



**NSS**  
Rest Assured

# Xecure Phone

**Communications are essential for operations.  
Securing the communication channels is crucial.**

**The NSS Xecure Phone is a one stop solution. Secure your voice and text communications. Maintain an invisible vigil over your handset.**



## Xecure Phone

- A feature-rich solution available on 10 commercially available phone models.
- Military grade encryption for Voice and Text.
- Equipped to track a stolen or lost phone.
- Remotely lock an unauthorized user out and delete all personal data via a user-initiated SMS.
- Solution works independent of mobile service providers and handset manufacturers.

**Xecure Phone is bundled with 3 cutting-edge security components:-**

### Xecure Voice

Encrypted voice communications over GPRS/EDGE/3G networks.

Software based, no proprietary handsets or expensive equipment required.



### CellSniper

Protects data on lost/stolen mobile handsets.

Automatically locks handset when the SIM card is replaced/handset is restarted. Tracks new user each time a new SIM card is inserted.

Remote Lock of phone enabled via SMS.

Remote Wipe deletes all personal data on phone via SMS.

Supports all languages.

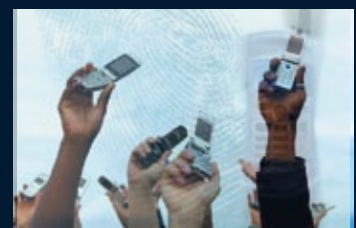
### SMS Encryption (XMS)

Encrypted and digitally signed text messages.

Protected Inbox, Outbox and Contacts list.

End-to-end Secure and trusted messages.

Supports all languages.



**Corporate Office: NSS MSC Sdn. Bhd.**

tel: +603 6203 5303  
fax: +603 6203 5302  
E-mail: sales@mynetsec.com

Suite E-07-21, Plaza Mont' Kiara  
2 Jalan Kiara, Mont' Kiara  
50480 Kuala Lumpur  
Malaysia

[www.mynetsec.com](http://www.mynetsec.com)

# Technical Specifications

## XECCURE VOICE

**Xecure Phone** uses state-of-the-art technology and is the most effective option to secure your mobile communication against tapping attacks and monitoring by third parties.

- Voice encryption with AES 256 Bit
- Key exchange with Diffie-Hellman 2048 Bit
- Verbal comparison of the “fingerprint” in order to avoid Man-in-the-middle-attacks

The call partners exchange an encryption key using the secure Diffie-Hellman key exchange method. To avoid any Man-in-the-middle-Attack a four-digit code is regenerated with every new call from a 2048 bit long number. Each time a connection is established this code is shown on the display of the mobile device and must be compared verbally with the other party, to make sure that the encrypted call is not intercepted.

For voice encryption, only the highest available encryption standard AES (Advanced Encryption Standard) with 256 bit key length is used. All encryption and key exchange algorithms are globally standardized and certified and provide reliable protection against all kinds of tapping scenarios.

### Xecure Phone supports the following phones on version 3

**Nokia E51**  
**Nokia E61i**  
**Nokia E61**  
**Nokia E65**  
**Nokia E71**

**Nokia N73**  
**Nokia N75**  
**Nokia N80**  
**Nokia N95**  
**Nokia E90**

## SMS ENCRYPTION (XMS - Xecure Message Service)

### Key-pair Generation

XMS technology uses Elliptical Curve Cryptography (ECC) for key-pair generation. ECC is best suited to mobile devices as it uses smaller keys than other methods — such as RSA — while providing an equivalent or higher level of security. Keys are generated during installation and are different on each phone. Private key is never shared.

### Encryption (Cipherring-Decipherring)

Bank-grade Advanced Encryption Standard (AES), a symmetric 128-bit block data encryption technique is used. AES has a fixed block size of 128-bits and a key size of 128, 192 or 256-bits. 256 bit key size is used for Xecure Phone XMS.

### Digital Signing and Verification

XMS technology uses Elliptical Curve Digital Signature Algorithm (ECDSA) for signing and verification purposes.

### Hashing

XMS technology uses Secure Hash Algorithm SHA-1.

## CellSniper

**CellSniper** uses a stealth-mode .exe file that is designed to detect any change in SIM card. When such an event occurs, it sends alert messages to the predesignated mobile phone numbers that are entered by the user. CellSniper also locks a phone when it is restarted for added security. Only the CellSniper password will unlock the phone for use. All applications and menus of the phone are accessible only after the correct password has been entered.

CellSniper also allows a user to lock-out his phone via a text message, allowing him to bar access to the device at any time. Similarly, a Wipe message sent via SMS deletes all personal information viz. native Contacts, SMS (Inbox, Outbox, Drafts and Sent Items), MMS, Video, Picture and Image files and all information on the memory card.



**Branch Offices: Network Security Solutions Ltd.**

**DUBAI**  
Tel: +971 501 533246  
Fax: +91 20 40091672  
E-mail: uae@mynetsec.com

**INDIA**  
Tel: +91 20 40091670/71  
Fax: +91 20 40091672  
E-mail: india@mynetsec.com

**SRI LANKA**  
Telefax: +94 11 2559082  
Mobile: +94 777 326273  
E-mail: srilanka@mynetsec.com

**SINGAPORE**  
Tel: +65 68357139  
Fax: +65 68357145  
E-mail: singapore@mynetsec.com

**USA**  
Tel: +1800 6971884  
Fax: +1888 2741689  
E-mail: usa@mynetsec.com