SecureScrypt Confidential System Description for Enterprises and Governments

The SecureScrypt is a closed environment system, and will be installed by SecureScrypt engineers on site the Customers choice of Data Center.

It consists of 2 (3) Major "Components".

(1) The Secure Double Node Servers with its exclusive Engima Software
(2) The Secure SD Card for the Android (4.X Versions preferred)/Windows Mobile Phone Environment based on the SecureScrypt Enigma encryption engine.
(3) The special to be loaded Enigma Software package for selected Iphone Models

Introduction

Encryptions offered by Telcos (GSM/GPRS) are meaningless, as this are standard encryptions of the basic analog GSM connections and / or VoIP connections via 3G.
VoIP Providers use open lines and common servers, matter of fact Telcos who provide VoIP use the same Servers , encryption here is not available and would also render useless, the environment still remains completely open.
Telcos who offer so called secure Phones and Encryption, offer that in connection with their insecure Networks, Networks that are wide open for "The Man in the middle".

The only solution is to create for each user a new, different closed environment, user must become themselves a "virtual operator", operate and manage their own System.

Another drawback of current systems that are operated via an APK or other Software is, that if encryption takes place, it takes place in an open environment (Servers are managed by 3rd Parties) and because for real MIL grade encryption real peer to peer communication as a MUST standard, 3rd Party managed sytems are totally useless for encryption.
Several Software solutions that are offered as "Encrypted" communication are totally meaningless, as these Software solutions CANNOT protect securely communications.

The problem for a long time was, how to convert existing handsets in a way, that peer to peer communication in a completely closed , operator independent environment, can take place.

SecureScrypt (SC) and its partners in Germany developed the secure SD card as Hardware Component and the Enigma Software as Soft Component. This allowed now two totally independent working encryption components add together into a totally customized environment.
This solution now also allowed a Software Solution for Iphone which is missing in its O/S structure necessary SDCard/USB ports. SecureScrypt's solution is worldwide unique and guaranteed secured.

SC's Encryption method was also sanctioned by the German Governments extremely strict BSI (Federal Office for Communication Security-Germany) as Encryption for high level German Government Officials and Government/ Police Services.

BSI sanctioned the Software /Hardware combination as the highest standard suitable for Military, Governments, Police and Enterprises, because of the structure that SC is using a completely different environment / Software for each Organization, it exceeds even Securitystandards and protects 100% from any attack.
Currently SC is in certification process for the highest Government Secrecy Level "VS-NfD" once this is accomplished all SC customers will benefit of that.

SC uses a proprietary , special developed vaulted security chip in the SDCards and thru a new Solution transfers this into a special Software package securing selected Iphone Models.
SC is not a common IP calling solution, everything is proprietary together with the server package. The only standard used is the Internet as transport media between 2 subscribers, Peer-to-Peer.

Operation principal

SC is based on peer to peer encryption and uses secure tunnels for voice and data.
Key exchange is strictly between two subscribers handsets, keys are not recorded.

Security

The actual crypto operation is not released as information for security reasons and to protect SC subscribers. An initial session key is generated for connection via the Server, from there the private keys are randomly generated at a very high frequency inside the SD chip, no key is ever recorded or stored inside the handset.

Subscriber registration

Once a SC subscriber buys a license (license means the SDCard or the Software package) an initial code will be sent once via SMS or Data connection to the Server, the server generates a special registration information using the handsets MAC/IMEI and Phone number. (Since this process of registration is customized from system to system, registration might be different from the basic standard). This method makes sure that Software or Hardware cannot be moved from one handset to another, which would be another Security risk. Any attempt to move the Software / Hardware between handsets will void the license immediately and render it useless.

Server function

The SC Server handles only the initial connection request between 2 subscribers (clients), redirects the connections accordingly so that the two concerned subscribers can set up the peer to peer tunnel connection, There will be no trace of the actual communication on the server. (This is a major difference from other so called Encryption Providers, who all use public open Servers which then store all kind of connection Data, logs, etc. which can be accessed later to trace communication data which actually should be secured and not available to anybody)
Customers are recommended to use complete new server hardware with the SC installed software, and connect / host in their Data center or selected environment, but SC can also install the Software on an existing Server in the Customers Data center. Management of the Server will be handed over to the customer, but in rare instances SC might sign a management contract with the Customer.

Connectivity

Subscriber Handsets can connect to a Data Backbone (Internet) from anywhere in the world. Connection to the Internet preferred is WiFi, WiFi cells have a very small operation radius, which again adds to the security and prevention of hacker attacks. So 3G and 4G connection are also possible, due to the nature of 3G/4G cells, tracking a location of a handset could be possible in very rare circumstances. Typically WiFi access point in companies, are the most secured way of connecting SC to the Internet. A nice commercial side effect is, that SC handsets can make calls from anywhere in the world, without any long-distance cost, no roaming charges or other Telco charges. Secure and very low cost Calls = SC.

Implementation

Once a customer orders a SC system, SC will consult with the customer to create a customized Software (Enigma), a customized UI (Dialer Interface) customized hardware (SDCards) to crate a unique package, so that no one SC system created is ever the same.
Customers customization wishes and requests will be discussed during the quotation and order processing.
SC engineers will install the Server at the customers location and hand over. SC will keep records for SDCard customization, so that customers can order at anytime more licenses for their system. All charges are one time.
Customer may request a SC management, which will be subject to separate charges.
Warranty and Updates are lifelong. Additional training sessions for customer personal after the initial training at hand over are subject to additional charges.

Current Users of SecureScrypt solutions:
German Government, Italian Government, 2 big German Enterprises, Border Police in several countries, Police Organizations in France, Switzerland, Belgium, Customs. Other Users are protected by very strict NDA and may not be revealed.

For any information please contact: info@securescrypt.com