SecureScrypt
COMMUNICATION ENCRYPTION
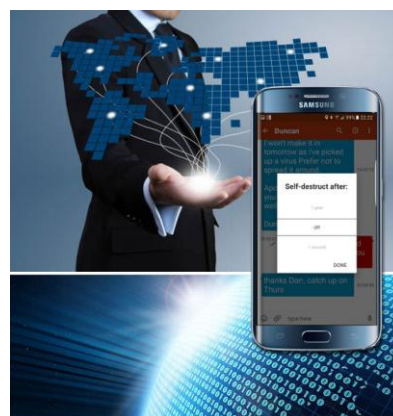### SECURITY ENCRYPTION SOFTWARE

Mobile phones, tablets & computers – each of these devices use global telecommunication networks to connect you to your friends and contacts. The vulnerability of these networks to outside interception and malicious hacking puts the privacy and confidentiality of your personal communications at risk.

To protect against such intrusions, SecureScrypt encryption software creates an encrypted private network between you and your contact(s).

Because the encryption & decryption of your communication exchange happens on your individual devices (End-to-End), you have total control over the security of this exchange. This guarantees that no third party can decrypt any part of your communication, documents, pictures, video conference, messages preventing any "Man in the Middle" attacks.

- Voice calls
- Text chat messaging
- Location Share
- Voice Messages
- Data file transfers including documents, pictures and videos
- includes a communications specific
- Self-Destruct Feature with predetermined time frame, a SecureScrypt digital locker
- Scalability of use within governments, enterprise and private networks, even militaries and services
- Quick and easy download across a variety of devices
- The ability to be installed, updated or deleted remotely on any supported device with access to the internet, including pre-paid devices or devices with no SIM cards

SecureScrypt is the world's most effective and comprehensive communication encryption security solution available

Through strategic partnerships and select high-profile service providers, The SecureScrypt Full Enterprise Solution delivers the kind of digital security experience government, enterprise and private consumers are looking for.

The SecureScrypt Full Enterprise Solution enables large scale organizations to communicate safely, knowing that the privacy and integrity of their conversations and proprietary information will not be eavesdropped nor stolen.

The SecureScrypt team can effectively cost to personalize the Full Enterprise security encryption solution for:

- Existing Server(s)
- Or own Servers
- Telco's
- Large Volume Business Solutions
- Authentication/Payment Processes
- Banks
- Governments
- Official Services
- And ….

SecureScrypt ENSURES YOUR BUSINESS STAYS YOUR BUSINESS

In today's world, consumers expect convenience and flexibility — but not at the expense of the privacy, confidentiality and integrity of their personal and intellectual property. This is especially true when it comes to private communications and the digital transfer of sensitive material across the internet.

SecureScrypt provides a complete real time security solution by encrypting - scrambling – digital communications.

It does this by applying a military grade encryption to all voice calls, text chat and digital data transfers on devices such as Android & iPhone's, and PC & Mac based computers and devices.

Developed specifically for the safe and secure communication of voice, text-chat and digital data, SecureScrypt is a sophisticated software encryption application which works by creating an "encrypted private network" between the sender and the recipient of a communication.

SecureScrypt does this by:

Generating a unique 'key' specific to the user's communication device. No other copies of that key exist on any other device or server.

- This unique encryption key is then encrypted again at the server level, providing a double layer of encryption.
- SecureScrypt encrypts using state of the art elliptic curve cryptography to protect the communication between two parties, as well as between the application and its servers.
- Each phone or connected device has its own contact book of 'trusted member contact numbers' relevant to that device's particular key. There is no need for a central server or certificating authority.
- When making or receiving a digital communication, the SecureScrypt encryption engine authenticates the other party and generates the unique session key that only lasts for the duration of that communication.
- In real time, voice calls, text-chat and data communications are then encrypted to prevent hackers from gathering information on the contact details and identities of the participants in the communication.
- Point to point security is thus established because only trusted devices at each end of the secure communication network are able to decrypt the exchanged data. Only the recipient's device is able to decrypt a voice, text-chat or data communication after it has been sent and received.
- Because SecureScrypt servers do not hold any encryption or decryption keys, and because SecureScrypt secure voice, chat and data communications are peer to peer, there is no potential for the 'man in the middle' threat that exists with other forms of network channel communications.
- A self-destruct feature can be applied to automatically delete by shredding and overwriting all metadata content from both the recipient's and the sender's devices after a predetermined period – from as little as 1 second up to 1 year after the original communication.

Because SecureScrypt servers are always owned and operated by the legal owners of the encryption Software, on their premises the original encryption keys used in a SecureScrypt communication exchange, make it impossible for SecureScrypt to enable any lawful or unlawful interception of information or interfere with the legal owners communication.

SecureScrypt
MINIMISING YOUR DIGITAL FOOTPRINT

While connected devices such as unsecured smart phones, tablets and computers offer convenience, they are vulnerable to compromise.

Voice transmissions, text-chat and data transfers are easier to intercept than ever before. Unprotected domains within the telecommunication networks and public locations such as open Wi-Fi areas or public hot spots, offer hackers and criminals the opportunity to illegally acquire private information with which to commit fraud, identity theft, and to exploit for malicious intent and self-gain.

The SecureScrypt Secure Communications Apps have been designed specifically to protect users from such intrusions into their private communications, and are available now from the App stores.

By creating an "encrypted private network" between the sender and recipient of a digital exchange, these SecureScrypt Secure Communications Apps provides an integrated solution for secure, encrypted voice, text-chat and data transfer within a telecommunication network.

The SecureScrypt Secure Communications features:

- Real time HD quality encrypted voice calls
- Encrypted text chat messaging
- Real time encrypted data transfer
- A self-destruct feature with pre-determined time frames
- Easy to use software with intuitive user interface
- An industry standard downloadable App that can be deployed within minutes from anywhere in the world
- Standard device management software
- The App can be installed, updated or deleted remotely on any supported device with access to the internet, including pre-paid devices or devices with no SIM cards.

SecureScrypt
COMMUNICATION ENCRYPTION
SECURITY SOLUTION

SecureScrypt 2017 the new solution   info@securescrypt.com