, giving alert of a best buy or any monitored event. Besides that it is being used these days in getting daily NEWS, stocks information, sports scores, quotes, travel and weather news. Many value added services such as contest voting, songs request, ring tone or service initiation is being also done using SMS. There are so many services that are being churned out because of widespread acceptance of SMS that it just cannot be summarized.

So much more to SMS

Many know today that SMS travels as plain text and privacy of the contents of SMS cannot be guaranteed. Individuals are more and more getting skeptical of using SMS for sensitive and personal message exchange. The same reason prevents Further with growing awareness of underlying security gaps in SMS, many value adding business services are not being rolled out for end users.

SMS services provided either by vendors or banks or other business house are mostly passive in nature. The SMS is not accepted to cause an active transaction. The underlying gaps in security and vulnerabilities that are inherent with SMS are the cause for of lack of such services. Gradual change and demand of active SMS based services can be met only by a solution that can address in an end-to-end manner security issues existing with SMS technology.

There are so many active SMS services that can be brought to users at a personal and at business front of SMS messaging:

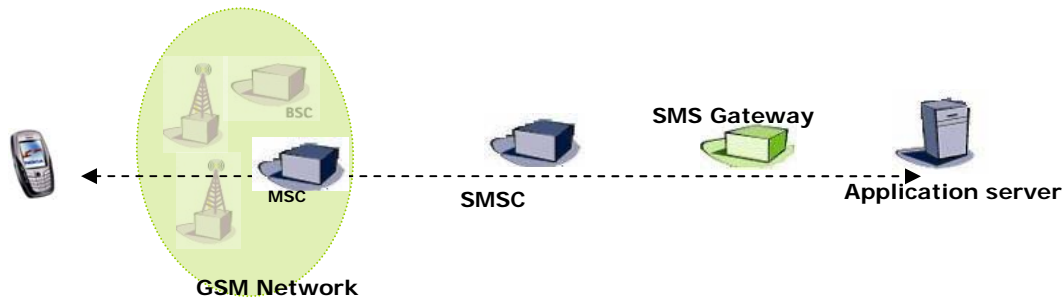
- Banking: Check balances, transfer funds between accounts, pay bills using credit cards. VAS valuable not only for the subscriber but also for financial institutions offering this service.
- Customer service: charge a customer's credit card right at the table, at any time, instead of going to a fixed POS terminal located by the register.
- Track the location of a moving asset. Interchange small amounts of information in an inexpensive manner, such as the longitude and latitude, current time, and perhaps parameters like temperature or humidity.
- Home security, vehicle security – Alerts and notifications in event of a break in.

SMS Architecture

Short messages are delivered in GSM signaling channels between the MS and the BSS. The messages flow as normal calls, but they are routed from the MSC to a

short message service center (SMSC). The SMSC stores the message until it can be delivered to the recipient(s) or until the message's validity time has elapsed. The recipient can be a normal MS user or a SMS gateway. The gateways are servers, which are connected to one or more SMSC's to provide SMS applications for the MS users. These applications include ring tone and icon delivery, entertainment, bank services, and many other beneficial services.

Following figure shows the positions of the components mentioned in this subsection.



SMS Security issues and vulnerabilities

Two important points for anyone using consumer technologies such as SMS for business purposes:

- SMS is not a secure environment.
- Breaching security often occurs more easily by concentrating on people rather than technology.

The contents of SMS messages are known to the network operator's systems and personnel. Therefore, SMS is not an appropriate technology for secure communications. Most users do not realize how easy it may be to intercept. Even though it would likely be a relatively complex to hack into telecom providers systems from an external source to obtain the content of SMS messages but finding staff privileged to look at the SMS messages and persuading them to reveal the contents is much proves easier. Gartner has already expressed reservations about security in U.K. trials of SMS voting in local elections held in May 2002. Enterprises, including governments, should not use SMS for any confidential communication. Enterprises seeking secure communication channels to mobile employees should consider encrypted end-to-end solutions on devices having additional security features.

The underlying specifications and technology for SMS transmission leaves many security gaps. These gaps make SMS vulnerable to –

Snooping

On device, at the store and forward network elements

SMS Interception

Over the air, in wired network



Spoofing

Using commercial tools, own SMS gateway

Modification

Using conventional hacking techniques

Attacks on GSM, the SMS carrier technology

Often the weakest link of security is the mobile phone itself. Even leaving the mobile phone unattended inadvertently could cause your private and confidential messages vulnerable to **snooping**. The above could be described in simple was such as the ease of getting a sneak preview of the messages and contacts on a colleague's handset left on desk during a coffee break! A stolen SIM not protected by a security, PIN code may reveal all messages and contacts that were stored in the SIM memory. This appears another convenient means to **snoop** if the mobile phone or SIM is compromised.

There are several ways of eavesdropping on a call, although it is not so easy to eavesdrop on real time calls. There are different attacks against the A5/1 algorithm, which is the algorithm used to cryptographically protect the voice, data (SMS) and signaling. A5/2 also exists, and it is even weaker than A5/1. The attacks include a brute force attack, which is quite time consuming and thus cannot be used in real time. Another attack is called divide and conquer. Although more efficient, this attack is neither fast enough to be implemented in real time. Third attack is called biased birthday attack, which can be implemented in seconds with a PC, although 2 or more minutes of GSM voice/data (SMS) stream must be recorded first. A random sub graph attack can be done in 4 minutes with a PC, and it only needs about 2 seconds of GSM voice stream recorded. The A5/1 algorithm can even be reversed and a secret called session key can be recovered. All the previously described attacks compromise the actual A5/1 algorithm. Anyway, there are other ways of eavesdropping GSM calls. The calls are only encrypted and decrypted between the BTS and the MS, leaving the rest of the network quite unprotected. If an intruder gets access to the SS7 network, which is used in the GSM operator's network, all the call and signaling traffic is completely unprotected. An attacker might also get access to the HLR, which is normally better protected, but is an attractive target for an intruder, since it contains all the subscriber information. Another possibility of eavesdropping GSM calls is to find out the secret of a subscriber, on which the whole GSM security system is based. This key can be recovered many ways. One can use a SIM card reader and a PC to send a huge amount of challenges to the SIM card of the victim. The SIM card generates responses to all of the challenges. When enough challenges are received, the key can be deduced, and the whole subscriber account is compromised. The same attack may be possible even over the air. A third possibility would be to make requests to the AC and constructing the key from the responses of the AC. The above limitations of GSM security could lead to of compromise of the carrier technology thereby also leaving SMS vulnerable to **snooping** and **interception**.

Stealing Mobile Stations:

One problem, which is characteristic of mobile networks, is that mobile devices are easy to steal. It is very common, that mobile phones are stolen and then either sold to third parties or used until the customer account is switched off by the operator. The current approach to prevent stealing GSM phones is the use of EIR, the equipment identity register. When a mobile phone registers itself to a GSM network,



it sends a special identity number of the phone device, International Mobile Equipment Identifier (IMEI), to the GSM network. This identity number is then checked against the EIR, which is a database including black, grey and white lists. Black lists include identity numbers of stolen or faulty equipment. If the identity number is on the black list, the device is not provided access to the GSM network. Grey lists include identity numbers of devices that must be tracked. White lists include ranges of identity numbers, which are granted access to the network, and they are not suspected of anything. As mentioned earlier, EIR is an optional part of the GSM standard. While it would be a powerful method to make stealing less useful, it is not used by many operators, since it is optional. This is why there might be some business opportunities in selling other ways of protecting the mobile devices from stealth. In addition to stealing mobile phones for unauthorized calls, modern mobile devices may attract thieves for **snooping** confidential content. Since some of the devices are more than just phones today, the phone owners may store important secrets into their mobile devices' memories. Also, a mobile device may be used as a means of payment. These extra threats provide further need for a good protection against theft. At least big companies could pay some extra for the additional security achieved by new inventions in this domain.

Attacks on SMS

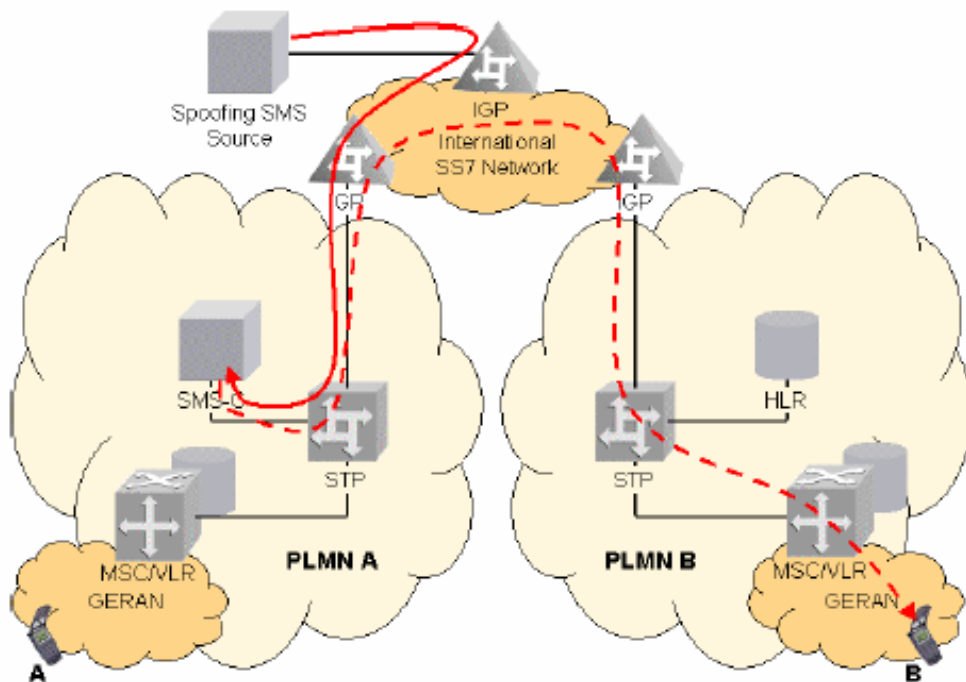
The connection between the SMSC and the SMS gateway is not part of the GSM standard. There are many different protocols available for use between the SMSC and the gateway. These protocols are built on normal protocols familiar from internets, such as TCP/IP and X.25. Also, the connections are not part of the GSM network, but part of the operator's or content provider's network or, even worse, the Internet. The connections are very loosely protected. It should be obvious, that the connection is an easy target for a cracker, since the content is delivered in plain text and binary fields. Although the gateways are authenticated, in many protocols this is done using plain text header fields containing a login name and password. Using the originator IP address is not any better way of authenticating, since it is very simple to do a man-in-the-middle attack against TCP/IP and **intercept** the communication.

Naturally one can **spoof** short messages as well as traditional calls exploiting the same GSM vulnerabilities described above but there is one easier way of spoofing short messages: It is a straight consequence of the weak protection of SMSC-gateway connections. Using a normal network listener one can record the login and password fields of a message passed from a SMS gateway to a SMSC. This seems very simple but is not that easy, since normally operators run both the gateway and the SMSC behind a firewall. But this is not demanded anyhow and this is not the case every time either. This way an intruder can set up his own fake gateway that pretends to be the real gateway. This fake gateway can then send all kinds of malicious short messages to the MS users through the SMSC. Also, in many SMSC protocols the original sender of the message is identified in a specific field of the short message. Using the **spoofing** technique described above and giving a false MSISDN in that field may cause the message to look like coming from another mobile phone. That depends on the SMSC implementation, because the SMSC may be smart enough to check the sender field and ban the message, since it comes from a gateway, not from a mobile phone. One possibility is to spoof the other way around, since the SMSC is not authenticated. This client authentication provides an attacker a chance to make a SMSC simulator to pretend to be the real SMSC. This way the gateway can be fooled and, for instance, a bank application using the

gateway could easily be made to send account information to outsiders. It could even be made to make unauthorized bank transactions.

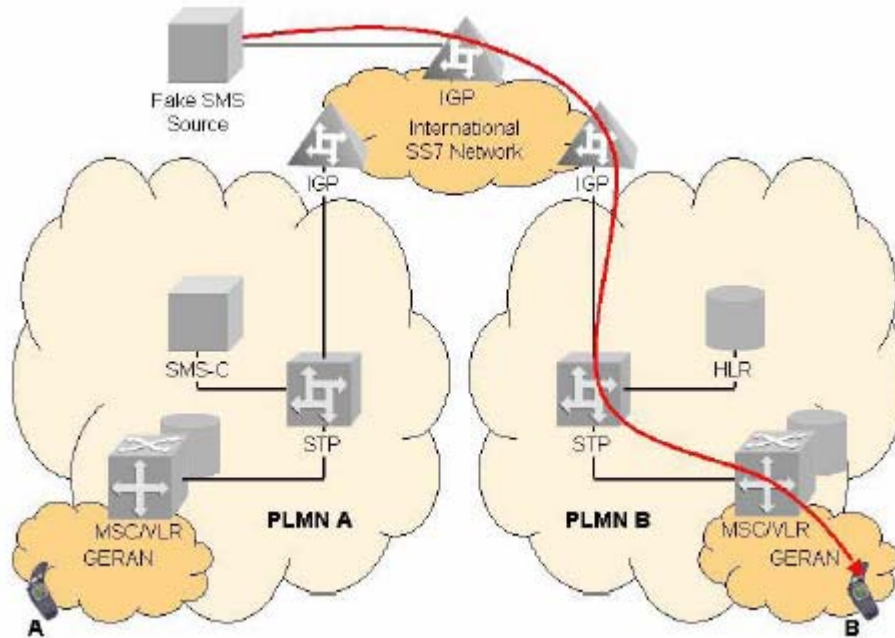
Eavesdropping and **Modifying** are possible to implement just like in the case of normal GSM phone calls. The SS7 network and the A5 algorithms are vulnerable, as was mentioned earlier. Anyway, it may be easier to eavesdrop on messages passing to and from the SMS gateway, if the connection between the SMS gateway and the SMSC is not protected. Just a normal network listener is enough. One could read all kinds of confidential information in clear text with simple software. At this point it is also possible to alter the message content, if possible check sums and field lengths are taken into account. Another part of the SMS application, which could be easily eavesdropped, is the connection between the SMS gateway and the application server. That connection is not protected in every case, either. These ways it could be possible to change sums or account numbers in a bank transaction and alter stock information broadcasted to stock service subscribers etc.

Example: SMS spoofing in a cellular provider's infrastructure



- The SMS sent to the SMS-C have a manipulated originating MSISDN A number
- One example is shown in Figure, where the "SMS Spoofing Source" simulates a roaming end-user from PLMN A, sending an SMS to a foreign end-user in PLMN B
- The "Spoofing SMS Source" is a specific system with an SS7 application. It uses real or wrong MSISDN A numbers, originating VLR and / or SCCP addresses

Example: SMS Spam in a cellular provider's infrastructure



- The Faked SMS have manipulated MAP addresses. The source address of the SMS pretends that these are sent from another network (in Figure, from PLMN A).
- To do so, it has to know the end-users' IMSI, otherwise an HLR interaction has to take place. In this case the Fake SMS Source has to use his own real SCCP and MAP SMS-C address.
- If the VLR is unknown, the source has to send the SMS to every VLR in the network, which together with the false IMSI addresses can generate a heavy load in the network equal to SMS Flooding.

SMS Security: What is needed?

Confidentiality

Through key based encryption

Integrity

Messages are tamper proof

Non Repudiation

Signed & Secure messages

An end-to-end key based encryption technology for SMS plugs the gaps in transit security of SMS. Authentication added for resident SMS security access together with encryption, address the 'Confidentiality' issue of SMS technology. Added features of message integrity and digital signing of SMS address 'Integrity' and 'Non Repudiation' for SMS technology. By having the above feature set integrated into the

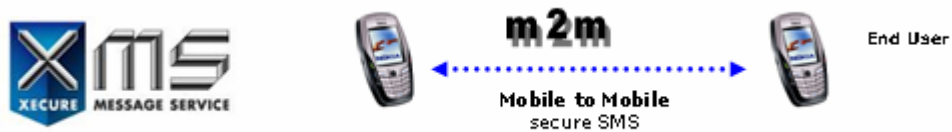


SME (smart message entities), be it mobile phones or application servers originating and/or receiving SMS messages, users can be assured completely of the security and authenticity of SMS and transactions they trigger.

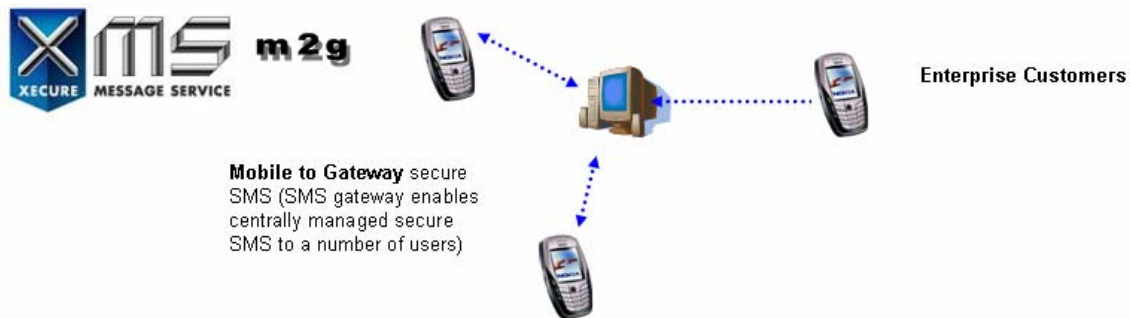
XMS Technology

XMS as a technology platform for SMS messaging, addresses in an end-to-end approach all security vulnerabilities inherent to SMS technology.

'XMS Mobile' product on mobile phone provides an end-to-end total security solution for assures messaging in a peer to peer environment.



'XMS' product suite also provides a complete security solution for 'peer to server' SMS applications. The 'XMS Business (plus)' product extends the end-to-end security solution for SMS driven business solutions.



XMS Technology: Specifications

XMS Cryptography standards

XMS technology adopts Public Key (PK) encryption standards for ciphering and digital signing. Collectively required are: a 'key pair generation' algorithm, a 'ciphering, deciphering' algorithm and 'hashing' algorithm.

Key pair generation



XMS technology uses Elliptical Curve Cryptography (ECC) for key pair generation. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the mathematics of elliptic curves. The main benefit of ECC is that under certain situations it uses smaller keys than other methods — such as RSA — while providing an equivalent or higher level of security. The ECC approach to key pair generation is best suited to mobile phones and smart mobile computing devices.

Encryption

XMS technology uses AES, short for Advanced Encryption Standard, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

XMS Mobile optionally allows users to select the size of key for encryption. Provided as 'Low', 'Medium' and 'High', an XMS Mobile may choose key length for cipher as 128, 192 or 256-bits if the downloaded copy of XMS Mobile provides this feature.

Digital Signing and verification

XMS technology uses Elliptic Curve DSA (ECDSA) for signing and verification purpose. It is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups. Superior efficiency is one reason this algorithm is preferred over DSA. DSA requires that $p > 2512$ in order to be secure against a number field sieve attack and $q > 2160$ in order to be secure against a baby-step giant-step attack.

Hashing

XMS technology uses Secure Hash Algorithm, SHA-1 for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then, for example, be input to a signature algorithm which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature. Any change to the message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

Strength of XMS crypto technology

Crypto strength of XMS technology is as strong as the strength of the above used and published crypto standards and algorithms. XMS technology uses the algorithms in their published and unaltered state.



XMS Manager Specifications

If not purchased as a box solution, XMS Manager requires a software installation and following is the software and hardware specifications for the same

Software Specifications

- *Operating System - Windows 2000 Server With updated service pack 4*
- *Browsers - Internet Explorer 6.0+, Mozilla Firefox 1.0.4+ (with updated service packs/patches)*
- *Database - MySQL 4.1*
- *Web server - Tomcat 5.0.16*
- *Java J2SE SDK 1.4.2_07*

Minimum Hardware Specifications

- *Server CPU Speed - Intel(r) Pentium(r)4 processor, 520, 2.8GHz, 1MB Cache, 800MHz FSB*
- *SINGLE processor*
- *Server Memory 512 MB RAM*
- *Network Card (NIC) Integrated Network Card Suggested INTEL/3COM*
- *Storage Type Serial ATA*
- *Hard Drive Specs 7.2k RPM drives*
- *Hard Drive Space 72.8GB*
- *Network Cabling Category 5*
- *Network Switch 100/1000 Megabit*
- *Accessories Keyboard, Mouse, CD/DVD ROM drive*

XMS Mobile Specifications

XMS Mobile product issued by XMS Manager will have following specifications:

XMS Mobile license

Supported OS

'XMS Mobile' product is compatible with mobile phones having Symbian Operating System. The Symbian phones having any of the following specifications are supported:

- *Series 60 1st Edition (Symbian OS v6.1)*
- *Series 60 2nd Edition (Symbian OS v7.0s)*
- *Series 60 2nd Edition with Feature Pack 1 (Symbian OS v7.0s enhanced)*
- *Series 60 2nd Edition with Feature Pack 2 (Symbian OS v8.0)*
- *Series 60 2nd Edition with Feature Pack 3 (Symbian OS v8.1)*
- *UIQ 2.0,*
- *UIQ 2.1*

Supported phones

Nokia 7610

Motorola A920



Nokia 6600	Motorola A1000
Nokia N-Gage QD	Motorola A925
Nokia 3660	Motorola A1010
Nokia 3620	BenQ P30
Nokia N-Gage	Sony Ericsson P910
Nokia 7650	Sony Ericsson P900
Nokia 3650	Sony Ericsson P800
Nokia 6682	Sendo X
Nokia 3230	Sendo X2
Nokia 6681	Siemens SX1
Nokia 6670	Arima U300
Nokia 6630	Panasonic X700
Nokia 6260	Panasonic X800
Nokia 6680	Lenovo P930
Nokia 6620	Samsung SGH-D710
BETA	
Nokia N70	Nokia N90

Application size

XMS Mobile for Series60: 187Kb

XMS Mobile for UIQ: 238Kb

XMS – Length of messages

The overhead of Encryption and Digital Signing of SMS will consume additional bytes apart from the size of the plain text message typed by the user. The following table highlights the space consumption has incurred by XMS technology:

Category	SMS*	XMS*			
		Short Message	Encrypt	Encrypt and Sign	Sign only
Default messaging (English and special characters)	160	160	108	61	66
Localized messaging (e.g. Chinese, Arabic etc.)	70	70	55	31	33

* The number of characters that cause SMS charge to be 1 unit.

Installation options

XMS Mobile may be installed in either **Phone memory** or **Card memory** of the mobile phone.

XMS Mobile licensing

XMS Mobile installer is license bound to the buyers mobile phone number (MSISDN). The product gets activated only if installed in the phone with the licensed MSISDN number. In the event where the MSISDN number of the mobile phone is changed after installation and activation of XMS Mobile, the originating messages will be marked as corrupted on recipients XMS Mobile phone.



Glossary

1. Mobile station (MS) (e.g. mobile phone)
2. Base (transceiver) station (BTS)
3. Base station controller (BSC)
4. Gateway mobile services switching center (GMSC) and mobile services switching centers (MSCs)
5. Home location register (HLR)
6. Visitor location register (VLR)
7. Authentication center (AC)
8. Equipment identity register (EIR)
9. Operation and maintenance center (OMC)
2. Base (transceiver) station (BTS)
3. Base station controller (BSC)
4. Gateway mobile services switching center (GMSC) and mobile services switching centers (MSCs)
5. Home location register (HLR)
6. Visitor location register (VLR)
7. Authentication center (AC)
8. Equipment identity register (EIR)
9. Operation and maintenance center (OMC)
10. Operation and maintenance center (OMC)



XMS (Xecure Message Service) **Mobile messages you can Trust**

For XMS Mobile Manager Enquiry Please Contact:

Malaysia

malaysia@mynetsec.com

Phone: +603-6203 5303

Fax: +603-6203 5302

Pune

india@mynetsec.com

Phone: +91-20-2614 1596/97

Fax: +91-20-2613 6471

Delhi

india@mynetsec.com

Phone: +91-120 - 2513586, 5316242

Fax: +91-120-2513345

Singapore

singapore@mynetsec.com

Phone: +65-6835 7139

Fax: +65 6835 7145

USA

usa@mynetsec.com

Phone: +1 800 697 1884

Fax: +1 888 274 1689