



PROJECT DETAILS

The Zein Group Holding Company provides government agencies such as national security agencies and foreign missions with Encrypted Headphones Series that are integrated with military-grade encryption technologies classified as “Top Secret” to combat spying on the communications of presidents, ministers, and senior local and international officials in the armed forces and various ministries that deal with confidential defense information, to ensure that highly sensitive government communications are not exposed to spying by hackers and are protected from all types of severe attacks, providing the highest level of security for local and international communications conducted over public cellular network under any circumstances, anywhere in the world, and on all types of terminal equipment.





TABLE OF CONTENT

- 01. Appearance Series
- 02. Project Introduction
- 03. Project Advantages
- 04. Digital Voice Encryption Technology
- 05. AMSI Modulation and Demodulation Technology
- 06. Analog Speech Scrambling Technology
- 07. Analog Audio Coding Technology
- 08. Technology Description
- 09. Performance Indicators
- 10. Support Phones
- 11. Instructions for Using
- 12. Partnership



PROJECT

01. APPEARANCE

SERIES



Telezein® Sec-Voice™ Earbuds

Figure 01

This theme meets the encryption of mobile communications such as smartphones.



Telezein® Sec-Voice™ Handset

Figure 02

This theme is suitable for encrypting fixed communications such as office telephone.



Telezein® Sec-Voice™ Headset

Figure 03

This theme meets the military tactical communications encryption in battle.



02. PROJECT INTRODUCTION

Encrypted Headphones Series integrates two voice coding algorithms, digital voice coding and analog voice coding. The digital voice coding algorithm adopts AMSI modulation and demodulation technology and high-level coding algorithm, the encoded voice signal has no audio or clarity characteristics, it is a military-grade voice coding scheme with "Top Secret" classification. The analog scrambling encryption algorithm not only guarantees certain voice security, but also has good applicability to the call line. The combination of the two algorithms allows users to achieve privacy protection in any high-level communication environment. The Encrypted Headphones Series can be used with terminal equipment such as phones to implement recording encryption, voice message encryption, mobile call encryption, VoIP call encryption and other functions.

It realizes sound source protection and can resist eavesdropping risks to the maximum extent, including operator eavesdropping, network eavesdropping, signal 7 wiretapping, pseudo-base station eavesdropping, spy UAV drones and other line eavesdropping, interference and brute force, electromagnetic leakage, as well as spyware on phones, backdoor and other terminal eavesdropping, without the need to build expensive and high-maintenance government private networks.

- | | | | |
|-----------|---|-----------|--|
| 01 | Support digital voice encryption and analog scrambling two military-grade voice security technologies; | 02 | Realize GSM, UMTS, CDMA, Satellite, VoLTE cellular voice encryption call; |
| 03 | Cooperate with mobile phone voice short message software (such as voice message function in Whatsapp) to realize voice message encryption; | 04 | Cooperate with mobile phone recording software and voicemail to realize voice encryption recording; |
| 05 | Cooperate with mobile phone VoIP software to realize encrypted VoIP calls; | 06 | Enables secure multiparty conferencing across radio and telephone networks; |





03. PROJECT ADVANTAGES

- 01** Simultaneously realize three privacy protections: call protection, voice message protection, and recording protection. In addition to the protection methods, the system can resist UAV drones spying on the base station of cell towers.
- 02** Support digital voice encryption and analog scrambling two voice security technologies, users can choose to use them according to security needs and actual line conditions at a “top secret” level;
- 03** The system form factor relies on headset and handset, to hide the system features inside the device, and thanks to its form factor, the call cannot be recorded by a third party such as installing an external voice recorder for the call;
- 04** The system has all the functions of a traditional Bluetooth headset and handset, switching to secret calls only when needed, without changing the daily habit of answering phone calls;
- 05** The sound source is encrypted to prevent all kinds of wiretapping means such as line monitoring, Trojan horse, back door and call recording applications;
- 06** Decentralized, end-to-end encrypted calls, independent of operators to provide special services, secure, autonomous and controllable;





CORE TECHNOLOGY

04. DIGITAL VOICE ENCRYPTION TECHNOLOGY

Digital voice encryption is based on the speech compression algorithm, data encryption algorithm, and signal demodulation technology implementation. In secret speech, the "secret speech" stored in a recording file or transmitted in a mobile cellular network channel is entirely a data modulated signal, without any human voice characteristics, and its security depends entirely on the strength of the cryptographic algorithm and the randomness of the key. The workflow of digital voice encryption technology is shown as follows:



01

The encrypted speech transmitter receives the user's plain speech, performs analog-to-digital conversion, and compresses the plain speech through the vocoder;

03

The encrypted speech is compressed and encoded cipher text for signal modulation to generate audio modulation signals, making it top secret;

05

The receiver demodulated the audio modulation signal, and decrypted the demodulated data using the standard cryptographic algorithm;

02

Standard encryption algorithm is used to encrypt audio data after compression and encoding, protecting it from all forms of brute force spying;

04

Audio modulation signal is stored by recording software or transmitted over mobile cellular network, encrypting the signal from any trace;

06

It restore the decrypted data and perform digital-to-analog conversion through vocoder algorithm, and finally play the restored voice;



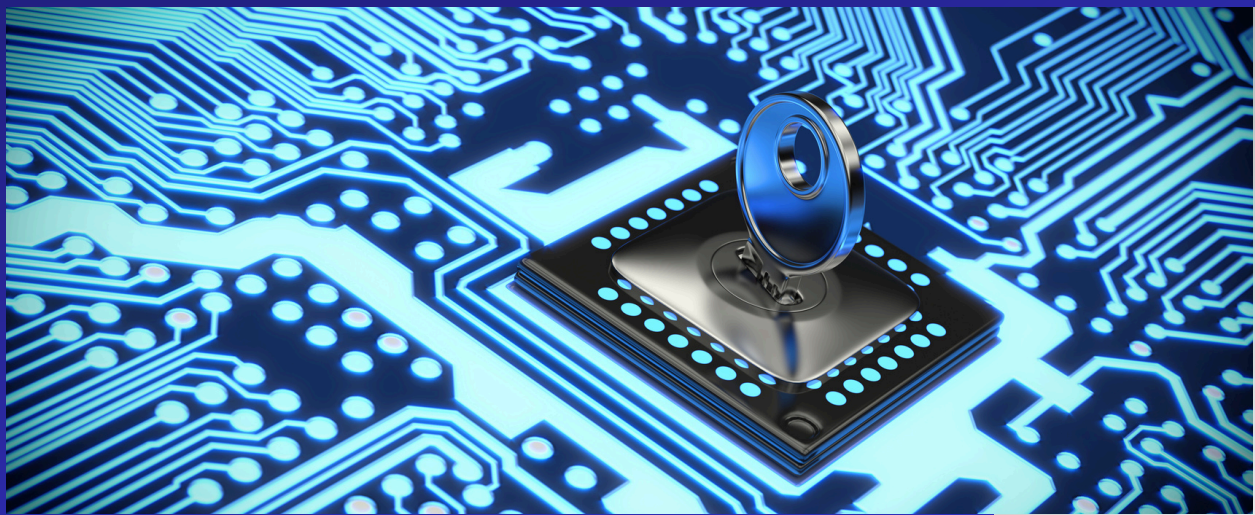
05. AMSI MODULATION AND DEMODULATION TECHNOLOGY

In order to carry out end-to-end encrypted digital voice communication over cellular voice lines, it is necessary to realize highly reliable data communication with a minimum transmission rate of 2kbps to 3kbps over standard voice channels. At present, whether in cellular mobile network or fixed telephone network, due to the existence of vocoder algorithm, the traditional PSK, QAM, OFDM modulation technology and recently emerging voice-like modulation, wavelet modulation, cosine modulation and other schemes can not achieve more than 1.5kbps and practical reliability of data transmission. It does not have the data communication capability to realize digital voice encryption communication.

AMSI modulation and demodulation technology is an advanced digital signal modulation and demodulation technology, its working principle is similar to the traditional telephone Modem. At the sending end, the data through AMSI modulation is converted into analog modulation tone, like ordinary voice signal through the telephone, mobile phone, VoIP voice channel transmission; At the receiving end, the analog modulation tone is demodulated by AMSI and restored to a data stream. The difference between AMSI and the traditional telephone Modem is that the audio signal modulated by AMSI can still be accurately demodulated after being compressed and restored by the medium and low rate voice vocoder, that is, AMSI has enough penetration of the medium and low rate voice vocoder, thus providing a reliable basic data channel for military-level digital audio coding through standard voice channels such as phones.

AMSI technology currently penetrable voice coding channels: GSM EFR、UMTS AMR WB、UMTS AMR NB、AMR NB12.2、AMR WB24.4、SILK、OPUS、G.711... ;

Basic performance of AMSI technology: It can provide 2Kbps to 4Kbps basic communication bandwidth, and the bit error rate is less than 0.2%.





06. ANALOG SPEECH SCRAMBLING TECHNOLOGY

The conventional analog speech scrambling technology is usually to process the time domain signal of human voice, and then scramble the signal sequence in the transform domain, and then execute the reverse transformation, and finally produce scrambled speech. The disadvantage of this approach is that the scrambled speech usually no longer has human voice characteristics, such as pitch, resonance frequency, etc., so that when the scrambled speech passes through the conventional voice channel (such as micro reliance voice call), it will be determined as noise by the voice communication system and be reduced or even completely eliminated, resulting in the receiver can not restore the voice.

The analog scrambling algorithm integrates the speech construction technology, and uses the typical human voice model to process the scrambled signal, ensuring that the scrambled signal can deal with most noise reduction algorithms, and even in the call channel with AI noise reduction.

ECDH protocol allows two parties to communicate securely by creating a shared public and private secret key pair over insecure communication channels. The advanced technology allows this shared secret to be used directly to encrypt communications using symmetric key encryption, and with the self-destruction technology of voice data, it becomes impossible to eavesdrop on calls in Encrypted Headphones Series in any way or even obtain the basic data.





07. ANALOG AUDIO CODING TECHNOLOGY

01 Analog Voice Encryption

The analog voice encryption technology of the Encrypted Headphones Series can support various brands and models of mobile phones, 2G/3G/VoLTE cellular voice network, and real-time voice call function of various mainstream social software such as Skype, WhatsApp.

02 Recording Encryption

The system supports voicemail recording on all types of phones. For the voice recording software at present, the built-in voice memo software of iOS can support Bluetooth pickup, so the iPhone supports the Encrypted Headphones Series (voice message private mode) for encrypted recording. Huawei, Motorola, Samsung, Cisco, and other phones, because the system's native recording software does not support Bluetooth pickup function, it is not possible to use for encrypted recording.

03 System Restrictions

1. When using the recording encryption and voice message encryption functions of the Encrypted Headphones Series, the corresponding application software must support Bluetooth device pickup and playback;
2. When Encrypted Headphones Series communicates with phone through Bluetooth function, due to external signal interference (especially 2.4G WiFi), it may cause loss or deformation of secret voice audio signal, resulting in tone change, tone loss, noise addition and other phenomena of secret voice;
3. When making a cellular voice call through a Encrypted Headphones Series, the signal quality of the cellular network has a great impact on the sound quality of the secret voice, and the poor signal quality of the cellular network will lead to the increase of AMSI data communication errors, which will deteriorate the quality of the secret voice;
4. The digital voice encryption function of the Encrypted Headphones Series cannot support all VoIP applications to achieve encrypted calls, mainly because some VoIP voice will be denoised as noise, resulting in the distortion of the secret voice signal and cannot be decoded.





08. TECHNOLOGY DESCRIPTION

01 Cellular Voice Coding Standards

The Encrypted Headphones Series supports cellular voice coding systems including: VoLTE, GSM EFR, Satellite.

02 Support Voip Encryption Function

The noise cancellation algorithm of most VoIP software will eliminate the encrypted modulation audio signal of the Encrypted Headphones Series as noise, resulting in a surge of error codes of the secret signal, which makes the encrypted call effect worse, or even impossible to call. At present, VoIP applications that can support digital voice encrypted calls include, FaceTime and WhatsApp, For other VoIP applications, customers need to test themselves.


03 Support Encryption Voice Messages

The system supports Voip applications, the iOS system supports most voice messaging applications and the Bluetooth pickup function. The encrypted voice messaging function of the Encrypted Headphones Series can be used. For Android system, except Skype, other voice message applications do not support Bluetooth pickup function, so Skype can only support Telephone Set Series series encrypted voice message function under Android system.





09. PERFORMANCE INDICATORS

 Tactical Headset Version	Bluetooth Protocol	5.2
	Call noise reduction	Dual microphone noise reduction
	Secret speech mode	Digital secret speech Analog cipher Voice message encryption
	Digital secret speech function	Key negotiation algorithm for real-time voice calls: ECDH Voice recording and message key: Preset shared key Voice encoding encryption and decryption algorithm: AES256 Setup time of secret words: ≤5s
	Analog scrambling function	Preset scrambling algorithm and scrambling sequence
	Plain secret change mode	One key switch
	Secret call time	2 hours
PTT; Self-organizing network capability		
Dedicated digital encryption (AES256)		
Function of calling and group calling		
IPX-4 Waterproof		



10. SUPPORT PHONES



			Brands	Models
			iPhone	All Series
			Motorola	All Series
			Samsung	S series ,Note series
			Huawei	Mate series,P series
			Cisco	8800 Series & others
Voice Message App	iOS	Android		
Skype	Support	Support		
Line	Support	-		
WhatsApp	Support	-		
Telegram	Support	-		

The system supports phones and other applications.

Most phones are powered by Snapdragon 8 series chips or Kirin 9 series chipsets.



11. INSTRUCTIONS FOR USING

01 Pairing

Long press the battery compartment button, the headset enters the pairing state, and use the mobile phone to search for the headset for pairing.

The analog phone handset can be paired via Bluetooth or by connecting it directly to the handset wire.

02 Switching The Device Security Mode

The Encrypted Headphones Series has three security modes: digital voice encryption, analog voice encryption, and voice message encryption. The default mode is digital voice encryption. Users can quickly double-click the function key to switch the safe mode.

03 Call Encryption

In the digital voice encryption mode, a user can switch to the open secret call state by clicking the function key during a call. In the analog voice encryption mode, both sides of the call need to click the function key at the same time to switch the state of plain and secret speech.

04 Encryption Recording & Voice Message

In voice message encryption mode, you can use the recording, voicemail, or voice message software that supports Bluetooth pickup/playback to perform encrypted recording/decryption and playback, as well as encrypted voice message sending/listening.

Note: In voice message encryption mode, users cannot make regular voice calls.

05 Updating user keys

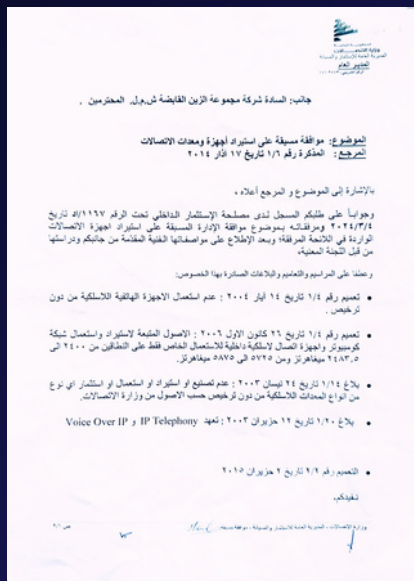
In voice message encryption mode, users can enter the shared key by entering a specific command string through the phone dial keyboard.





CONTACT US

12. PARTNETSHIP



- The project has undergone technical inspection and testing by the Lebanese Ministry of Telecommunications and has been classified as top secret.
- Approved by the Lebanese Ministry of National Defense - Signals Intelligence Regiment.
- This project is protected by intellectual property law.
- The Zein Group Holding Company S.A.L. warns against publishing or distributing this file or using the trademark without a written authorization from the publishing or distributing party, duly signed, under penalty of legal prosecution.
- This file contains general information about the company's project. The company disclaims any responsibility for any misuse of this file.
- The company warns against violating the project's intellectual property rights under penalty of legal prosecution.



Address :



Phone :

Lebanon, Beirut Central District Solidere, Allenby Street, Building No 1479, 2nd Floor.

+961 1 957 610