



# XMS Anti Identity Theft Solution

15 April 2006  
Version: 1





Version Information

<b>File name:</b>	NSS XMS Anti Identity Theft Solution Version 1.0
<b>Creation date:</b>	01 <sup>st</sup> April 2006
<b>Latest Update</b>	15 <sup>th</sup> April 2006
<b>Next Revision Due</b>	01 <sup>st</sup> July 2006
<b>Original Author:</b>	Anurana Saluja



## About NSS

Network Security Solutions (NSS) is an information security company headquartered in Kuala Lumpur, Malaysia. A niche player 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. Please visit NSS MSC SDN BHD at [www.mynetsec.com](http://www.mynetsec.com) for more information.

## A Brief on XMS

XMS is a NSS proprietary application that is possibly the first end-to-end secure text SMS solution in the world. XMS includes NSS patented technologies/workflow. It is essentially an Advanced Encryption Standard (AES – the de facto industry standard) based encryption solution that works on public-private keys generated by Elliptical Curve Cryptography (ECC) whose key strengths can be selected as 128 bits, 192 bits or 256 bits. XMS involves key pairing between users (peer-to-peer mode) or between customer and server (When banking or financial applications are considered). This ensures a unique pairing between any two persons or a person and server (institution). The Application on the phone is password protected (this password is set by the user himself during installation). Messages are encrypted and signed at point of origin (mobile handset) and decrypted only at point of termination (recipient's mobile handset or bank server). Thus data at rest, as well as in transit remains protected.

XMS rides on the SMS protocol, so we do not introduce anything new, instead use a mature, popular technology in a new business workflow. XMS assures the following:

- Confidentiality (Encrypted contents)
- Integrity (Hash value and digital signature)
- Non Repudiation (Digital signature)

Presently XMS technology powers two applications used in different target groups – generic users who want to send private or confidential texts within their group - and XMS Mobile Banking. In a mobile banking workflow, XMS will satisfy the two factor authentication requirement of banks – what you have (a mobile handset with a custom delivered application) and what you know (Mobile PIN that the bank will authenticate at their end to allow a transaction). Please visit [http://www.mynetsec.com/XMS\\_Mobile\\_Banking.pdf](http://www.mynetsec.com/XMS_Mobile_Banking.pdf) for a pdf on XMS Mobile Banking.

XMS has bridged the only problem area of the workhorse SMS, by providing it business-ready security features. While GPRS and WAP are emerging technologies that will provide impetus to m Commerce, SMS was not considered thus far by financial services other than for non personal notifications because of its security vulnerabilities. This killer app now has its XMS shield and huge potential.

The XMS application can be downloaded over the air (WAP push) or sent via email to a recipient who can then transfer it to his mobile phone via Blue tooth or IR. The application is light by itself, between 160 -180 KB. Once installed, the user is prompted to enter his password for the application, it generates automatically the user's key pair (private and public keys) – public keys are exchanged with the peer group and the person is ready to send out secure text. The UI is easy and intuitive, and the encrypting is done at the backend, so user experience is good.

Over 200 smart-phones in the market are compatible for XMS – all Java enabled phones with MIDP 2.0 and Symbian phones are supported. We are looking at a potentially huge market. The application distribution and function is independent of telecom service providers, which does away with avoidable dependencies.

This paper needs to be read in conjunction the white paper on XMS Technology, which provides technical details of the encryption standards and other technologies used.

## The Anti Identity Theft workflow:

The XMS Anti-Identity Theft Solution builds upon the XMS Mobile and XMS Mobile Banking solutions by allowing banks and credit card issuers to securely implement personal two-way authentication of credit card transactions with their customers in a real-time environment.

### How Does It Work?

#### *Register & Download*

- Customer registers with their bank and/or credit card issuer for Mobile Credit Card Authentication services.
- Upon registration, a unique application is generated for the customer's registered mobile number and can either be downloaded from the Internet, or sent via Bluetooth or Infrared.
- Install the Application on the mobile handset.
- For activation, set password and initiate device registration.
- An encrypted Mobile PIN (M-PIN) will be sent through XMS to the registered mobile number.

#### *Mobile Credit Card Transaction Authentication*

- Upon usage of a credit card (either online or offline) a secure automated XMS message containing a description, location, time, and amount will be immediately received by the registered phone number of the user from the XMS Server located at the bank or credit card issuer. (Note that an adapter will have to be designed/implemented with the assistance of the Credit Card Company, so that this app talks to their workflow. Additionally, the specific basis for activation of the XMS notification- for instance – purchases above a certain value, graded suspicious transactions, usage anomalies etc that are already being “identified” by CC companies – may be defined and customized by the CC and/or the user, upon registration – this would feed only selected transaction info into the XMS notification channel, as may be intended)
- The user opens the message and is prompted for his/her personal password (as per XMS Mobile) followed by their allocated M-PIN.
- The message with the aforementioned details of the transaction will then be decrypted and displayed to the user.
- Displayed within the message will be a simple (Y)es and (N)o query asking for confirmation that this transaction took place.
- The user selects their response and the reply will be packed into an SMS message, encrypted, digitally signed and sent using the SMS protocol to the bank or credit card issuer's registered short code.
- The reply will be received by the XMS Server, authenticated, decrypted and passed on to the bank or credit card issuer's server for processing.
- If the user confirmed the purchase the payment will go through. If it is denied then payment will not take place and a caution 'flag' will automatically be placed on the user's credit card and normal investigation procedures would commence.

#### *Value Proposition:*

- **Real-time authentication** - the XMS message is sent as soon as any credit card transaction is made. It therefore ties the user's credit card to his mobile phone for added security. Payment is halted until such confirmation is given, and halted if the user denies such a transaction.
- **Fraud prevention** - due to the need for the user to authenticate transactions, online phishing and real-world un-authorized transactions (skimming) are prevented at the point of sale.
- **Control and User confidence** - Allows customers to play a more personal role of being in control of their credit card transactions.
- **Flexible and Ubiquitous** - Can be used for both offline and online transactions anywhere in the world.
- **Cost effective** - the cost of a normal SMS as opposed to IVR or Call centre agent calling every time a transaction is 'flagged'. Cost effectiveness in manual investigating and processing lower value transactions through process automation.
- **Interfaces** with automated response systems and customer relationship databases.



- **Creation of an SMS audit trail** for both the bank or credit card issuer and the customer.
- Ability to couple the XMS Anti-Identity Theft Solution with other products in the XMS suite to allow for secure peer-to-peer messaging or mobile banking.

#### *Security and Assurance*

XMS features two-factor authentication, a pre-requisite for most financial transactions, through:

- **What you have:** A registered handset with the XMS application.
- **What you know:** M-PIN registered with the bank or credit card issuer.

Additional security features include:

- Password-based user authentication.
- Application level encryption on the handset that ensures data both at rest as well as in transit remains confidential.
- Public/Private key based authentication mechanisms and digital signatures ensure message integrity.