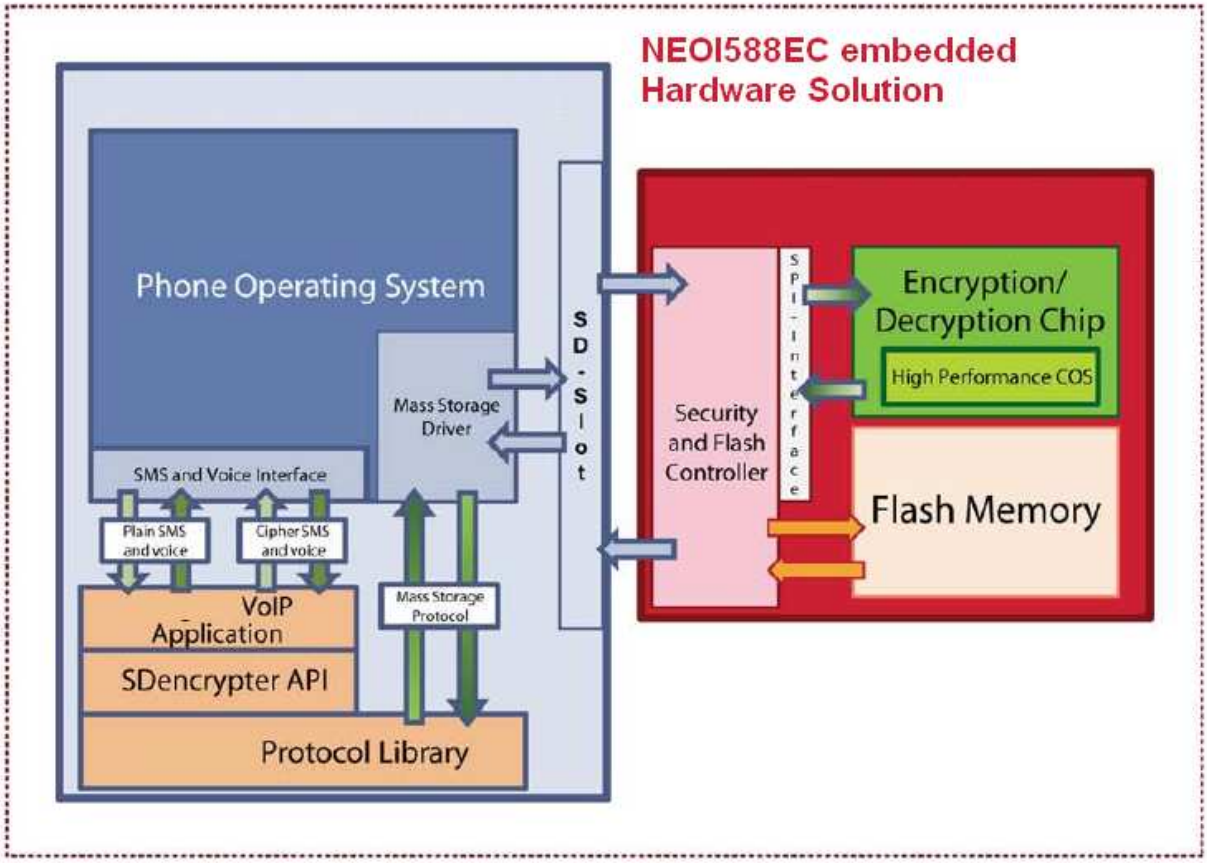
Nimicscrypt – the ultimate security in Mobile Communications with the Neoi588EC Smartphone!

Protecting Valuable Information Organizations make significant efforts and invest huge amounts to protect their valuable data from loss or interception – particularly when accessed outside the office and traveling abroad. Several Software based encryption solutions offered are only as secure as their software allows, only encryption with hardware embedded special micro-chips will allow unlimited SECURITY!

Since 2010 cell phone security is significantly reduced since hackers computed and published free on the internet a codebook to decrypt GSM calls– used in 80% of cell phones worldwide – as well as demonstrating interception equipment that is readily available for under $2,000.- . However exactly the same hackers developed also the encryption Software that they claim works on any standard Phone. Even none expert will understand immediately that such solutions provide no security at all, as the developers at any time can access the so called secure environment.

Intelligent embedded Hardware is the ONLY solution.



With Nimicscrypt™ , calls can easily be protected on popular cell phones – and securely connected to office phone systems – so that you can be assured conversations remain confidential wherever they are.

Security

- **Strong end-to-end encryption**
- **US Government FIPS 140-2 validated (cert number 1310)**

Against Eavesdropping

Any intercepted voice packets or messages are encrypted by AES-1281256 algorithms that would take thousands of years to crack.

Against Trojans and Viruses

All confidential information and encryption keys are stored and processed inside the Nimicscrypt security chip. They are never exposed to the handset. There is no chance a rogue application can access or export this information.

Against "Man-in-the-Middle-Attack"

- **All communication that leaves the handset is encrypted and unintelligible to anybody who intercepts it**

Against Physical Attacks on Encryption Chip

• **The security chip inside the Nimicscrypt is Common Criteria EAL 5+ certified (Military and National Security Levels). The chip is able to withstand all kinds of physical and side channel attacks.**

Simplicity

• embedded Microchip especially developed by NEOI Technology that runs on Android smartphones. User do NOT need to install additional hardware or Software. The Neoi588EC Phone is ready to use. Just setup the Phone Number and an additional Password, register automatically to the Nimicscrypt Certification Server and make instant totally secured Phone Calls and send receive messages from/to other Nimicscrypt™ users. • Intuitive user experience, runs in background & integrates with device phonebook

Performance

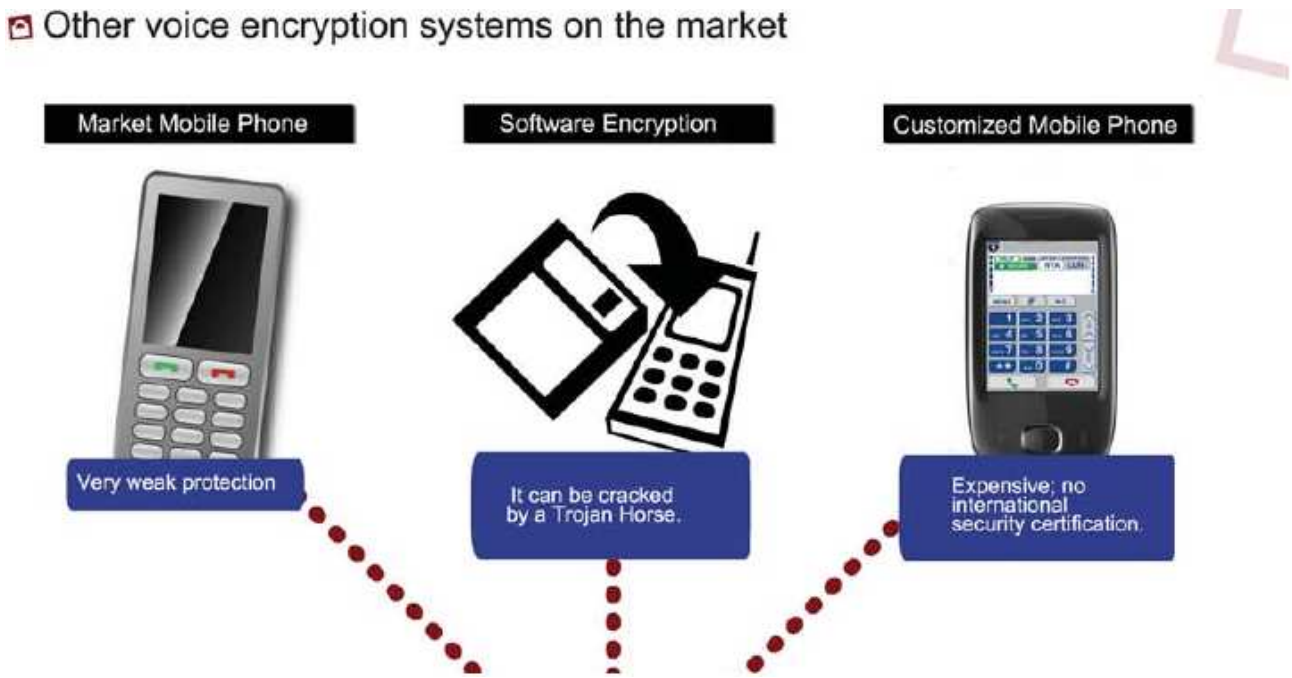
• Interoperates across and between leading smartphones and cellular networks

• *High call quality with low latency*

• Operates on all data-capable wireless networks

• *International* calling via the Nimics™ IP Network at low cost, save thousands of dollars monthly and still be totally secured.

• *Secure* calling to landlines with NEOI™ Enterprise Gateway –



Network Support

• Any IP-enabled network, e.g. - GSM/CDMA - 2G - 3G - 4G – Satellite - Wi-Fi™

Nimicscrypt™ Mobile's intuitive user interface makes a secure call as easy as making a normal call:

- **To make a call, users simply open the Nimicscrypt Mobile application by selecting the icon on their NEOI588 Android Smart-phone, manually enter a Nimicscrypt secure number (or select a previously saved contact from the Nimicscrypt address book) and press send**
- **Nimicscrypt™ Mobile needs to be running on both devices so that both can encrypt/decrypt the voice calls / messages at each end to provide security along the entire path between the callers**
- **It also uses the data channel (IP) rather than voice channel so both devices also need to be connected to the internet using standard data connectivity provided by the service provider**
- **Government-grade cryptography is used to check the identity of each device on the call and then encrypt the call**
- **The recipient's phone rings or vibrates, automatically shows the Nimicscrypt™ Mobile screen and displays an incoming call**
- **If the call is accepted a normal conversation is conducted until one of the callers hangs up. The caller is notified if the recipient is busy or not online**
- **All communications products that rely on cellular networks are dependent on the strength, availability and reliability of the underlying radio network for their performance. Nimicscrypt understands this industry problem and is one of few companies to deliver specific technology solutions for optimizing performance in poor and variable wireless conditions, including its Encrypted Mobile Content Protocol™ and Encrypted Content Delivery Network™.**

Nimicscrypt™ Mobile automatically switches to the highest quality network that the handset is connected to so that Wi--Fi™ is selected in preference to cellular networks. Also calls work across changing cellular networks (for example if a 3G connection is degraded by the carrier to an EDGE or GPRS connection) even as the call is in progress. Callers can be on different networks in different countries for example Wi--Fi at one end and HSDPA at the other.

Setting up Nimicscrypt™ Mobile on a cell phone is easy:

- **Users just insert their Username (in most cases the Mobile Phone Telephone Number of the SIM Card) and a password**
- **The Nimicscrypt™ Mobile software now validates with the Nimicscrypt / NEOI SIP server the users request for registration**
- **Is the user registered in the system, the Phone will be connected and ready for secure calls / messages.**
- **If the phone is lost or stolen, Nimicscrypt™ Mobile can be disabled remotely, instantly**
- **Secure including US NIST FIPS 140--2 (certificate #1310) for its encryption and UK CESG**
- **Tested Mark for its product implementation.**

In any product, security is only as strong as:

- **The strength of the encryption it uses**
- **The security of the secret keys used to unlock the encryption**
- **The integrity of the product implementation and the trustworthiness of the supplier**
- **And ! most importantly the encryption has to be embedded into the HARDWARE of a specially**
- **designed Mobile Phone. The ONLY available Android Smartphone worldwide with a special**
- **embedded micro encryption chip is the NEOI 588EC™**

- **Nimicscrypt™ Neoi588EC™ Mobile uses encryption algorithms that are recommended for**

military and government secure communications and its secret keys never leave the mobile device.

The product has been tested by third parties and validated to several government standards

Speak With Confidence

Nimicscrypt™ Mobile for Android is an easy-to-use, next generation Hardware solution that runs on Neoi588EC phones and uses the data network to serve up unparalleled voice quality, low voice delays (latency), global coverage and intercontinental call capability - all delivered securely. Using Nimicscrypt™ Mobile is as easy as making a normal call, yet provides the confidence that phone
calls, whether in the Home or Office environment , at home or overseas, within or outside departments, suppliers and business partners, are protected end-to-end.
Security is assured; Nimicscrypt uses a much higher level of encryption then well-established and trusted encryption technologies to protect voice communications that are used to protect laptops, corporate data and financial services transactions. Nimicscrypt™ achieves an until now unknown level of security.

Nimicscrypt Technology

advanced hardware solution leads the industry in delivering multi- layered secure high-performance encrypted voice call between trusted wireless devices. It utilizes Encrypted Protocol (EMCP), a set of standards-based protocols for optimizing delivery of encrypted between cell phones over low-bandwidth wireless networks. Nimicscrypt's products are certified 140-2 standard, approved by the US National Institute of Standards & Technology (NIST).

Cryptography & Random Number Generation
Public Cryptography
(2048-bit RSA & ECDSA using curves with 384-bit prime module)

RSA and ECDSA are used for authentication. The key pairs are generated on the phone during the installation and are unique to each phone. A private key is never shared. The Elliptic Curve Diffie-Hellman (ECDH) and RSA algorithms are used for key exchange. The session key is only valid for one phone call and securely destroyed after use. If the user inserts 5 times the wrong password, the phone will be totally disabled, and even the factory cannot recover any files anymore, the Phone has to be totally setup with a new Source code and Software.

Symmetric Cryptography
(AES & RC4, both 256 bits)

Both encryption algorithms are used at the same time. The data packet is first encrypted with RC4 and the cipher text is then encrypted again with AES in Counter Mode (CTR). Both algorithms are initialized with the exchanged session key.

Hashing Algorithms
(SHA512, MD5)

Two industry standard hashing algorithms are used for increased integrity assurance.

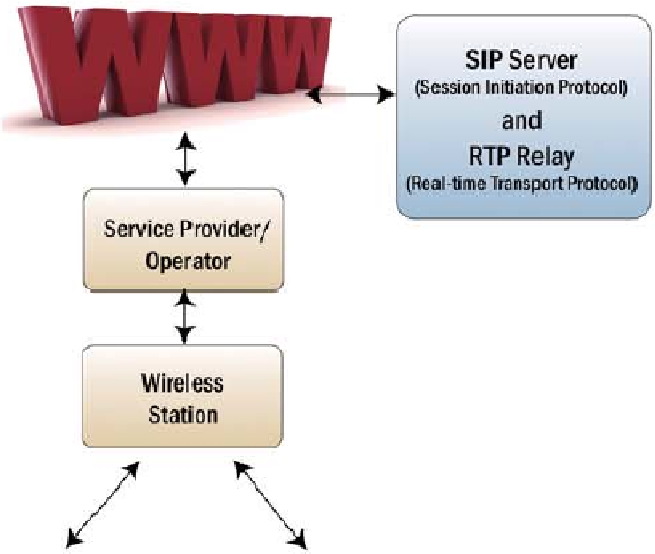
Random Number Generation

A 2048 bit seed pool is generated during the installation and is periodically updated. The initial seed is derived from the microphone input.

About NEOI Technology Pte. Ltd.

Neoi Technology was founded 1977. Specialized in shortwave communication devices. One of the founder partners of the company was working in the telecommunications division of the National security forces from 1967 to 1977. Neoi designed the world's first Inmarsat satellite phone in

1987 with secure voice transmission. The preferred Satellite Phone for Government and Military organizations.
After 1995 Neoi started development and production of GSM and WCDMA / CDMA based communication devices as well IP based services and encryption solutions for leading security agencies around the world, police and commercial enterprises. Still today NEOI technology is the leading design house for secure communications and with its latest, the Neoi588EC, hardware embedded voice and message encryption again leads the industry.



NIMICSCRYPT – Confidential Voice encryption Instructions.

NimicsCrypt is a hardware based High Security MIL Grade Voice encryption system.
It CANNOT be copied or separated from the installed Hardware.
Please do not de-install either the APK Software, nor remove the installed SD Card. The encryption device works on the base that the internally installed hardware encryption chip, interchanges Data with the SD Card. Any attempt to change this, or remove parts will result in permanent disabling of the Phone, and needs to be returned to the Factory for resetting.

1. **To start the Voice Encryption you need to have following basic conditions**
   a. **in Slot 1 of the Phone, 1 SIM 3G SIM card installed and enabled**
   b. **Data connection set up and connected to a carrier (3G HSDPA required)**
   c. **Or connect to a WiFi access point (using the Phones internal WiFi settings enabled and connected**
2. **Click on the "CALL" icon and start the encryption process**
   a. **Use default Password 123456 (password can be changed later)**
   b. **Note, if the password is entered 5 times wrong (see call count displayed), the set will be automatically blocked, and has to be returned to the manufacturer for resetting (for security reasons)**
   c. **After Password has been entered, and a reliable Network connection has been detected, the encryption will connect (Icon in Notification area turns from color brown to gray)**
   d. **Each DEMO set has a pre-assigned phone / Call Number, see inside the Battery cover label.**
   e. **To make a call, enter another sets Phone number, Press Call.**
   f. **If a reliable Network connection is available, monitor the connection process and exchange of security Certificates.**

3.) Call
a.) once a call is connected, adjust the audio settings on the phone to minimum echo (Volume up or down selection)
b.) alternatively recommended to use the earphone set, for perfect noise cancellation and more security.
c.) End of call press END
4.) Network and connection conditions
a.) to have a stable encrypted clear Voice, you need a minimum QoS of 60%
b.) Check QoS: Press Menu >>>>Options >>> System Information Net. QoS: (60% +)
c.) Note under 60%, there will be no reliable stable connection, as Bandwidth is not enough provided by the operators Time Slots.
d.) In same Menu check connection IP: if IP empty, set is not connected the IP will be empty (Notification Icon color Brown)
e.) Reset Connection: Press EXIT from Menu, restart CALL with PIN
f.) Other Menu settings :
g.) My Number, shows Phone Number for encrypted Calls
h.) Change PIN, to change PIN
i.) Firewall settings : setting Default for all Networks, or Fixed / customized port.
j.) Call History, shows calls made to other NimicsCrypt Phones.
5.) During a call
a.) Press Menu during a call allows Option to SWTCH OFF Voice encryption for clear Calls
b.) Note: Both sets must switch off voice encryption to communicate free an open, if only one set goes into open mode, for security reasons any audio will be blocked.
6.) Others
a.) NimicsCrypt operates with a Dual SIM card system, in case there is no reliable Data Connections, phones always can call each other in normal open GSM Mode. This might be practical in poor reception areas, to schedule an encrypted call via WiFi for example.
For service please contact: info@nimics.net Keyword: NimicsCrypt

Neoi588EC-Nimicscrypt Technical Specifications

Basic Specifications	Details	Remarks
◇ Chipset	MTK6573+Android2.3	
◇ NimicsCrypt Micro Chip embedded	Embedded Voice and Message encryption	Requires always 2 Neoi588EC phones for secured communications
◇ Band/Mode	GSM/GPRS/:850/900/1800/1900MHz	
	WCDMA:2100 MHz	HSPA 5.76Mbps~ 7.2Mbps ,
◇ Dual Card Dual standby	Yes	Dual SIM SIM 1: GSM/3G/WCDMA SIN 2: GSM
◇ Type	PDA	
◇ Size (mm)	124*68.2*12.6MM	
◇ Weight	approx 290 gr	
◇ Battery	1500mAh	high capacity for long talking and standby
◇ MMI Input	Android mode	
◇ Screen Size/Pixel	4.3" WVGA 480*800	
◇ System memory	4Gbit Flash+4Gbit RAM	
◇ External Memory Connector	T-Flash(no hot plug)	Max support 32G not included
◇ Camera	front 0.3M+rear camera 5.0M	
◇ Navigation key	Soft Key	
◇TV	NO	additional APK download
◇ Multimedia	MP3/MP4	
◇ Headset	3.5mm	
◇HW Description		Remark/Supplier
◇ Main CPU or Co-CPU (MHz)		
* CPU	MTK6573	650 MHz

* GSM	Yes	
* GPRS	Yes	
* EDGE	Yes	
◇ LCD		
* Sub LCD	No	
* Sub LCD backlight	Softkey backlight Yes	
* Main LCD	4.3" (4.4" internal) TFT WVGA	4.3" effective user size
* Main LCD backlight	White	
* Touch Lens	CTP	CTP
* Keypad Backlight	White	
◇ Multimedia		
* Stereo ring tone	64 polyphonic	
* Record	Yes	
* Handsfree	Yes	
* FM radio	Yes	
* MP3 decode	Yes	
* MPEG4 decode	Yes	
* Gravity sensor	3D Accelerator	optional APK download
* USB Storage	Yes	USB2.0
◇ Wireless transmission		
* WAP/MMS/JAVA	Yes	
* JAVA	Yes	
* Bluetooth	Yes	BT2.2
* Wifi	Yes	
* Backup battery	Yes	For Internal clock and System
◇SW description		Remark/Supplier
◇ Basic Functions		
* Languages (On browser)	34 Languages, English default	can be customized by customer
* Phone book	1000＋Sim	
* E- book	Yes	TXT, Office,PDF
* E-mail	Yes	SMT, POP3,IMAP4,Push-mailE-
* Phone book Copy	Yes	
* Schedule/To_Do	Yes	
* Calendar	Yes	
* Alarm clock	Yes	
* International clock set on world map	Yes	Google Map settings
* Calculator	Yes	
* Currency converter	Yes	
* STK	Yes	
* Call forwarding	Yes	
* Call waiting	Yes	
* Call urgency（no sim）	Yes	
* Handwriting	Yes	
* Lock all keys	Yes	
* Calling Record	Yes	
* Google Market	Yes	
◇ SMS		
* SMS	255	
* Instant Messenger	Yes	IM+ APK. MIM, Facebook, Twitter, otehrs
* News	Yes	BBC , others,
◇ EMS		
* email	Yes	Google Mail, Push Mail, POP3 mail

* EMS MMS	Yes via optional APK	
◇ MMS		
* MMS supported format	JPEG/GIF89a/GIF87a/WBMP/PNG/MIDI/AMR	
* MMS audio supported format	MIDI/MP3/AMR/PCM/AAC	
* MMS Total size	100k	
◇ Browser		
* WAP version	2	
* WWW Browser	Yes	
◇ Movie		
* Audio format	AAC, AAC+, AMR-NB, MIDI, MP3,WMA	
* Video format	WMV,MPEG4,3GP(H.263)	
◇ Other		
* Communicate tools	Yes	IM and others APK
* Widgets	Yes	Android Standard, additional APK Yes
* Video chat	Yes	Video Phone Calls Yes
Customer		
NO.	Item	Plan
1	Gift Box	Customer design
2	Inner Box	Customer design
3	Gift Box Label	OEM/Customer design
4	Charger Label	OEM/Customer design
5	Product Information Label	OEM/Customer design
6	Pallet Label	OEM/Customer design
7	User Manual Cover	OEM/Customer design
8	IMEI Range	OEM/Customer range supplied
9	Cartoon Box Label	OEM/Customer design
10	Battery Label	OEM/Customer design
11	Warranty Card	OEM/Customer design