Secure Phone: a new way of private voice and text communication

A suite of new hardware and software technologies to protect your right to privacy of correspondence

End-to-End Encryption

RSA 4096 asymmetrical keys

AES-256 block encryption

A new key is generated for each session

Private key (RSA) is generated on first activation and is securely stored on your phone

Users can generate a new key at any time for any reason for additional security

Custom kernel

Our custom kernel includes only the absolute minimum required for functionality and has been designed with security as the primary consideration.

MITM attack shield

We implement our own algorithm for protection against MITM attacks. We do not rely on the conventional CA-authority. Our certificate is hard-coded into the software, CA-root private key is created on a computer with an air gap.

Android based

Android-based proprietary features are kept to a minimum and are quarantined in their respective drivers.

Peer to peer connection

Voice connection occurs in a peer-to-peer model directly between subscribers. In the case of symmetric NAT from your

ISP, we use our servers as a proxy. All data is encrypted end-to-end.

voiceless GSM

GSM module is used only for the Internet connection. Flash SMS, MMS, SMS provider attacks and attacks with malicious programs sent via SMS/MMS are prevented by both the hardware and software.

Random wifi MAC-address

To prevent the collection of metadata on MAC-broadcast a random MAC address is generated on each unlock.

No Logging

We do not log any usage data on our servers or client devices. Servers are used only for communication and authorizing users. Only the attempts to attack our infrastructure are logged.

Servers based on OpenBSD/FreeBSD

All servers run on the genuine Unix. Timely updates, well configured firewall, minimum set of software run by experienced security-minded professionals.

Firewall

Each phone has a statically configured firewall. The rules allow access only to our servers. All input and output ports are closed, all connection types except "new" and "established" are blocked. Our daemon does not allow anyone to change the firewall rules.

App armour based on selinux

Limited set of applications. Only required software is installed (minimal Gentoo style).

The access rights of these programs to the system and memory is rigidly controlled.

Encrypted local data

The key for stored data encryption is not contained in the hardware keystore. Each time

the phone is switched on, the user must enter the key. While the device is active, the key

is only in RAM store. Data encryption - AES-256. In ordinary phones, the key

for encryption is generated when it is first turned on and stored in a special section of the read-only

memory. If you change the password, only the master key is re-encrypted. In our case, when changing the password, the data is re-encrypted with the new keys.

Panic PIN

Panic PIN to unlock the screen in case you are forced to enter the PIN-code. Erases all

user data from the device.

HD voice codecs

High quality voice codec.

Minimalist interface

The interface is minimalistic yet complete, with a set of applications for the most used functions.

Scratch card for activation

Scratch card to activate and recover a device.

Scratch card is generated on the computer with an air gap. The scratch layer is applied using the PCI DSS standard. Scratch cards have no serial number. Subscriber's number is assigned after activation. Thus, no one except the person erasing the layer knows the number placed on the scratchcard and which number is assigned by the server.

Switzerland based servers

All servers are located in Switzerland and protected by extremely strong privacy laws. A good team of Swiss lawyers awaits any challenges. Regardless, our servers do not and cannot store any correspondence or customer info.