«SSG Phone»
is the phone protected* from the tapping and interception of information

Target audience: The first person's states, representatives of power structures of the highest level, the secret services, the military, the PMCs, security organizations, financiers and attorneys.

** The protected phone means the smartphone or tablet based on the Android/Ubuntu platform with a unique firmware.*
Security features from all major threats of data transfer over networks GSM / UMTS / LTE / Wi-Fi are realized by installing special operating system and software.

Description

The firmware (the operating system or OS) must be written in taking into account the verification of Android source code on the presence of internal tabs that allow you remotely manage any telephone anywhere in the world - using the hidden modules, such as Galileo (talking about lawful interception means that some hidden modules in OS legally deliver the authorized access to the private data area for government attorneys). We need the detailed verification of Android source code by the professional native Android developers with close cooperation with professionals in the area of practical IT security. The OS must have no pre-standard software, Google Play, etc.

Each time OS must be loaded from the internal memory module of the smartphone in his RAM following the example of similar systems for the PC like live CD/USB. The key point is to make impossible to restore any service information used by the system during a working session, after reboot or shutdown. Therefore call lists, SMS, personal dictionary keywords, e-mail, the browser history, and other data used in a particular session of the device are protected - so there is a complete ban on the recording device's internal memory on the OS and hardware levels.

All the necessary programs will have already been pre-installed in the device's OS. Internet access will be tightly controlled by built-in firewall with port and host filters. Also there will be an access to the protected remote server wherein the access to the network is carried out only by active VPN connection.

The device shutdown option is necessary to be implemented at the hardware level, that is meant unusual software disabling the standard Android OS features such as camera, mobile communication units, Wi-Fi, A-GPS, and also the lawful interception module (allowing the implementation of background mode work of the device as a microphone for remote voice data interception) and complete turn off the device in which it is physically impossible reception and transmission of any data.

It is also necessary to forbid the downloading and installation on user device third-party applications, wherein on the hardware level the inclusion of these functions have to be protected by complex's administrative password to secure the user from accidental, reckless actions.

If some features cannot be restricted by using official firmware, it`s necessary to eliminate them physically - for example A-GPS module or the camera can be removed from the device.

At creation of phone we need to realize the maximum protection, as if it was used in the area of war or anywhere else with a potentially unsafe IT infrastructure. In other words if your opponent will intercept the whole communication data streams, he will not be able to decrypt them, as well as infect remotely the device by spyware or extract the information in case of physical smartphone`s seizure.