



SMS Vulnerabilities - XMS Technology

White Paper

Prepared by



Network Security Solutions



Contents

Preface	3
Purpose of this Document.....	3
About Network Security Solutions.....	3
Document History	4
Version History	4
SMS Vulnerabilities.....	5
SMS	5
Ubiquitous SMS.....	5
SMS Security Loopholes Preclude Business Transactions	5
SMS Architecture	6
SMS Security Issues and Vulnerabilities.....	7
Attacks on GSM, the SMS Carrier Technology	7
Attacks on SMS.....	9
Example: SMS Spoofing in a Cellular provider's Infrastructure ...	10
Example: SMS Spam in a Cellular provider's Infrastructure.....	11
SMS Security: What is needed?	11
XMS Technology	12
XMS Technology: Specifications	13
XMS Cryptography Standards.....	13
Key-pair Generation.....	13
Encryption (Cipherring-Decipherring)	13
Digital Signing and Verification	13
Hashing	13
Strength of XMS Crypto Technology	14
Application Specifications	14
Smart Phone Support.....	14
Symbian OS	14
Supported Phones	14
J2ME Support.....	15
Application Size.....	15
XMS – Length of Messages.....	15
Installation Options.....	15
XMS Mobile Licensing	15
Glossary	16



Preface

Purpose of this Document

The aim of this White Paper is to give the reader an understanding of present-day SMS vulnerabilities and how XMS Technology addresses each concern to provide an excellent secure messaging option. This paper contains details of XMS technology and its major applications; it also describes the primary features of the XMS product. This White Paper is likely to be published in several revisions as the XMS product suite is enhanced. Some of the headings and tabular formats iterated may be updated in subsequent versions as necessitated.

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

Constituencies that may benefit from this document include:

- Telecom service providers.
- Banks and Financial services enterprise.
- Government and Federal agencies.
- Mobile phone SMS users.
- Any organization that values security of information disseminated through text messages.

About Network Security Solutions

Network Security Solutions (NSS) is an information security company headquartered in Kuala Lumpur, Malaysia. A recognized leader in security consulting, products and services, NSS develops, markets and supports proprietary products that secure sensitive/confidential information and are in use by a broad base of enterprises, businesses, governments and individuals. Over the past five years, NSS recommended and developed solutions have been used by scores of corporate/government and individual users worldwide. These include some of the world's most security-sensitive enterprises, government departments/agencies, individuals, and cryptography experts. Visit [NSS MSC SDN BHD at www.mynetsec.com](http://www.mynetsec.com) for more information or contact sales.xms@mynetsec.com for any queries related to XMS.



Document History

Version History

3 Jan 2006	Version 1.0	First Edition
12 Feb 2006	Version 1.1	R. Dave

This White Paper has been 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, 2006. 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 (Jan 2006)

Version 1.1 (Feb 2006)

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.



SMS Vulnerabilities

This paper offers a detailed description of SMS specifications and its inherent security issues and vulnerabilities. It describes in brief XMS Mobile technology and its specifications. XMS Mobile has been built over mobile applications using cryptography technology. XMS Technology helps makes SMS messages trustable.

SMS

The mobile phone is already an integral part of the lives of more than 1.8 billion people worldwide. Mobile usage is increasing in volume as well as diversity. 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 employees anywhere anytime. The desire to communicate more easily and have timely access to information is universal. The mobile phone is today being adopted and adapted in innovative ways to enhance business productivity. The Short Message Service (SMS) facility plays a leading role in this adoption.

Ubiquitous SMS

SMS enjoys enormous popularity as an economical and convenient mode of exchanging information. It not only saves time and cost but in many situations is also found to be more convenient than making a phone call. SMS has changed our working habits and social lives in many ways. SMS has simplified exchange of important short messages and also led to creation of services that are fun to use. People can easily share a private moment with their friends, family and work in other geographical locations in a cost effective and instant manner. SMS is further being used in business: for instance simplifying grocery shopping, providing alerts for best buys, bank alerts or such monitored events. Besides that it is being used these days in getting daily news, stock-market information, sports scores, quotes, travel and weather news. Many value added services (VAS) such as contest voting, songs request, and ring tone or service initiation are also being done using SMS. The list of services being facilitated through SMS is growing every day.

SMS Security Loopholes Preclude Business Transactions

It is known that SMS travels as plain text and privacy of the contents of SMS cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. Informed individuals have grown more and more skeptical of using SMS for sensitive and personal message exchanges. With growing awareness of such security loopholes in SMS, many value-adding business services are not being rolled out or are being deferred for end-users until appropriate security assurance is available.

SMS services currently provided by vendors, banks or other business houses are mostly passive in nature. The SMS, with its underlying gaps in security and

vulnerabilities, is not accepted for active business transactions. The demand for active SMS based services can only be satisfied when a solution that addresses end-to-end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality and non-repudiation are satisfied.

A number of active SMS services can be brought to users at a personal level and to government and corporate users at a business level:

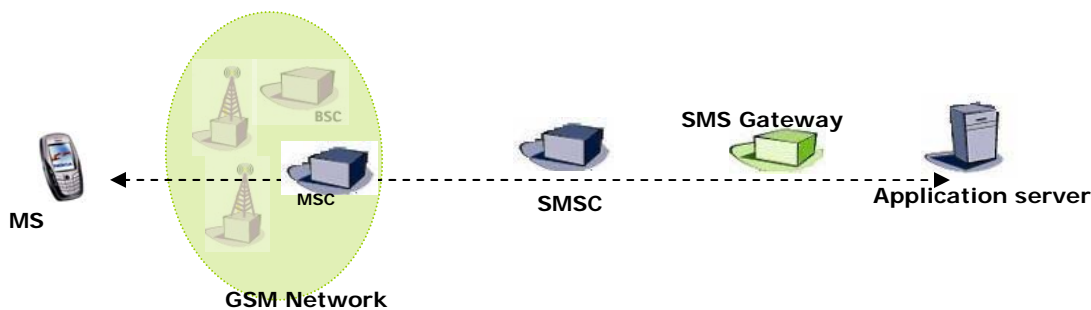
- **Banking:** Check balances, transfer funds between accounts, pay bills using credit cards. VAS is valuable not only for the subscriber but also for financial institutions offering this service.
- **Customer service:** charge a customer's credit card right at the table, at any time, instead of going 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.**

SMS Architecture

Short messages are delivered in GSM signaling channels between the Mobile Station (MS)* and the Base Transceiver Station (BTS). 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 that are connected to one or more SMSCs to provide SMS applications for the MS users. These applications include ring tone and icon delivery, entertainment, bank services, and many other beneficial services.

* Note – Please refer to Glossary at the end of the paper for a guide to acronyms used in the paper.

The figure below provides a diagrammatic representation of the components mentioned in this subsection.





SMS Security Issues and Vulnerabilities

Two important aspects for any entity using consumer technologies such as SMS for business purposes:

- SMS is not a secure environment.
- Security breaches often occur more easily by concentrating on people rather than technology.

The contents of SMS messages are visible 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 is to intercept messages. It would likely be a relatively complex to hack into a telecom provider's systems to obtain the content of SMS messages, but finding staff privileged to look at SMS messages and persuading them to reveal the contents is much easier. Gartner Research has already expressed reservations about security in U.K. trials of SMS voting in local elections held in May 2002. Enterprises, including governments, can not use SMS in its present state 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 leave 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 in security is the mobile phone itself. Even leaving the mobile phone unattended inadvertently could expose your private and confidential messages to **snooping**. For instance, 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.



Attacks on the A5 Algorithm:

There are several ways to eavesdrop on a call, although it is not very easy to eavesdrop on real time calls. There are different attacks against the A5/1 algorithm, the algorithm used to cryptographically protect 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 also not fast enough to be implemented in real time. A third attack called "biased birthday" 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 session key can be recovered. All the previously described attacks compromise the actual A5/1 algorithm.

Limitations in GSM Security:

There are other ways of eavesdropping on 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 obtains 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 key of a subscriber, on which the whole GSM security system is based. This key can be recovered in many ways. A SIM card reader and a PC can be used to send a huge number of challenges to the SIM card of the victim. The SIM card generates responses to all 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 is to make requests to the AC and construct the key from the responses of the AC. The above limitations of GSM security could lead to compromise of the carrier technology thereby making SMS vulnerable to **snooping** and **interception**.

Theft of Mobile Phones:

One problem characteristic of mobile networks is that mobile devices are easy to steal. Mobile phones are commonly stolen and 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 that are granted access to the network and not suspect. 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. 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 or sensitive information into their mobile devices' memories. Also, a mobile device may be used as a means of payment. These extra threats showcase the urgent need for protection against theft.

Attacks on SMS

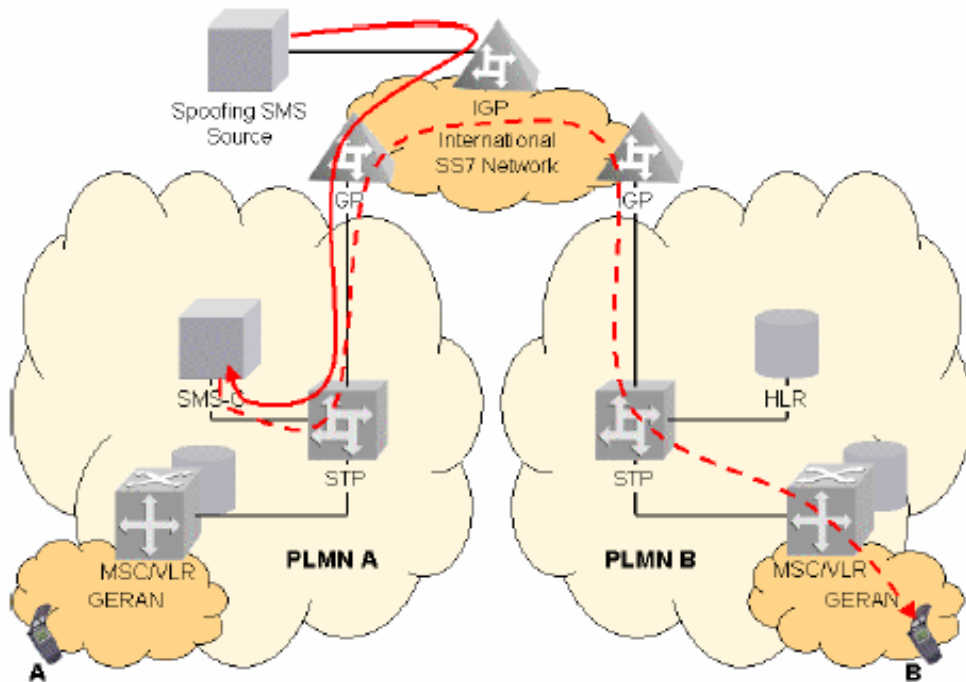
The connection between the SMSC and the SMS gateway is not part of the GSM standard. There are many different protocols available for use between the SMSC and the gateway. These protocols are built on familiar protocols, such as TCP/IP and X.25. Also, the connections are not part of the GSM network, 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 really a superior way of authenticating, since it is very simple to do a man-in-the-middle attack against TCP/IP and **intercept** the communication.

Short messages as well as traditional calls may be spoofed by exploiting the same GSM vulnerabilities described above but there is an easier way of spoofing short messages: 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 isn't actually the case, since operators normally run both the gateway and the SMSC behind a firewall. But this is not a rule and 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 Mobile Station International ISDN Number (MSISDN) in that field may cause the message to appear as one 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 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 used to make unauthorized bank transactions.

Eavesdropping and **Modifying** can be implemented just as in the case of normal GSM phone calls. The SS7 network and the A5 algorithms are vulnerable, as was mentioned earlier. 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. A normal network listener is enough to gain access to information. At this point it is also possible to alter the message content, if possible checksums and field lengths are taken into account. Another part of the SMS application that is not always protected is the connection between the SMS gateway and the application server. It is easy to eavesdrop this connection also. It is thus possible to change

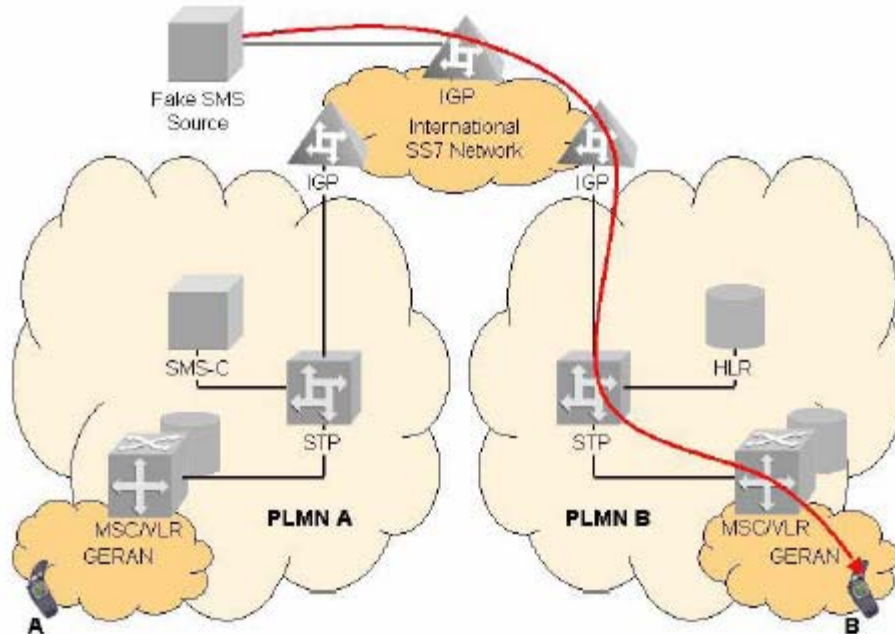
sums or account numbers in a bank transaction and alter stock information broadcasted to stock service subscribers etc.

Example: SMS spoofing in a Cellular provider's Infrastructure



- The SMS sent to the SMS-C has a manipulated originating MSISDN A number.
- One example is shown in the 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 false MSISDN A numbers, originating VLR and / or SCCP addresses.

Example: SMS Spam in a Cellular provider's Infrastructure



- The Faked SMSes have manipulated Mobile Application Part (MAP) addresses. The source address of the SMS pretends that these are sent from another network (in Figure, from Public Land Mobile Network A (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

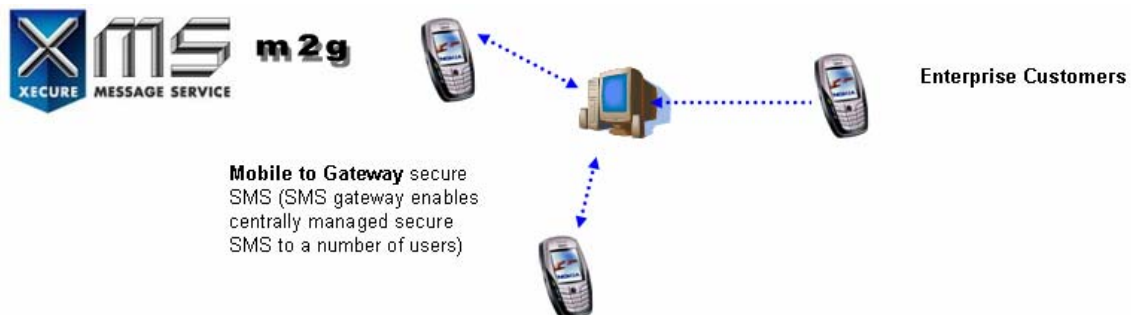
An end-to-end key based encryption technology for SMS plugs the gaps in transit security of SMS. Authentication added for resident SMS security access together with encryption, addresses the 'Confidentiality' issue of SMS technology. Added features of message integrity and digital signing of SMS address 'Integrity' and 'Non Repudiation' for SMS technology. With the above feature set integrated into the SME (smart message entities), whether it is 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 crypto-technology platform for SMS messaging, addresses end-to-end security in SMS messages. 'XMS Mobile' product on mobile phones provides an end-to-end security solution for assured messaging in a peer to peer (P2P) environment.



'XMS' product suite also provides a holistic security solution for 'peer to server' SMS applications. The 'XMS Enterprise Server Plus' 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. These standards require: 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. 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 and smart computing devices.

Encryption (Ciphering-Deciphering)

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 Elliptical Curve DSA (ECDSA) for signing and verification purpose. It is a variant of the Digital Signature Algorithm (DSA) which operates on elliptical 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-mentioned crypto standards and algorithms that have been used and published. XMS technology uses the algorithms in their published and unaltered state.

Application Specifications

Smart Phone Support

Symbian 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
-----------	-----------

J2ME Support

Smart phones that support J2ME MIDP 2.0, CLDC 1.1

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 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 permissible in a unit SMS charge.

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 buyer's 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 corrupt on recipient's XMS Mobile phone.



Glossary

Mobile Networks

Authentication Center (AC)
Base Station Controller (BSC)
Base Transceiver Station (BTS) or Base Station (BS)
Enhanced Data Rates for GSM Evolution (EDGE)
Equipment Identity Register (EIR)
Gateway Mobile Services switching Center (GMSC) and Mobile Services switching Centers (MSCs)
General Packet Radio Service (GPRS)
GSM/EDGE Radio Access Network (GERAN)
Home Location Register (HLR)
Integrated Services Digital Network (ISDN)
Mobile Application Part (MAP)
Mobile Station (MS) (e.g. mobile phone)
Mobile Station (Subscriber) International ISDN Number (MSISDN)
Operation and Maintenance Center (OMC)
Public Land Mobile Network (PLMN)
Value Added Services (VAS)
Visitor Location Register (VLR)

Cryptography

Advanced Encryption Standard (AES)
Digital Encryption Standard (DES)
Digital Signature Algorithm (DSA)
Elliptical Curve Cryptography (ECC)
Elliptical Curve Digital Signature Algorithm (ECDSA)
Public Key Infrastructure (PKI)
RSA (algorithm invented in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman)
Secure Hash Algorithm (SHA)



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

For XMS Mobile Sales 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