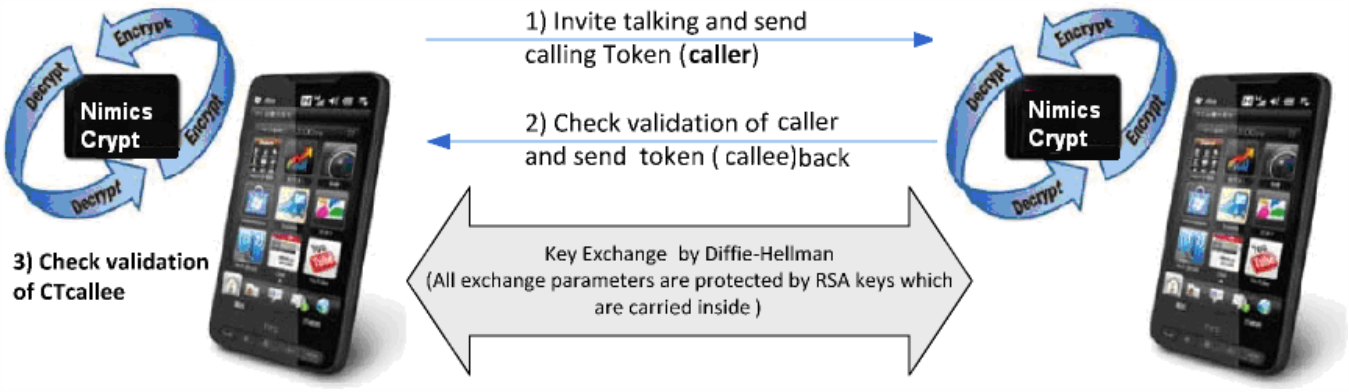
NimicsCrypt Call

is the best choice to secure your phone calls.

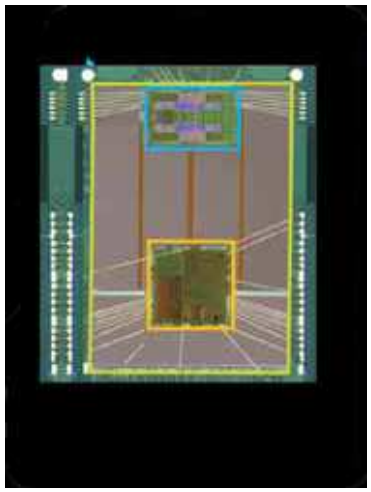
Everything need for high security Government Communications, Voice, Audio, Video, Data, Messaging, in one closed System, totally managed and controlled by Government Security departments.
Each System is widely individualized, so not even a Systems Administrator can access into another System.

The one and only military strength Hardware encryption solution for Neoi Android Phones and Tablet-Phones



The Nimics-Neoi Android NimicsCrypt securely encrypts Voice, SMS ,Instant Text , communication, confidential documents. Pictures and other Confidential Files are also encrypted and safely stored on the special phone or using cloud storage on the special Certificate server provided by Neoi-Nimics. A special secure Software provides even in areas were voice communication is not possible a safe and secure method to send and receive files and messages.

Neoi provides the complete Server Solution, Hardware and Software installed, ready to use by the local user / Operator. After installation the entire Systems will be handed over to the owner, who then can reset the system with new passwords , so that even Neoi cannot enter the system anymore.



The NimicsCrypt uses a powerful 32-bit Hardware Security Module (HSM) inside the special Neoi Android Smartphone. This design means your Neoi Android Smart Phone is ready for military strength communications. No further modification is required or possible to the Android operating system, it comes completely secure installed in a Neoi Android Smartphone.

Just set up a new personal secure Password and special Phone Number and be ready to

use Military Strength Encryption.

More functions:

SMS text scrambling between groups of Neoi NimicsCrypt Phone and Neoi NimicsCrypt Tablet Users . The SMS address book, stored messages (sent and received) and all history is encrypted and stored inside the Phone's flash memory; and like NimicsCrypt they cannot be reviewed without the personal PIN even if the phone or microSD is stolen or confiscated. NimicsCrypt also encrypts any data files or photographs selected and allows to store them securely in the phone, on the microSD flash memory or using cloud storage.

Voice scrambling & instant messaging between private groups of NimicsCrypt phones and NimicsCrypt Tablet Users. Groups can be as small as two people or communities of many thousands. Ideal for high profile personalities in Special Services and Security Departments. The address book and call history are encrypted and stored inside the microSD flash memory, they cannot be reviewed without a PIN even if the phone or the NimicsCrypt or microSD is stolen or confiscated. (Five invalid PIN attempts and all information is locked forever).

Special configurations are available with complete SIP server and RTP relay ownership. Bridging (gateway) options allow interfacing with existing office wire phones. Everything is 100% under the systems owner's control.

Capability Need Bandwidth 3.2Mbps (both Uplink and Down link) to support up to 200 concurrent calls.

NimicsCrypt Server Features

- SIP
- RTP Relay
- Registrar Service
- Call Routing
- NAT Traversal
- Dial Plan
- Authentication
- Session Management
- TCP Transport Support
- UPnP
- Presence Agent support - RFC 3856
- XCAP support for Presence Agent -
- RFC 4825 Logging capabilities
- Supports Radius

Security Features

Protects against the exploitation of SIP protocol vulnerabilities, as well as SIP server non-vulnerability-based threats including:

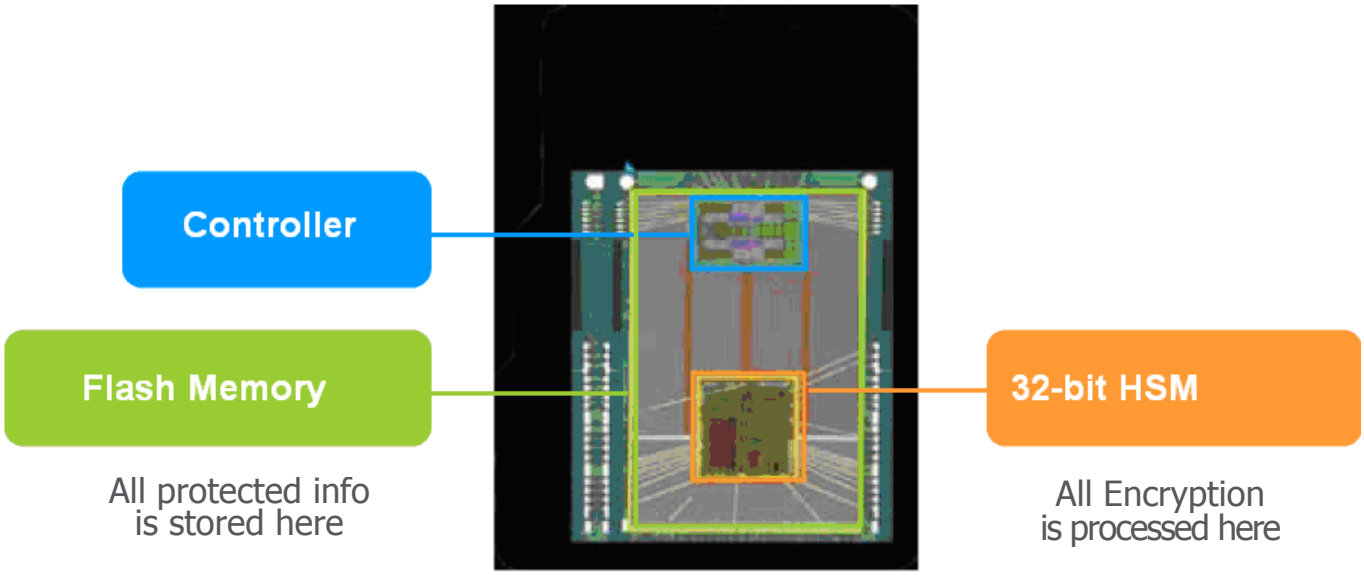
- **SIP server resource misuse**
- **SIP application brute forcing SIP Application**
- **scanning SIP application**
- **flooding**

Requirement of DataBase

MySQL recommended. Any other relational Data-Base will also work.

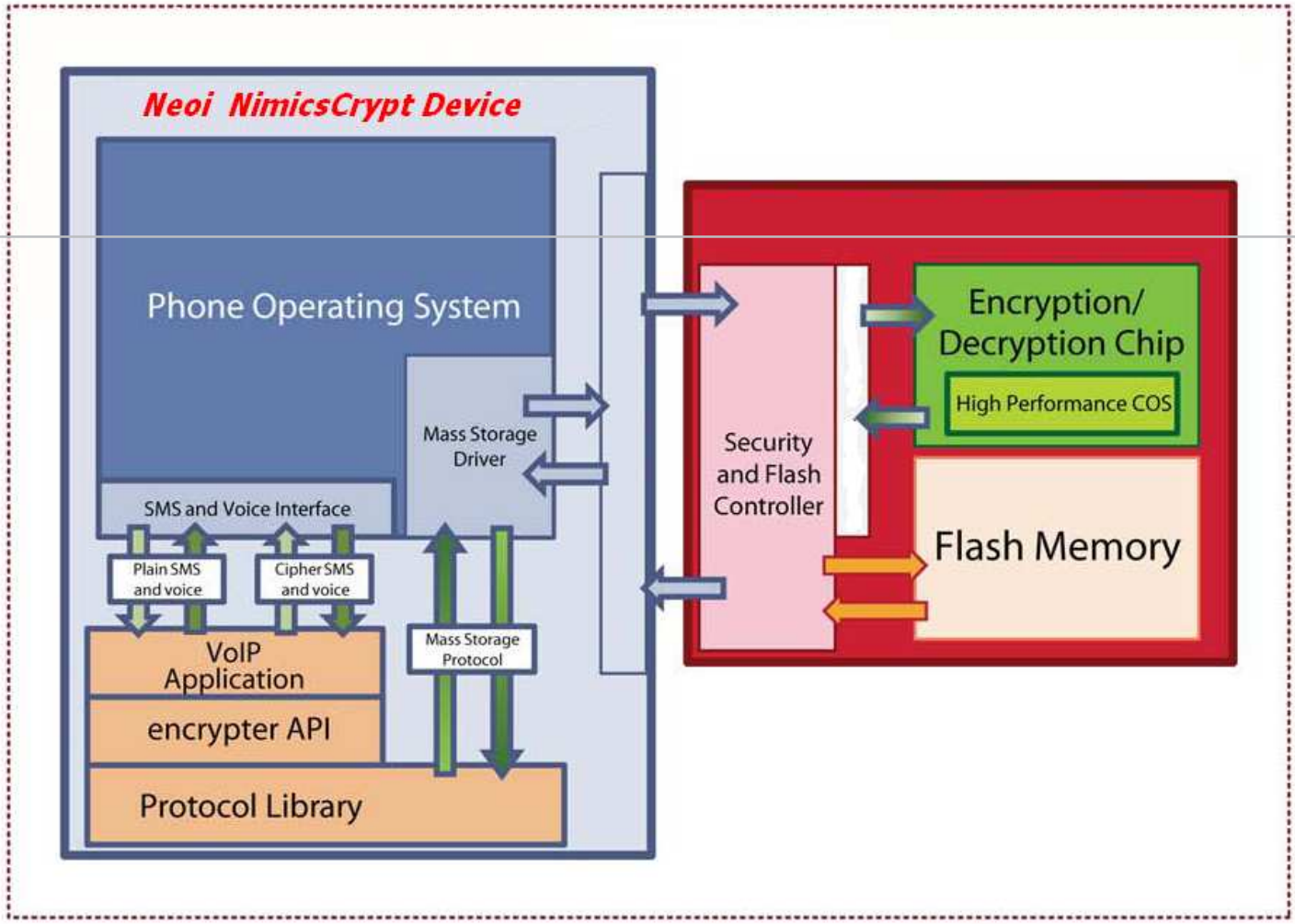
Hardware Security is inside a special chipset

All your communications and files are protected by a military strength hardware security module embedded inside the Neoi Phone. No secure operations take place in the open in your smart phone's operating system, they all take place hidden deep inside the device.



Technical Specification

- **32-bit Security chip inside the secure device is certified by Common**
- **Criteria EAL 5+ In –Chip Crypto Operations: RSA 2048, SHA256,**
- **AES-256, Key Exchange.**
  AES encryption module is certified by
- **NIST in the USA Secure device certification of FIPS 140-2 Level 3 (military grade in the USA).**
- **RSA Key pair is generated by the secure device and the private key is never**
- **exposed. No confidential keys are stored or computed in the device**
- **Voice encryption key (session key) is generated by a True Random Number Generator and exchanged by RSA and DiffieHellman.**
- **Voice encryption key is completely random and different for each phone call and instant messaging.**
- **Voice is encrypted by the AES-256 session key and the operation is done inside secure device.**
- **Security chip is able to withstand physical attacks.**
- **VoIP is based on standard SIP Technology.**



Against Trojan attack

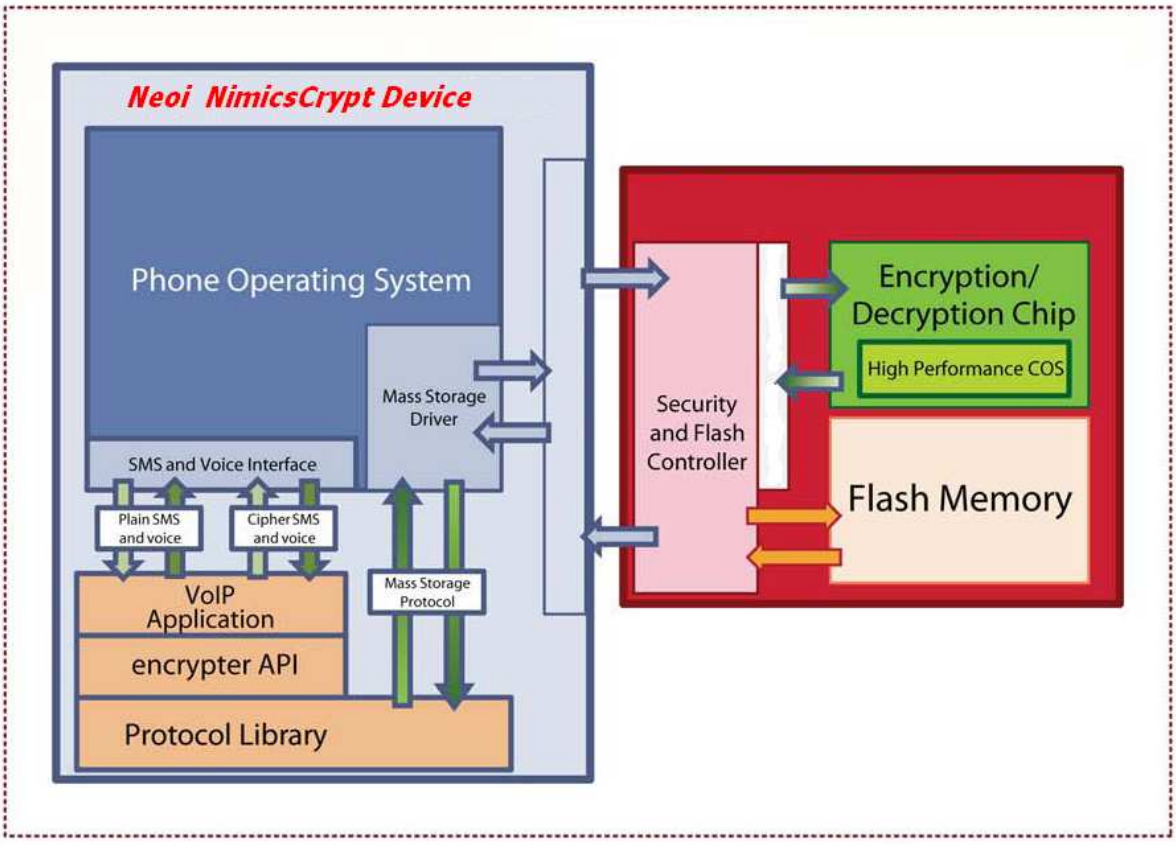
Against man-in-the-middle attack

Against eavesdropping

Against physical attack

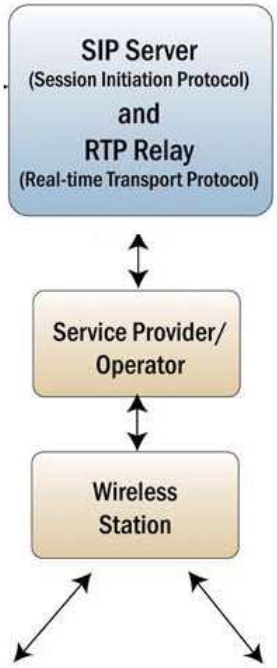
Product Features

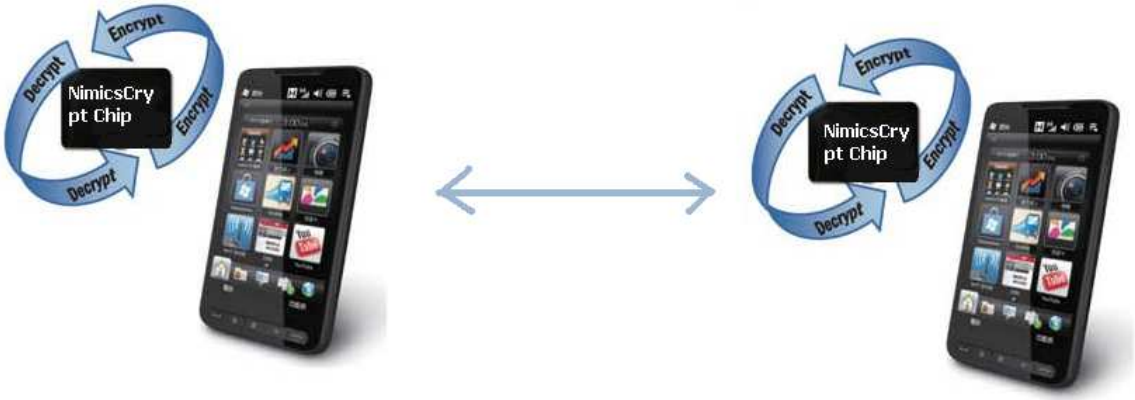
Feature	NimicsCrypt	Nimics Audio	Nimics Text
Voice Encryption	●	●	—
Instant message Encryption	●	●	—
Voice Address Book Encryption	●	●	—
SMS Encryption	●	—	●
SMS History Encryption	●	—	●
SMS Address Book Encryption	●	—	●
File and Photo Encryption	●	—	●
Secure Cloud Storage options	●	—	●
Military Strength Encryption	●	●	●
Common Criteria EAL 5+	●	●	—
AES Encryption key length	256/1	256	128
New random key per session	●	●	—



NimicsCrypt Call

is the best choice to secure your phone calls.





NimicsCrypt – Mobile Communications

Security has never been better!