Document beginning

"SecureScrypt" also known as "SSCSIM" (SIM card based / integrated Voice Data encryption developed by Neoi Technology Partners and / or Bernhard Bowitz)

Different from SD Card based solutions of earlier SecureScrypt versions, which did not allow a removable Media in Iphones, the SSCSIM version now allows a removable Media (SIM) on Iphones and so allows on all Hardware to remove critical files and Software completely from the Hardware and block all hackers from intruding into the encrypted files and media.

The SSCSIM or SecureScrypt is a combination/integration of Voice-Data encryption based on 256AES or higher*

1. * (The **Advanced Encryption Standard** (**AES**), also referenced as **Rijndael)** , Diffie Hellman (**Diffie–Hellman** key exchange (D–H)**

** a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle) code, the SecureScrypt/Crysp encryption code (SSCSIM)***

*** an algorithm developed by Neoi Technology Partners****

**** Neoi is the registered Brand name of Bernhard Bowitz , Germany and Neoi Technology Holding Pte. Ltd. a Software and Hardware development partnership located in Germany and Singapore with the developed and assembled quell code (SSCSIM) integrated into a SIM Card*****.

***** A (**SIM**) **subscriber identity module** or **subscriber identification module** is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

The SecureScrypt/Crysp (SSCSIM) Quell code is an advanced version of above cited AES, Diffie Hellman, Neoi Tec algorithm, with elliptic and/or symmetric/asymmetric Voice/Data encryption and SQL / Cassandra Data base.

The new development is integration of the quell / source code into a SIM Card, therefore allowing a higher standard of security / encryption in mobile P2P / P2Proxy2P mobile and fix line communication and Data traffic.

Using the standard security of SIM card hardware allows this advanced security standard (SSCSIM) developed by SecureScrypt / Crysp / Neoi developers.

***** The SIM circuit is part of the function of a Universal Integrated Circuit Card (UICC) physical smart card, which is usually made of PVC with embedded contacts and semiconductors. "Sim cards" are designed to be transferrable between different mobile devices. The first UICC smart cards were the size of credit and bank cards; the development of physically smaller mobile devices prompted the development of smaller SIM cards where the size of the plastic carrier is reduced while the electrical contacts remain the same.

A SIM card contains its unique serial number (ICCID), international mobile subscriber identity (IMSI), security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to and two passwords: a personal identification number (PIN) for ordinary use and a personal unblocking code (PUK) for PIN unlocking and the (SSCSIM).

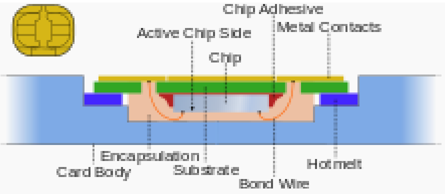
The (SSCSIM) is manufactured for licensed SIM card providers under the additional license of Neoi Technology to integrate the SSCSIM quell code. License will be provided by Neoi Technology to Partners contracted by Neoi Technology. Integrating the encryption code SSCSIM is a new unique way of Voice and Data encryption and first been developed and copyright protected by the above and undersigned Bernhard Bowitz and / or Neoi technology Holding Pte. Ltd. /Partners.

More technical information for components and Software codes used in the development and are required to allow a certified and licensed partner to offer the SSCSIM.

The SIM was initially specified by the European Telecommunications Standards Institute in the specification with the number TS 11.11. This specification describes the physical and logical behavior of the SIM. With the development of UMTS the specification work was partially transferred to 3GPP. 3GPP is now responsible for the further development of applications like SIM (TS 51.011) and USIM (TS 31.102) and ETSI for the further development of the physical card UICC.

The first SIM card was made in 1991 by Munich smart-card maker Giesecke & Devrient, who sold the first 300 SIM cards to the Finnish wireless network operator Radiolinja.

Design



SIM chip structure and packaging

There are three operating voltages for SIM cards: 5 V, 3 V and 1.8 V (ISO/IEC 7816-3 classes A, B and C, respectively). The operating voltage of the majority of SIM cards launched before 1998 was 5 V. SIM cards produced subsequently are compatible with 3 V and 5 V. Modern cards support 5 V, 3 V and1.8 V.

Modern SIM cards allow applications to be loaded when the SIM is in use by the subscriber. These applications communicate with the handset or a server using SIM application toolkit, which was initially specified by 3GPP in TS 11.14 (there is an identical ETSI specification with different numbering). ETSI and 3GPP maintain the SIM specifications; the main specifications are: ETSI TS 102 223, ETSI TS 102 241, ETSI TS 102 588, and ETSI TS 131 111. SIM toolkit applications were initially written in native code using proprietary APIs. In order to allow interoperability of the applications, Java Card was taken as the solution of choice by ETSI. Additional standards and specifications of interest are maintained by Global Platform.

Data

SIM cards store network-specific information used to authenticate and identify subscribers on the network. The most important of these are the ICCID, IMSI, Authentication Key (Ki), Local Area Identity (LAI) and Operator-Specific Emergency Number. The SIM also stores other carrier-specific data such as the SMSC (Short Message Service Center) number, Service Provider Name (SPN), Service Dialing Numbers (SDN), Advice-Of-Charge parameters and Value Added Service (VAS) applications. (Refer to GSM 11.11.)

SIM cards can come in various data capacities, from 32 KB to at least 128 KB. All allow a maximum of 250 contacts to be stored on the SIM, but while the 32 KB has room for 33 Mobile Network Codes (MNCs) or "network identifiers", the 64 KB version has room for 80 MNCs.[citation needed] This is used by network operators to store information on preferred networks, mostly used when the SIM is not in its home network but is roaming. The network operator that issued the SIM card can use this to have a phone connect to a preferred network, in order to make use of the best commercial agreement for the original network company instead of having to pay the network operator that the phone 'saw' first. This does not mean that a phone containing this SIM card can connect to a maximum of only 33 or 80 networks, but it means that the SIM card issuer can specify only up to that number of preferred networks; if a SIM is outside these preferred networks it will use the first or best available network.

ICCID

Each SIM is internationally identified by its integrated circuit card identifier (ICCID). ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalisation. The ICCID is defined by the ITU-T recommendation E.118 as the*Primary Account Number*. Its layout is based on ISO/IEC 7812. According to E.118, the number is up to 22 digits long, including a single check digit calculated using the Luhn algorithm. However, the GSM Phase 1[4] defined the ICCID length as 10 octets (20 digits) with operator-specific structure.

The number is composed of the following subparts:

Issuer identification number (IIN)

Maximum of seven digits:

- Major industry identifier (MII), 2 fixed digits, *89* for telecommunication purposes.
- Country code, 1–3 digits, as defined by ITU-T recommendation E.164.
- Issuer identifier, 1–4 digits.

Individual account identification

- Individual account identification number. Its length is variable, but every number under one IIN will have the same length.

International mobile subscriber identity (IMSI)

SIM cards are identified on their individual operator networks by a unique International Mobile Subscriber Identity (IMSI). Mobile network operators connect mobile phone calls and communicate with their market SIM cards using their IMSIs. The format is:

- The first three digits represent the Mobile Country Code (MCC).
- The next two or three digits represent the Mobile Network Code (MNC). Three-digit MNC codes are allowed by E.212 but are mainly used in the United States and Canada.
- The next digits represent the Mobile Subscriber Identification Number (MSIN). Normally there will be 10 digits but would be fewer in the case of a 3-digit MNC or if national regulations indicate that the total length of the IMSI should be less than 15 digits.
- Digits are different from country to country.

Authentication key (K_i)

The Kn_i is a 128-bit value used in authenticating the SIMs on the mobile network. Each SIM holds a unique K_i assigned to it by the operator during the personalization process. The K_i is also stored in a database (termed authentication center or AuC) on the carrier's network.

The SIM card is designed not to allow the K_i to be obtained using the smart-card interface. Instead, the SIM card provides a function, *Run GSM Algorithm*, that allows the phone to pass data to the SIM card to be signed with the K_i. This, by design, makes usage of the SIM card mandatory unless the K_i can be extracted from the SIM card, or the carrier is willing to reveal the K_i. In practice, the GSM cryptographic algorithm for computing SRES_2 (see step 4, below) from the K_i has certain vulnerabilities[5] that can allow the extraction of the K_i from a SIM card and the making of a duplicate SIM card.

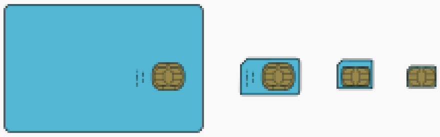
Authentication process:

1. When the Mobile Equipment starts up, it obtains the International Mobile Subscriber Identity (IMSI) from the SIM card, and passes this to the mobile operator requesting access and

authentication. The Mobile Equipment may have to pass a PIN to the SIM card before the SIM card will reveal this information.

2. The operator network searches its database for the incoming IMSI and its associated K_i.
3. The operator network then generates a Random Number (RAND, which is a nonce) and signs it with the K_i associated with the IMSI (and stored on the SIM card), computing another number known as Signed Response 1 (SRES_1).
4. The operator network then sends the RAND to the Mobile Equipment, which passes it to the SIM card. The SIM card signs it with its K_i, producing SRES_2, which it gives to the Mobile Equipment along with encryption key K_c. The Mobile Equipment passes SRES_2 on to the operator network.
5. The operator network then compares its computed SRES_1 with the computed SRES_2 that the Mobile Equipment returned. If the two numbers match, the SIM is authenticated and the Mobile Equipment is granted access to the operator's network. K_c is used to encrypt all further communications between the Mobile Equipment and the network.
6. The SSCSIM quell code will be loaded and identified with the SecureScrypt/Crysp node, starting the encryption protocol and process.

SIM card Formats Samples



Full-size SIM (1FF), mini-SIM (2FF), micro-SIM (3FF) and nano-SIM (4FF)

SIM card sizes

SIM card	Introduced	Standard reference	Length (mm)	Width (mm)	Thickness (mm)	Volume (mm³)
Full-size (1FF)	1991	ISO/IEC 7810:2003, ID-1	85.60	53.98	0.76	3511.72
Mini-SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25.00	15.00	0.76	285.00
Micro-SIM (3FF)	2003	ETSI TS 102 221 V9.0.0, Mini-UICC	15.00	12.00	0.76	136.80
Nano-SIM (4FF)	early 2012	ETSI TS 102 221 V11.0.0	12.30	8.80	0.67	72.52
Embedded-SIM		JEDEC Design Guide 4.8, SON-8	6.00	5.00	<1.0	

SSCSIM state of the art specifications :

- SecureScrypt/Crysp a globally functioning encryption solution

- Crysp High end Voice/Message/Data Encryption- Software Version for all platforms (Android 3.0+,Iphone 4+,Windows, Nokia(Smart), Blackberry (Android4+), Laptop(with USB Adaptor, Desktop Android Phone.

- SecureScrypt same as Crysp, are now available with enhanced security SSCSIM and/or SD card security
  - Secure phone calls and sending messages via all platforms
  - communication in all networks, wireless internet and satellite connection

  The SecureScrypt brings one of the first providers for worldwide usage, a mobile encryption solution for Smart phones on the market.

  The solution Mobile Encryption APK for Android, Blackberry, Nokia, Windows and iOS devices works in contrast to other solutions in any phone network **and even without a GSM SIM card function , even via wireless or a satellite link.**

  Even in countries where the calls will be blocked via the Internet, SecureScrypt SSCSIM can help with the solution to communicate encrypted.

  The Solution only requires a bandwidth of 12,2 kbit net and works so well in areas with poor wireless networks. The SSCSIM Mobile Encryption is the currently strongest encryption methods on the markets that are considered unbreakable even by expert cryptographers in the foreseeable future. The solution is intended for large Governments and Agencies, business customers, small businesses and home users, networks, hardware manufacturer and branded mobile manufacturers.

The encryption can also be used on laptops, PCs, using a small USB adapters, and thus makes the ENTIRE system compatible with communication companies worldwide.

"Protecting private data, is for most companies now taken for granted. When it comes to making calls and sending text messages, many do not know of their protection requirements , however, just now they are beginning to realize. We offer these companies a simple, affordable and stable solution, as their employees can communicate safely mobile, "says Dr. Bernhard B., Head of Business Unit Cyber Security within the parent company Neoi Technology. The areas of application of such a solution are multiple, emphasizes B .: From secret treaty negotiations or discussions to business combinations, on research and development to witness protection programs should be encrypted communication a must essential.

SecureScrypt encrypts as the only available solution which debuted on the market even secret video conferencing, data and also the operational company / Government / internal networks, phones worldwide.

If two users want to communicate with the new solution, it is sufficient that both have installed the Mobile Encryption app on their Smartphone. A customized technical infrastructure in the background is not necessary. The communication partners do not have to be customers of the same wireless service provider also, the encryption solution works with any vendor. "We have chosen deliberately to offer an as flexible product as possible, which is especially interesting for our multinational customers," says Dr. B. The keys that allow to solve secure communications are exclusively generated on the users smart phones and even deleted after a call immediately. They are thus always and exclusively in the hands of the user and therefore completely independent from the network operator.

This principle exclude that third parties in a communication engage ("Man in the middle attack"). In addition, the contact details, messages, and texts in the app are encrypted as in a secure container and then stored on the Smartphone separately. For the reading of the confidential information, a password is required.

As for highest security in addition for highest secrecy, SecureScrypt offers the possibility to the keys, data, etc. on a special SIM (SecureScrypt internally named SSCSIM (C)) represented by a special embedded chip to store. Thus, the user can remove the SIM card from the phone and it will remain NO data on the Smartphone. The SIM card renders automatically useless, if it is removed from the phone, even if the phone is lost or separated, none of the devices remain in secure function. The Smartphone is the plain old telephone unsafe again.

Why is SecureScrypt such a big deal? *Independent experts* inform that its SSCSIM Security Card is "a mini-computer integrated into the SIM" that "contains something similar NXP SmartMX P5CT072 crypto-controller with a PKI coprocessor for authentication" and features "an additional high-speed coprocessor encrypts voice and data communication using 256 bit AES." In plain English, this means that SecureScrypt's top product has multiple layers of security to keep voice and data communications safe.

This is particularly important because in the wake of the massive NSA spying scandal, many governments around the world have been reluctant to trust American companies such as Microsoft and Google when it comes to keeping their data safe. While there aren't many people who need a Smartphone that's as secure as ones that are equipped with the SecureScrypt SSCSIM, the people who do need it are a potentially profitable niche. After all, both U.S. president Barack Obama and German chancellor Angela Merkel both only use Smartphone devices for mobile communications since no other devices have yet proven themselves up to snuff.

The Mobile Encryption App for Android, iOS and all other devices work in any phone network. The solution is available for everyone and is very cost effective because no new hardware (mobile phones, etc.) pieces must be purchased. It is part of a modular system of complementary and cumulative products of SecureScrypt group for secure communications, such as centralized management of mobile devices, the company's internal telephone and data network or particularly developed (e.g. tropical Secure, Mil grade, water protected) includes Smartphones.

The data of the system summarized:

- Developed by the Neoi Group in Germany as SecureScrypt product, a technology leader in mobile voice and message encryption with more than 25 years worldwide experience
- Solution is valid for all clients traveling on business, Enterprises, Governments, even Police and Military and all service areas worldwide.
- costs very low , affordable for any level.
- No additional investment needed in infrastructure
- app runs on Android and Apple devices, and Windows, BlackBerry and Nokia, IP landline phones, mobile and stationary, even on laptops un PCs
- Robust solution anywhere, work reliably worldwide unlimited!

Communication even with a limited network throughput and even if VoIP blocked in certain areas or the quality is even normal GSM, it works perfectly..

SecureScrypt only requires bandwidth of 12.2 kbit net, works so well in areas with poor power supply (eg 2G networks in developing countries), suitable as a network are LTE, GPRS, 4G, 3G, 2G, Wifi etc.

- Keys are generated solely on the devices themselves and are deleted after the call is ended immediately.
- Additional security SSCSIM.
- No pre-installed and thus predictable keys
- Solution uses the strongest encryption methods currently on the market
- Redundant encryption algorithms on two parallel paths
- Works independently from a particular mobile operator and also entirely without a SIM card in the wireless network or via satellite link
- use on the current device of the owner possible. No secondary device required no additional hardware

Features Summary:

- **Encrypted voice communications (focus: wireless networks)**
  1:1 (P2P) calls and mobile conference calls (arbitrary number of participants)
- **P1Proxy2P communication in countries were blocked P2P**
- **VoIP based on UDP (connectionless)**
  State-of-the-art encryption mechanisms
  No draw-backs in system integration and use of standard phone features
  e.g. phone book / contacts, concurrent operation with other not encrypted applications, common not encrypted phone calls
- **Full encryption of Data , Documents, Video, Pictures and other Data traffic**
- **Intuitive graphical user interface and use of the standard function keys and Automatic connection establishment as requested by partners and users**

- **Mobile: WiFi, UMTS, EDGE, GPRS, Fixed line: LAN (where suitable)**
- **Key exchange: Diffie-Hellmann 1024-4096 Bit**
  User data encryption: AES 256 Bit
  Secured end-to-end connectivity (P2P) (man-in-the-middle prevention)
  Authentication: IMEI, PKI, verbal feedback of individual session fingerprints
- **Removable media with SSCSIM or SD-Card, leaves not even a trace of any data or communication or logs.**
- **encrypted local data in a safe location of the device (SSCSIM or SD-Card)**
- **Nurugo (FidoScrypt) password less authentication process for all functions with bio-metric access control**
  Centralized session management, etc.
  Dynamic access control at the routing server

About the SecureScrypt:
The SecureScrypt a German company, which has manufactured already in the 80ties special satellite phones with encryption.
Today the administration sits in Singapore, and uses the global Capacity of about 70 software and hardware experts to develop such solutions as SecureScrypt (Made in Germany). **The unique thing about SecureScrypt is that every system sold is completely different, and it is therefore impossible that one can possibly compromise an existing system technically then invade other SecureScrypt systems.**

A "hacking" of SecureScrypt SSCSIM is not only pointless, but completely useless.
For further questions or a personal confidential meeting please contact us at:
info@securescrypt.com Thank you, The company Management

Document end