DataProtect

HESP

The secure, customer-controlled smartphone with stealthy military-grade encryption

March 2018

DataProtect

Why HESP?

All existing secure solutions have at least one of the following drawbacks:

1. Secure calls that are initiated and/or go through 3rd party servers (solution provider, Apple, Google, Facebook) which can act as a single point of attack, allowing for the theft of hundreds of millions of users' information in one attempt.

2. Crypto phones draw unnecessary attention and can be even confiscated in certain situations like when crossing borders. Besides that, low profile methods can also be applied as soon as the user reveals that he is using a special phone.

3. Standard protocols, like SRTP and ZRTP protocols, which reveal encrypted communication to the network providers. In some countries, like UAE, those protocols are blocked by default.

4. No protection against viruses and spyware. This makes good cryptography useless since there are a number of viruses, trojans and exploits which can capture the phone audio or screen view, steal user credentials etc. It makes even good cryptography useless.

The HESP Phone closes all security gaps

1. No 3rd party services and complete control. We have even made our own push notification service in order to provide customers with complete control.

2. All server components, call establishment, key/certificate management services, also belong to the customer.

3. Protection from viruses and trojans, provided by hardened OS/firmware is installed on the HESP Phone.

4. HESP does not put secure communication at risk:
   - Calls are done via an encrypted binary protocol which looks like a VPN connection for network providers
   - It looks and registers in network as an ordinary smartphone

5. No viruses/trojans with hardened OS.

DataProtect

HESP Phone overview

- Point-to-point Encrypted Voice Calls with HD audio
- End-to-End Encryption
- Encrypted Text Messages
- Encrypted Group Chats
- Encrypted File transfer
- Encrypted Video Messages
- Support of extended security set
  - remote revocation
  - panic wipe
  - 5 times incorrect password entry wipe
- Only signed, pre-checked apps allowed
- Full verified boot, covering all firmware and OS partitions
- Safe against all major vulnerabilities, avoids exploits
- Filesystem layer encryption, covering all data and metadata

DataProtect

Military grade cryptography

Key exchange	DH 8192 or ECC B571 (over Binary Fields) / ECC P521 (over Prime Fields)
Encryption	AES 256 in the GCM mode
Hash function	SHA512
PRNG source	Several options available: Non-blocking */dev/urandom* Custom software/hardware (HSM) entropy source Mixing user input (radio signal, touch screen, audio, camera) to provide better entropy
Authentication	Built-in Public Key Infrastructure (PKI) system, certificate based authentication
Secure communication protocol	Custom binary communication protocol featuring: • New encryption key exchange per call • Backward and forward secrecy • End-to-end encryption, e.g. only the participants hold encryption keys • Mutual point-to-point authentication • Data integrity • Replay and mirroring attack protection

HESP Phone OS security specs

- Unsigned apps installation disabled
- Full verified boot, covering all firmware and OS partitions
- Forensic wipe feature
- Preventing all major vulnerabilities, avoiding exploits
- Filesystem layer encryption, covering all data and metadata
- UX focused on security: separate lock screen, encryption passwords, etc
- Backported security, regular updates (patching) to address new threats

Out of the box HESP Operating System is available for 2 models

Premium model

HTC Google Pixel

Budget model

LG Google Nexus 5x

HESP works with all available networks

Our solution works great with new age networks such as 3G, 4G, in offices (Wi-Fi), as well as with older networks (2.5G, EDGE).

Furthermore, our solution works in regions without mobile coverage (satellite link), as well as in offices with tighter security where only IP Ethernet networks are allowed.

The list of supported networks includes:

- 3G, 4G
- Wi-Fi
- 2.5G, EDGE
- Satellite (Thuraya SatSleeve, Satellite Hotspot, Landline Satellite, InCar Satellite)
- Landline Ethernet (IP Desk phones, PC, Mac)

The HESP Communication Server for corporate communication systems

The HESP Server communication system can be installed on corporate premises. It acts as a communication system backend to register/manage HESP user and initiate the communication.

Features:

- Complete control over the corporate telephone system
- No 3rd party services
- Authorized devices only, with hardware binding
- PKI infrastructure and certificate management
- Control panel for managing users and keys
- Extended PKI support
- Client and server apps protected from third party interference
- World Wide and Regional servers infrastructure supported
- Redundancy and Load Balancing
- Secure devices support: HESP Phone, HESP Deskphone
- BYOD support: iOS, Android, PC and Mac

Full synchronization with the HESP Deskphone, HESP BYOD for iOS, and Android devices

The HESP Deskphone

The HESP Deskphone enables encrypted voice, text communication and file transfer over a secure landline (Ethernet) connection. The phone features dual Gigabit ports, HD audio, integrated Wi-Fi (802.11b/g/n) for network flexibility, PoE, and a tiltable CMOS camera for encrypted video messages.

The HESP Deskphone provides:

- Point-to-point Encrypted Voice Calls with HD audio
- End-to-End Encryption
- Encrypted Text Messages
- Encrypted Group Chats
- Encrypted File transfer
- Encrypted Video Messages

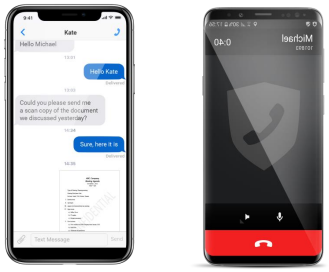
HESP BYOD (Bring-your-own-device) licenses for iOS and Android

HESP works on the iPhone 5C, 5S, SE, 6, 6+, 6S, 6S+, 7, 7+, 8+, X (OS 8.x.x and higher) or any Android device with OS 4 and higher

HESP provides a unique set of products and components

HESP provides a set of products and components that have no analogues on the global market. Customers can choose between:

- HESP Phone
- HESP Deskphone
- HESP Server
- HESP for Android and iOS (BYOD)
- HESP Desktop (currently in beta) for Win PC and Mac
- Remote flashing - producing secure phones on a distance.



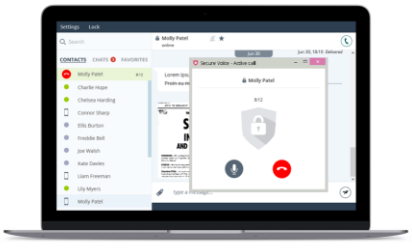
iOS, Android app

HESP

Server

Deskphone

Server (mobile)



Desktop (beta)

How to start

We offer the following steps in order to get better understanding and start using HESP:

- We can make an online presentation for HESP phone in order to provide more information about its benefits and technical details. We can also discuss your needs and while selecting the most relevant options for our HESP product
- Get Demo units of the HESP Phone and HESP Deskphone at a special demo price
- Get a quote for the HESP Server to have full synchronization, including BYOD and other benefits. Here you can get a server with DataProtect infrastructure as a starter option (to see how it works, you can move to the dedicated one later on)

Please contact us to schedule a presentation or get additional information

Tel: +46 (0)75 7000 700

Mail: info@dataprotect.se

Web: www.dataprotect.se

DataProtect Sverige AB

Södra Kyrkogatan 57B

503 43 Borås

Sweden