Quantum Shieldz® Cipher™

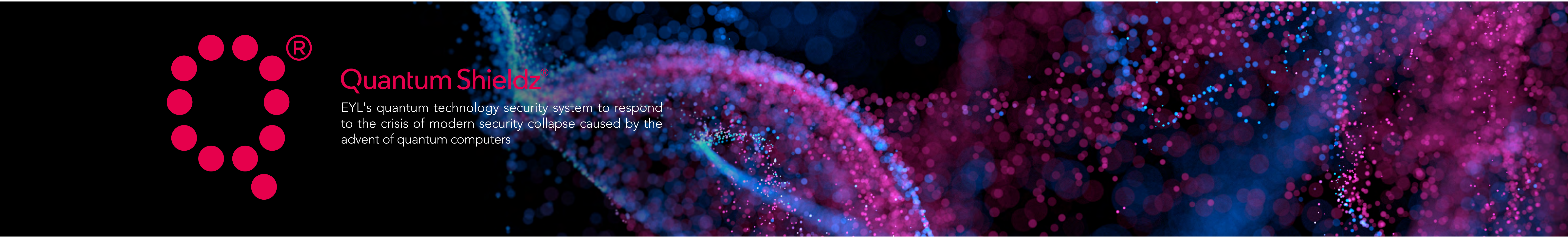
Anti-Eavesdropping Solution

Powered by Quantum Shieldz

Quantum Entropy :
The ultimate randomness nature has to offer

Meet with Quantum Shieldz®

The Quantum Random Number Generator (QRNG) and application product family from EYL is designed to directly address the convergence security demands introduced by the 4th Industrial Revolution and the new generation of connected IoT devices and systems.



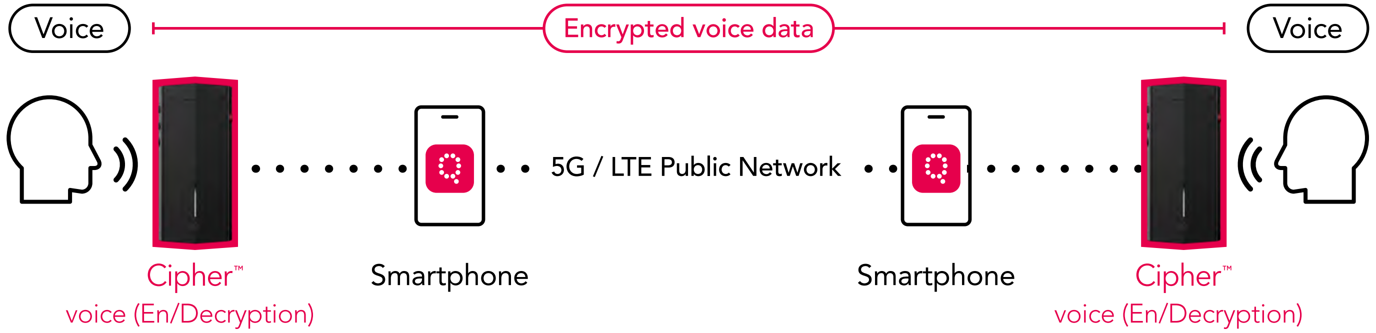
Quantum Shieldz®

EYL's quantum technology security system to respond to the crisis of modern security collapse caused by the advent of quantum computers

Secret communication solution with your own smartphone

Quantum Shieldz® Cipher™ is a self-sufficient voice encryption device that works with your personal smartphone. It uses an encryption key generated by a quantum random number generator (QRNG) to securely encrypt the user's voice, completely blocking eavesdropping or unwanted recording through spyware. Quantum Shieldz® Cipher™ is an accessible yet highly secure communication device that allows users to use their own smartphone.

Voice Encryption and Decryption using Quantum Shieldz® Cipher™



Is your phone safe?

Recently, a bank app, with a stealthy tapping function, impersonating a financial company was installed on 40,000 smartphones.

As such, tapping is prevalent not only in the national defense field, information combat amongst countries, competition between companies, and political activities, but also for the general public.

In fact, many phone-tapping apps are being sold and spread widely, and if such an app is installed without your knowledge, your conversations via phone will be transmitted live or recorded to be dispersed anywhere.

Your phone is no longer secure.

Secure dialog with Quantum Shieldz® Cipher™

Quantum Shieldz® Cipher™ converts the user's voice into strongly secured encrypted data and transmits it to the smartphone, thus, even if one hacks the smartphone to attempt to eavesdrop, it will be impossible to recognize the encrypted data.

Smartphones would have to serve only to connect to public networks such as 5G or LTE as no information would be stored.

When the receiver uses Quantum Shieldz® Cipher™, the transmitted encrypted data will be decrypted into an audio signal, enabling a call.

Can you trust smartphone manufacturers, operating systems, and apps?

"CIA Hacks Apple, Google and Samsung Operating Systems, Utilized as a wiretapping and interception platform"

Most smartphones we use run on operating systems such as Android or iOS. As the range of things that can be done through smartphones expands, users download dozens, perhaps hundreds, of various apps.
However, not many are conscious of whether these apps are free from tapping.
Is the app you are currently using safe from eavesdropping? Would Google and Apple, which provide the operating systems, not have created backdoors? Can you really trust the smartphone manufacturers like Samsung, Apple, Huawei, etc.?

Cryptophones in the Status Quo

From the 1970s, when the NSA developed a 'secure telephone unit', many encryption devices have been developed to allow private officials to have secret conversations.
In general, the use of cryptophones have been limited to such government and private officials.Not available to the general public.
However, the extensive use of smartphones by individuals have created an explosion of new risks for snooping. For example, in 2011, news broke out that news Corporations sought to hack and tap the phones of the 9/11 victims in order to investigate details of their lives leading up to the atrocity. To this end, one police source stated, more than 4,000 victims had their phone hacked.
As such, nowadays, ordinary individuals are at great risk of hacking and tapping. Recently, many efforts have been made to prevent such issues, yet Cryptophones with a price greater than $3,000 puts the device beyond the reach of most ordinary individuals.

Quantum Shieldz® Cipher™ is a voice encryption device available to anyone

This is why we released Quantum Shieldz® Cipher™.
Any possible danger from spyware or tampering is eliminated when using Quantum Shieldz® Cipher™ as it is a device functioning solely with firmware, completely independent from operating systems.
Since the information transmitted through the smartphone is encrypted, even if the security of the smartphone itself is not guaranteed, eavesdropping on the content of the message is essentially impossible.
Now, with Quantum Shieldz® Cipher™, individuals concerned about eavesdropping can use cryptophones.
Not only is its small size easy to carry, you will also enjoy its convenient features by using your own, latest smartphone as it is while alleviating any concerns of tapping.

Users

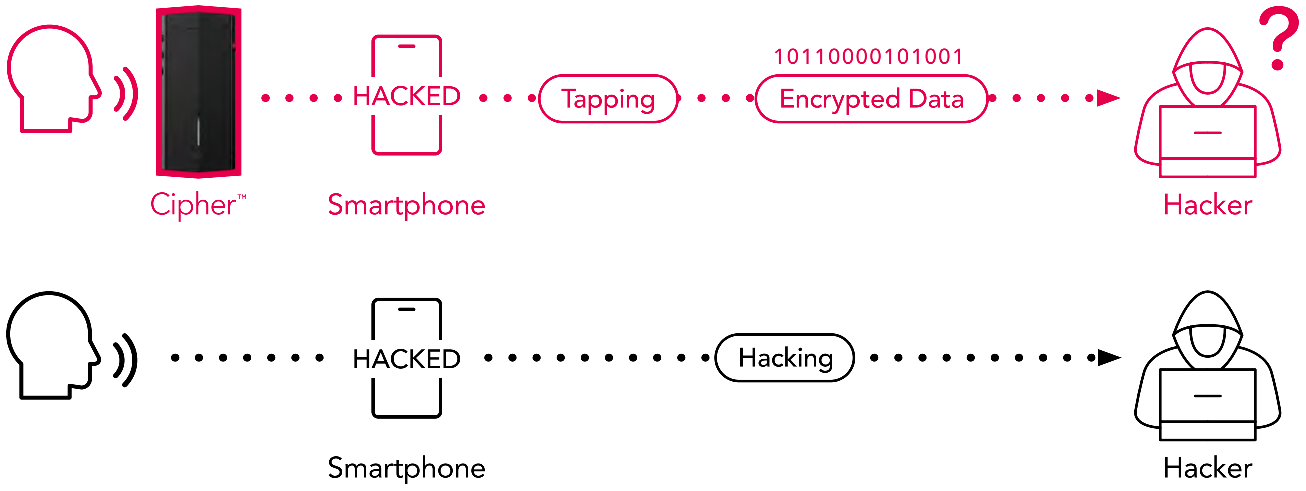
- ✓ Lawyers, clients, and law firms in cases where litigation is in progress
- ✓ State administrative agencies where major policies are discussed and decided; judicial institutions such as prosecutors and police with investigative powers
- ✓ Businessmen such as CEOs and key executives, development and sales planning departments who are exposed to industrial espionage
- ✓ Politicians, diplomats and lobbyists dealing with confidential information
- ✓ Election campaigns such as presidential elections, general elections, local government elections, union elections, etc. in which there is an opponent's election campaign, and the election management committee
- ✓ Members of the Parliament and local councils engaged in legislative activities
- ✓ Institutions that carry out various audits and crackdowns
- ✓ Smartphone users who are concerned about eavesdropping for other personal reasons

Quantum Shieldz® Cipher™ secures your life

Smartphones are easily hacked : they are easily affected by hacking programs or malicious codes as they connect to the internet through an overt system.
Since Quantum Shieldz® Cipher™ encrypts the user's voice when transmitting to the smartphone, despite many hacking and eavesdropping attempts on the phone, the encrypted data will not be decoded. This is because the encryption key for decryption exists only in the Quantum Shieldz® Cipher™ itself.

Can hackers crack the encryption key?

Encryption keys created by random number generators should be unpredictable.
However, since cryptographic devices we generally have used a programmed Pseudo Random Number generator, which contains a certain mathematical algorithm, hackers can crack the encryption key once they discern it.
Conversely, Quantum Shieldz® Cipher™ is equipped with a Quantum random number generation chip to generate its encryption key.
The Quantum Random Number Generator (QRNG) is the topmost secure technology existing today commonly used for extensive quantum encryption communication as it extracts the encryption key from the quantum phenomenon, which is not accessible nor predictable by humans.
To predict and decipher an encryption key generated by the QRNG is not only impossible at present but also in the future.



Encryption

With Quantum Shieldz® Cipher™, eavesdropping is not a possibility

Quantum Shieldz® Cipher™ is designed to take into consideration every vulnerability that may occur in phone calls via smartphones and mVoIP (services using voice calls over wireless Internet networks).
Also, Quantum Shieldz is powered by The Korea Cryptographic Module Validation Program (KCMVP) encryption module, a government certified encryption module.

User and device authentication

In order to prevent unauthorized users from accessing the service, every time the user tries to call by using the device, the user will have to authenticate him or herself with the device.
Quantum Shieldz® Cipher™ blocks user disguise by verifying whether the user and the device being used are authorized by the separate authentication server.

Encryption of critical information

All user and device information, and call logs are encrypted and stored to prevent external attackers from discovering or guessing the contents of sensitive information.
At this time, the required encryption key is stored separately only in the Quantum Shieldz® Cipher™.

Prevent credential attack

Quantum Shieldz® Cipher™ has a mechanism to prevent reuse of user's credential. Only the Quantum Shieldz® terminal stores authentication information, and it cannot be stolen over the network. For this purpose, quantum random numbers are applied.

Block Recording API

When a smartphone is infected with ma lware, calls made can be recorded and transmitted to the attacker. However, in the case of using Quantum Shieldz® Cipher™, not only is the recording API function blocked, but both the microphone and speaker functions are also stopped, thus making it safe from such threats.

Equipped with KCMVP-verified cryptographic module

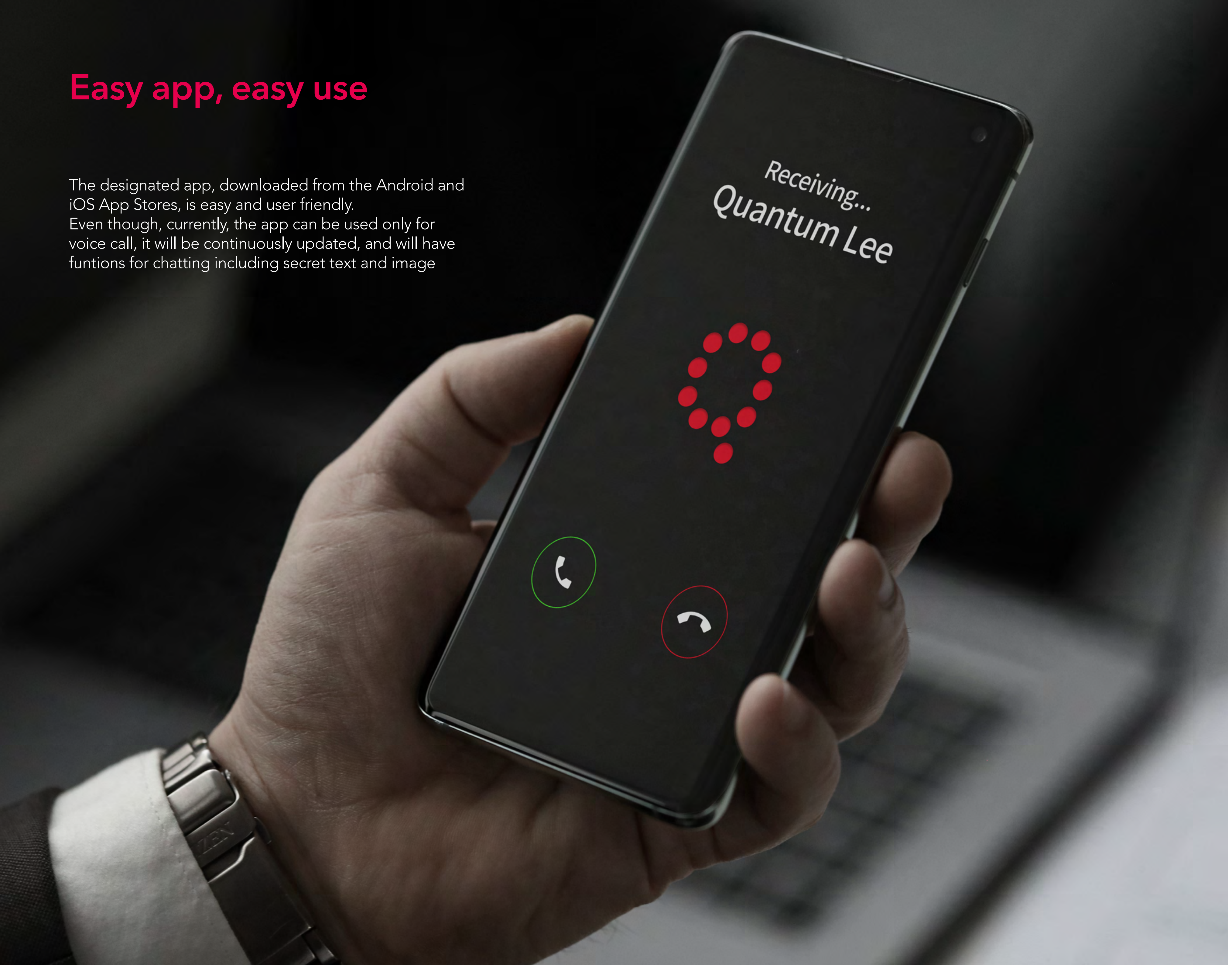
All cryptographic functions of the security protocol are provided by verified cryptographic modules of the Korea Cryptogrphic Module Validation Program (KCMVP).generated for one-time use and stored within Quantum Shieldz® Cipher™.

Voice encryption

All voice calls are encrypted.
The Secure Real-time Transport Protocol (SRTP) is appliedfor the encryption of call contents; the TLS protocol is implemented to prevent encryption key interception; the Diffie-Hellman method is used to exchange encryption keys between the Alice and Bob; and the AES and LEA encryption algorithms, which has been certified by the National Intelligence Service, has been deployed.
Furthermore, key exposure is not a problem since the encryption key is generated for one-time use and stored within Quantum Shieldz® Cipher™.

Easy app, easy use

The designated app, downloaded from the Android and iOS App Stores, is easy and user friendly.
Even though, currently, the app can be used only for voice call, it will be continuously updated, and will have funtions for chatting including secret text and image

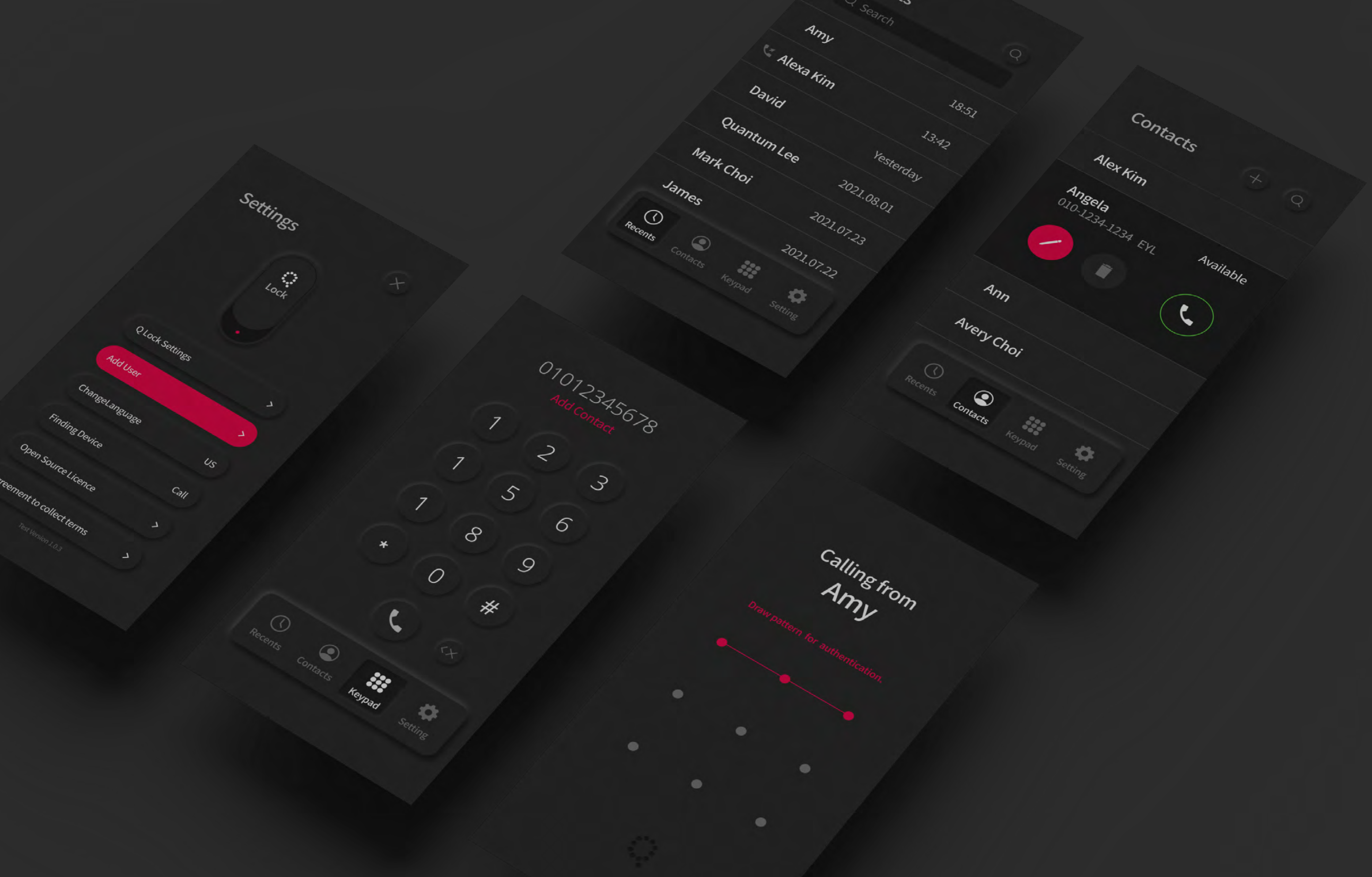


Making and receiving calls

When the Quantum Shieldz® Cipher™ terminal is powered on, it automatically connects to the already registered smartphone via Bluetooth. If the connection is not established, making or receiving calls, nor displaying connection status on the app is not available. You will have to request a call after confirming the receiver's availability status.

Authentication and registration using QR Code

In the app [Settings], register your new terminal and user credential through the QR Code provided in the product box.
This process verifies whether the device is cloned and whether the user is authorized.
The Quantum Shieldz® Cipher™ terminal and the user's phone are connected head-to-head, but when needed, changing connection to another smartphone is available.



Phonebook and recent call list

You can register the receiver's phone number for secret communication and check whether his or her device is available, also, you can make requests to the receiver's Quantum Shieldz® Cipher™ terminal for him or her to be available for secret communication. You can view your recent call history and easily make call backs.

Additional device and user authentication

When making or receiving a call, you have to successfully authenticate yourself and the device through pattern locks operated by quantum random numbers

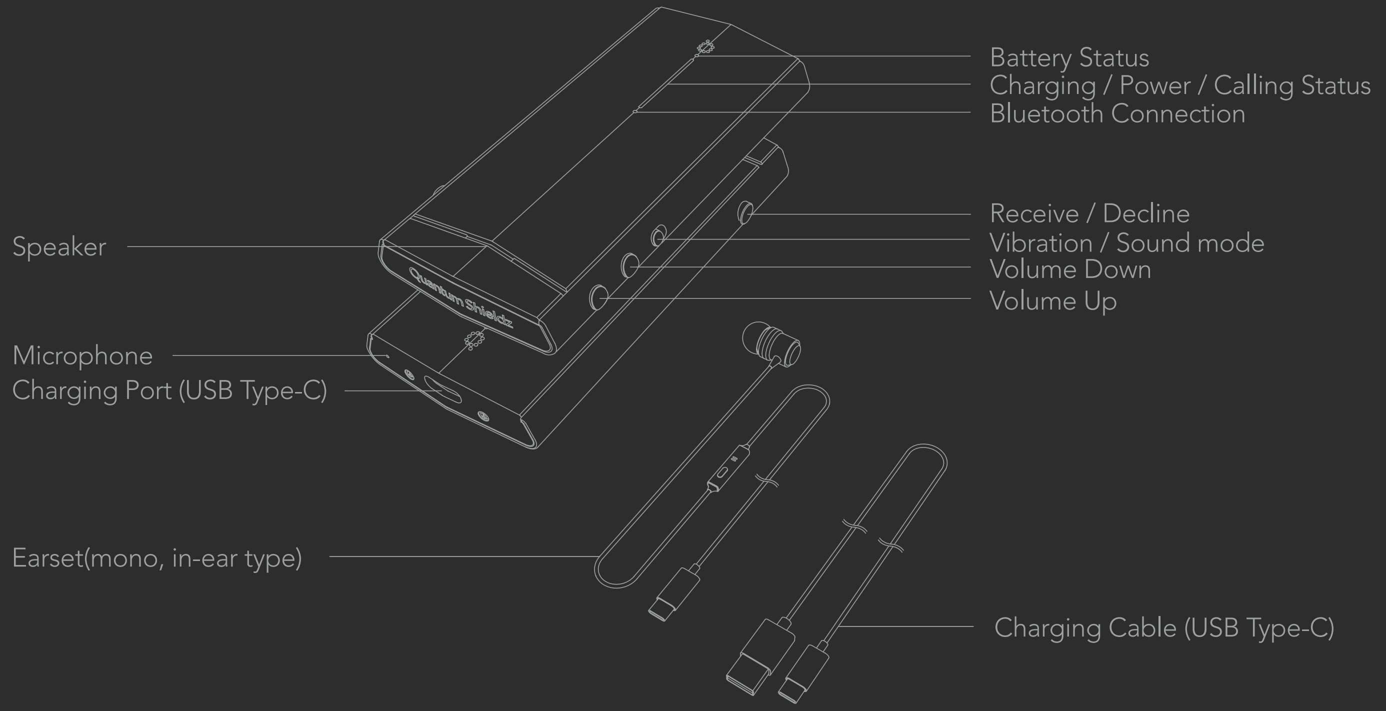
Setting

You can set up terminal registration, additional user authentications, languages, and various environment settings.

Groundbreaking design, function and class altogether.

With Quantum Shieldz® Cipher™, we don’t need to carry more than one smartphone for secret communication.
It is small enough to fit in one hand or to carry in your shirt pocket.
It has been developed considering both robustness and functionality along with a luxurious design.
Charging, sending and receiving calls, Bluetooth connection, battery level can be checked through LED lights, and it also supports volume control and vibration/sound mode conversion.

Size : 44 x 95 x 11(mm)
Weight : 70g
Connection : Bluetooth
Battery : 1,000mA
Full Charge: 2 hours
Call waiting: 36 hours
Continuous call: 4 hours


Battery Status
Charging / Power / Calling Status
Bluetooth Connection
Speaker
Receive / Decline
Vibration / Sound mode
Volume Down
Volume Up
Microphone
Charging Port (USB Type-C)
Earset(mono, in-ear type)
Charging Cable (USB Type-C)

Secure your company's secret

Quantum Shieldz® Cipher™ is not only available to the general public through subscriptions, but businesses and groups can also utilize this device. For example, if you apply for a service exclusive to executives of a specific enterprise, those with a Quantum Shieldz® Cipher™ terminal, may make calls through the service.

Also, in this case, outsiders are strictly forbidden to join the call. When performing special/specific tasks within the company, Quantum Shieldz® Cipher™ terminals may be used on a case-by-case basis.

In the case of law firms, the terminal can be used between the lawyer and client in progress, then, after the case is finished, once the preceding client withdraws, another client may use the terminal again.

Furthermore, in case a terminal part of a group service is lost or suspected of illegal use, convenient coping methods are provided. For example, the Quantum Shieldz administrator of the company can easily prevent the lost device from being exploited.

Product Inquiry

EYL, Inc.: (06776) 4F, 7-40, Mabang-ro 6gil, Seocho-gu, Seoul, Korea
Tel: +82-2-6933-7190, e-mail: contact@eylpartners.com

EVERYWHERE IN YOUR LIFE