SecureScrypt(C) 2015

White paper on the question of data and communications security.

The “man in the middle” must stay outside!

January 2015 - NEWS

- SecureScrypt with a worldwide functioning encryption solution
- Secure phone calls, messaging, data and Video Call add on Application
- Communication in all Networks, Wi-Fi and satellite connection

The SecureScrypt brings a world-ready mobile encryption solution for Smartphones as add on onto the market as one of the first providers.

The so-called mobile encryption app for Android, BlackBerry, Nokia-, Windows- and iOS devices works in contrast to other solutions in any telephone network **and even without a SIM card over Wi-Fi or a satellite connection**.

Even in countries where the telephoning over the Internet will be blocked, SecureScrypt can communicate with help of its encrypted solution

The app requires only a bandwidth of 4 8kbit NET and thus also works in areas with poor networks and bandwidth supply. The mobile encryption app uses the currently strongest encryption methods on the market (even stronger then current MIL garde), which are considered by cryptographers as unbreakable. The solution addresses itself to large business customers, medium-sized companies and private users, Governments and Security Companies, para-military, police.

The encryption can be used also on laptops, PC, by means of a small USB adapter, and is worldwide compatible so the entire corporate communication network is secure and protected.

"To protect your own data, is now a must for most companies. When it comes to the voice calling and sending text messages, protection needs thinking only recently started. We offer a simple, low-cost and stable solution, your employees can communicate safely mobile , between mobiles and enterprise office networks without any worries of industrial espionage, says Dr. Bernhard B., head of the business unit cyber security within the parent company Neoi technology holding. The areas of application of such a solution are numerous, emphasizes B.: secret contract negotiations or discussions to mergers, on research and development, investments, high level discussions, to witness protection programs,etc., encrypted communication is essential.

SecureScrypt as only app launched on the market globally can even secret video conferencing, data and also the enterprise internal telephone network secure and protect.

If two users about the new solution want to communicate, it is enough that both have the mobile encryption app installed on their Smartphone. A customized technical infrastructure in the background is not necessary. The communication partner must also be non-customers of the same wireless service provider, the encryption solution works with any provider. "We have decided consciously to offer a most flexible product that is interesting even for our multinational customers", says Dr B.

The keys that enable secure communication with the solution, are generated only on the Users Smartphones themselves and are deleted when the call ends immediately. You are completely independent from the network operator always and operation is exclusively in the hands of the user. **This principle excludes that third parties in a communication link ("man in the middle attack") can enter the system.** Also, the contact data, messages and texts in the app are in a secure "container" encrypted and stored separately on the Smartphone. A password is necessary for reading of the confidential information.

As additional security for highest secrecy offers SecureScrypt the possibility, that the key, data, etc. is on a special SD card (SecureScrypt internally as ENIGMA(c)) stored with an integrated security chip developed by the Swissbit,. Thus the user can remove the SD card from the Smartphone and there are no data on the Smartphone left. The SD card renders automatically useless, the moment it will be removed from your Smartphone or if it or the phoneis lost, separated, none of the devices has left a function. The Smartphone is again the normal old insecure phone.

Some examples of devices with add on installed SecureScrypt

The mobile encryption app for Android, IOS and all other devices work in any telephone network.

The solution is available to everyone and is very cost-effective, since no new equipment must be purchased. It is part of a modular system, that compliments and each other, based on products of the SecureScrypt group for safe communication. Such as a centralized management of mobile devices, the company internal telephone and data network or even particularly developed (IP67 and higher standards, MIL-grade, water protected) includes Smartphones.

Summarized data of the system:

- Developed by the Group in Germany as a SecureScrypt product, a technology leader in the field of mobile voice and message encryption with more than 25 years of global experience developed by the Neoi
- Offer is valid for all business and service areas, for every company size
- Very low cost
- No additional investment in infrastructure necessary
- App runs on Android and Apple devices, as well as Windows, BlackBerry and Nokia, IP landline phones, mobile and stationary, even on laptops and PC
- Robust solution which reliably, works everywhere all over the world!:

  Communication even with restricted network throughput and even if is blocked VoIP in the operational area or regulated by a service provider.

  App needed only bandwidth of 4 8kbit NET, GPRS, 4 G, 3 G, 2 G, LTE, WiFi etc. are thus also works in areas with poor network bandwidth supply (E.g. 2 g networks in developing countries), suitable for use as a private network
- Keys are generated only on the devices themselves and deleted when the call is ended immediately.
- Additional security through SD card with an embedded chip.
- No pre-loaded and thus unpredictable key
- Solution deploys the currently strongest encryption methods on the market
- Redundant encryption via two parallel algorithms
- Works independently from a specific mobile operator and also completely without a SIM card in the Wi-Fi network or satellite connection
- Use the owner's device , no new or additional hardware required.

You get here (http://securescrypt.com) a more detailed information of the encryption solution.

About the SecureScrypt
The SecureScrypt is a German company, which already in the 80 years has specialized in the design and manufacturing of encrypted satellite phones.

Today, sits the Administration in Singapore, and uses the global capacity of approx. 70 software and hardware experts, to develop such solutions as SecureScrypt. The unique of

SecureScrypt is that any selling system is completely different, and it is impossible so that you can disassemble an existing system may be technically and then use it in other SecureScrypt systems to penetrate. A "hacking" of SecureScrypt is not only pointless, but totally useless.

For further information or a personal consultation, please contact:

info@securescrypt.com

thank You very much for Your kind attention

the Executive Board

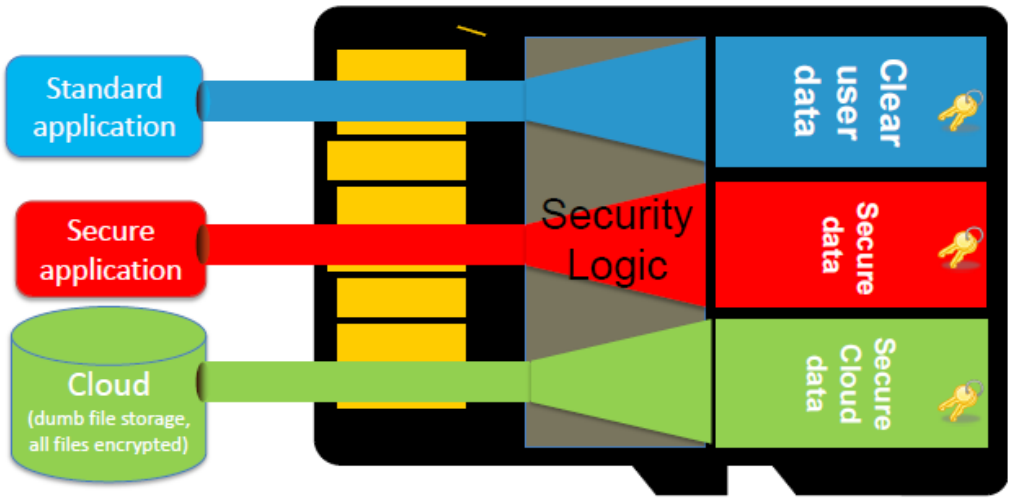
Cyber Security Group SecureScrypt

© 2015 Neoi Technology Holding Germany

Technical supplemental information:

ΣΔ14ΕΝΙΓΜΑ

SDCard PS100SEV14 Enigma



The German made SDCard PS100 with its special build in Security Chip is the key element for securing Android, Windows and Linux based Smartphones with Enigma / SecureScrypt systems.

Enterprise Security at new Levels, Enterprises need SECRECY for SUCCESS!

Existing SmartPhones/Iphones either private or Enterprise owned will be 100% secured with the SecureScrypt Enigma engine.

Base on the WW2 Myth that Germany had the ultimate unbreakable Encryption Machine, which never was broken only after Allied Forces captured an Enigma, the SecureScrypt Digital Enigma Machine cannot be broken, even if someone gets a copy of …. Yes of what? The secret is, there is no digital or otherwise copy possible, each SecureScrypt Enterprise System is completely different and customized from each other.

Security of this level has never been reached before!

Enterprise (or Government) Internal Installation

- **With this Solution, all necessary backend-components are hosted and installed in the Enterprise's Datacenter. This offers ultimate advantages to the Enterprise**
- **Strictly follow Enterprise's internal management rules**
- **No one external has access to the system and server only selected Enterprise employees or managers have access.**
- **Peer-to-Peer secured communications between registered and authorized Mobiles**
- **And now also to / from the new SecureScrypt Neoi Desktop wireless Phone, with large Message Display and PABX Interface to communicate securely with fix line subscribers**
- **No more IDD or roaming charges at all, The GSM section of the Phones is not needed, or used for standard unsecured communication**
- **Secure landing, communications from overseas becomes secured by using WiFi or 3G/4G/LTE. The most secure way is using the Enterprises WiFi or an external WiFi Network**

BUSINESS UNITS

DRAM MODULES

DRAM modules for industrial applications
Component and wafer business
Small and complex form factors
Niches, legacy and customization

FLASH PRODUCTS

NAND Flash Products for industrial applications
Component and wafer business
Focus on small form factors, MCPs and advanced features
Niches, legacy, dedicated usage and customization

SECURITY PRODUCTS

NAND Flash Products for security applications
Component business
Focus on advanced security features with and without smart cards
Niches, dedicated usage and customization

WHAT IS A SECURITY PRODUCT?

A security flash memory product:

Offers security functions to protect data and/or provide security functions to the host

Provides standard function of flash memory data storage via SD/SATA/PATA/... Interfaces

Can be equipped with highest possible security by a smart card controller inside

Enables security solutions in various platforms like embedded PC, industrial automation systems, mobile phones, etc. without extra reader hardware needed

Featuring Real Time OS with customized applications inside the Flash Controller

Provides standardized ASSD and proprietary file based security interface

Example: secure microSD

Confidential

PS-100U IS VERSATILE

microSD token

- 4/8 GB flash memory
- smart card inside microSD highly certified (can be even consigned by customer for specific requirements)

- nano USB reader available at Swissbit
- suitable for key chain, lace attached
- all components available off the shelf

microSD approach ready for
- mobile
- tablet
- PC and
- LapTop

Confidential

PS-100U IS VERSATILE

microSD token

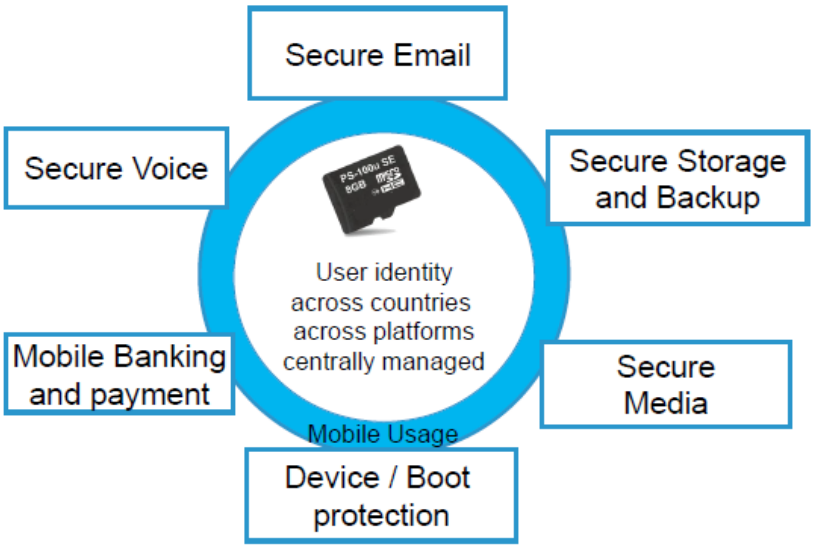
- 4/8 GB flash memory
- smart card inside microSD highly certified
  (can be even consigned by customer
  for specific requirements)

- nano USB reader available at Swissbit
- suitable for key chain, lace attached
- all components available off the shelf

microSD approach ready for
- mobile
- tablet
- PC and
- LapTop

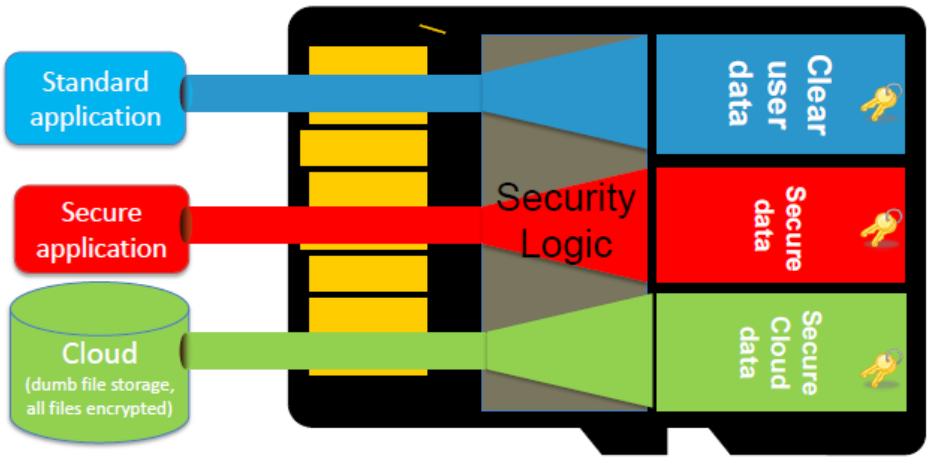
Confidential

MOBILE APPLICATIONS WITH SECURE MICRO SD CARDS



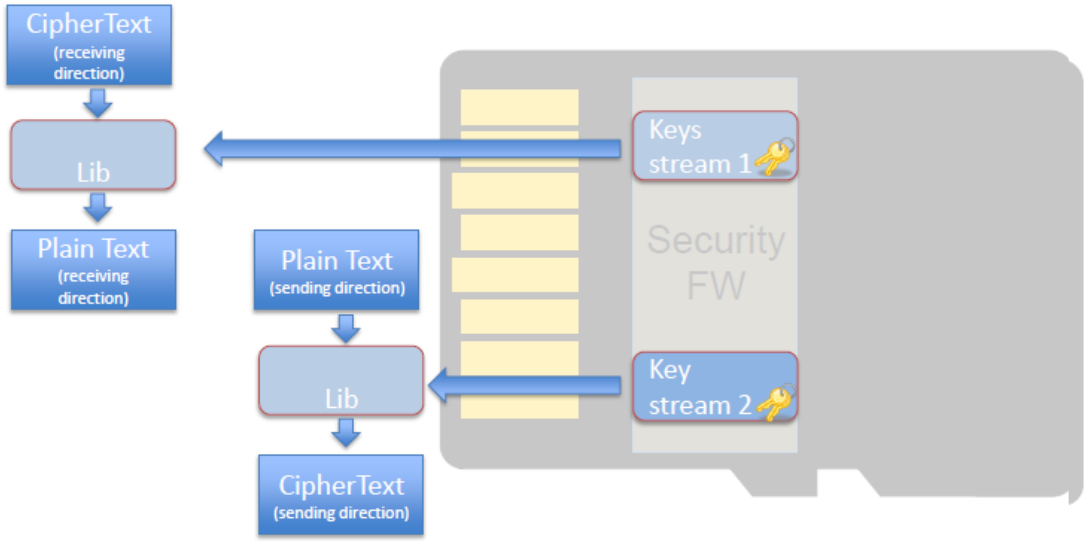
Confidential

OFFLINE DATA PROTECTION



OFFLINE DATA PROTECTION PATHS

ONLINE DATA ENCRYPTION (BIDECTIONAL)



SECURE MICRO SD MEMORY CARD

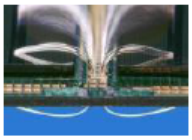
PS-100u SERIES

Compliance	SD 3.0 SD, ASSD V1.1
Data transfer	SPI mode supported, Speed class 10
Density	PS-100u 4 GB / 8GB
Temperature	Industrial temperature grade -40°C to 85°C
Performance	TBD
Features	SLE 78 smart card chip inside CC EAL 5+ HW and OS RSA up to 2048 bit, ECC up to 512/521 bit , SHA2 up to 512 bit
	Random number generator (FIPS, AIS31)
	Java Card 3.0, latest standard 80 k EEPROM for applets
Drivers / API	WinXP, 7, 8,Vista, Linux, BlackBerry, Android, ... SDK available

SERVICE OFFERING BEYOND THE FLASH MEMORY HARDWARE

Product related services
Customised security firmware and drivers
Customised logo printing
Optical and electronical personalisation

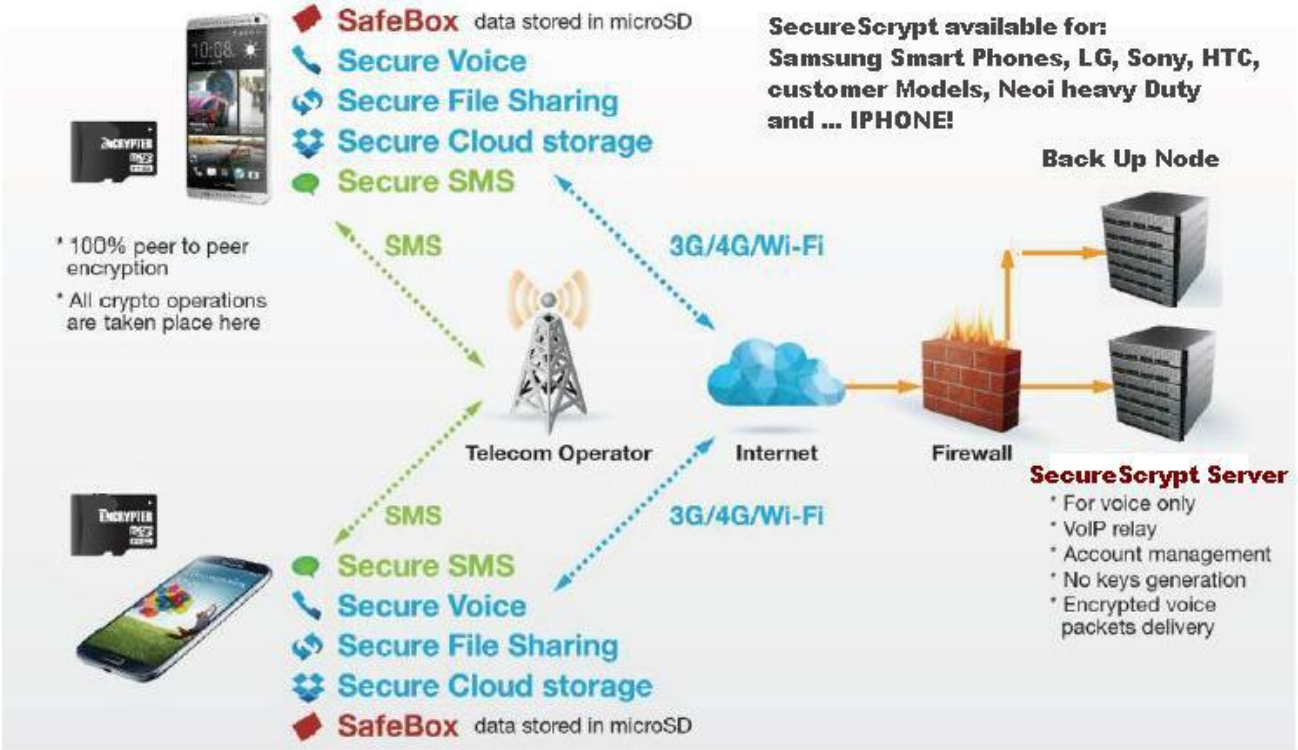
Extended Services
Security consulting and Training
Customer support
Design In Support
Connect with eco system partner network for turn key solutions and quick time to market
Prototyping



SecureScrypt

Closed Environment

SC will setup complete environment to customer side and the customer manages the servers. Appropriate concept for government, military, police, enterprise



Enigma and SecureScrypt are Copyright protected Product Names of Neoi Technology Holding Germany © 2015