



D-Zone 手機安全 APP 用戶操作手冊 V2.0

更新日期：2026 年 5 月 26 日

目錄

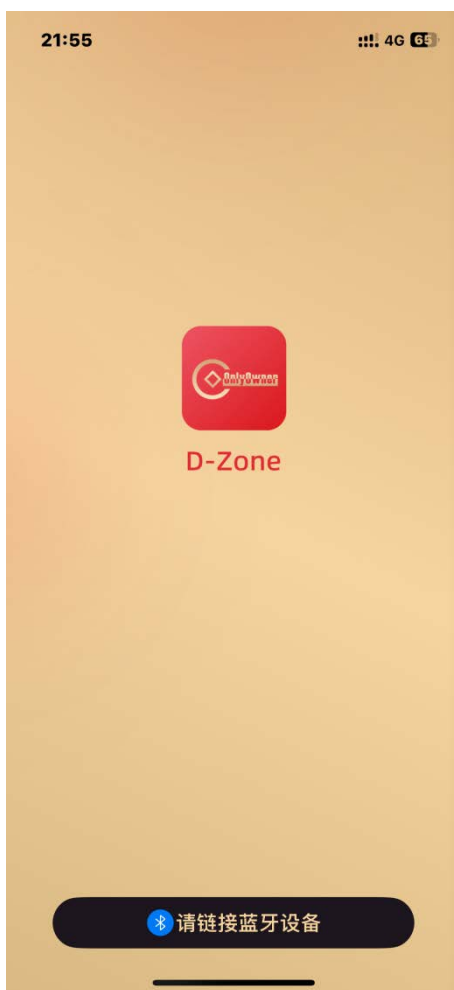
1 關於 D-Zone	錯誤!未定义书签。
2 安裝與登錄	錯誤!未定义书签。
2.1 安裝說明	錯誤!未定义书签。
2.2 登錄與藍牙設備綁定	錯誤!未定义书签。
3 底部導航與版塊佈局	錯誤!未定义书签。
1. 【檔】：本機檔案、安全區、雲空間	錯誤!未定义书签。
2. 【雲交互】：加密聊天、好友、群組	錯誤!未定义书签。
3. 【基本設定】：通訊錄、個人記事本、系統設置	錯誤!未定义书签。
4 【檔案】板塊——加密存儲	錯誤!未定义书签。
4.1 本機檔案	錯誤!未定义书签。
4.2 安全區（核心加密區）	錯誤!未定义书签。
4.3 雲空間——加密雲端備份	錯誤!未定义书签。
4.3.1 登錄與使用規則	錯誤!未定义书签。
4.3.2 核心功能	錯誤!未定义书签。
5 【雲交互】板塊——加密通訊	錯誤!未定义书签。
5.1 好友與群組管理	錯誤!未定义书签。
5.2 聊天功能	錯誤!未定义书签。
6 【通訊錄】功能	錯誤!未定义书签。
7 【基本設定】板塊	錯誤!未定义书签。
8 加密、解密、分享與雲備份	錯誤!未定义书签。
8.1 加密操作	錯誤!未定义书签。
8.2 解密操作	錯誤!未定义书签。
8.3 檔分享	錯誤!未定义书签。
8.4 雲備份與還原	錯誤!未定义书签。
9 雲空間收費規則與權益說明	錯誤!未定义书签。
9.1 雲空間	錯誤!未定义书签。
9.2 雲交互	錯誤!未定义书签。
10 注意事項	錯誤!未定义书签。
11 常見問題提示	錯誤!未定义书签。

1 關於 D-Zone

D-Zone 是一款去中心化的手機端數據加密機安全通訊應用，免註冊認證，必須配合專屬藍牙硬體 D-Key 使用，以 D-key ID 為唯一身份標識，所有數據採用硬體加密策略，本地與雲端均不明文存儲，最大限度保障用戶隱私安全，其主要提供如下三位一體安全能力：

- 安全區：本地隱私檔加密存儲與分享
- 雲空間：安全區檔加密雲端備份/還原
- 雲交互：硬體級加密文字/檔/語音消息聊天

重要：D-Key 設備出廠配套包含兩個硬體，一個為主設備，一個為輔設備。主輔設備共用相同的加密空間，用於解決單一設備丟失後手機內已存儲的加密檔無法恢復的問題。兩者的主要區別如下：主設備登錄後支持 D-Zone 軟體的所有功能；輔設備登錄後僅具備解密查看功能與通訊錄查看功能，例如解密查看所有已加密及接收的加密分享檔、雲交互/雲空間加密檔。



2 安裝與登錄

2.1 安裝說明

- 支持系統：支持 Android & iOS，本 APP 支持國內（iOS、應用寶、華為應用市場）及國外（iOS、Google Play）主流應用市場下載，華為手機支持鴻蒙系統（非純血鴻蒙）。
- APK 安裝方式：APK 下載安裝

下載更新地址：<https://onlyownerhk.com/ft-code-21.html>

2.2 登錄與藍牙設備綁定

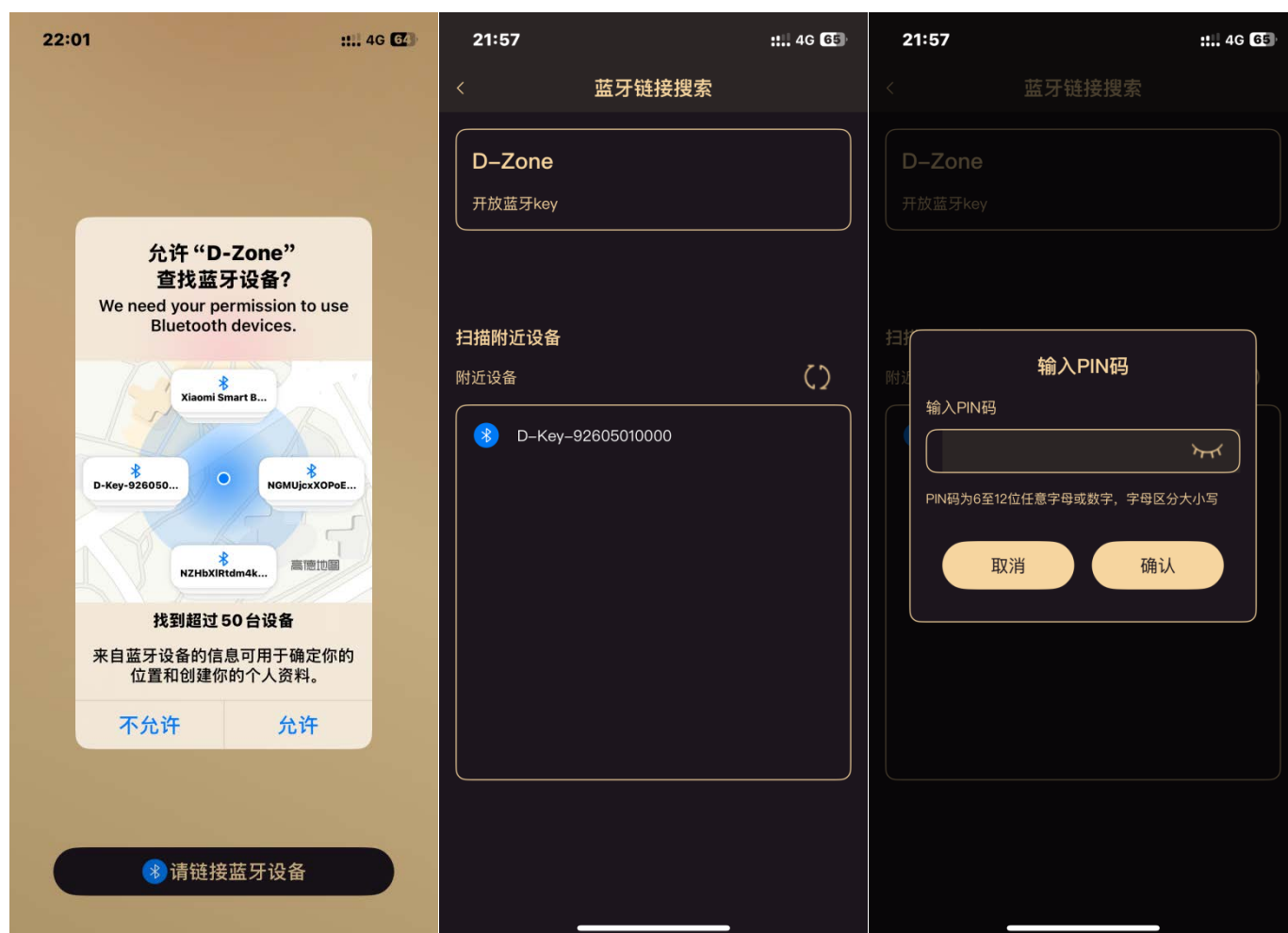
登錄需完成“藍牙連接→設備選擇→PIN 碼校驗→設備綁定”四步，具體流程如下

1. 打開 APP，點擊【請連接藍牙設備】，允許藍牙、位置、檔訪問許可權。
2. 點按藍牙硬體「D-Key」的【OK】鍵啟動藍牙裝置，（啟動後裝置自動進入藍牙配對模式），保持手機與硬體距離 ≤ 1 米。
3. 在設備列表選擇【D-Key xxx】（xxx 為該硬體 ID），輸入初始 PIN 碼：123456（注意：初始 PIN 碼登入後會強制導引 PIN 碼修改，修改完 PIN 碼後亦可在 APP 設定中再次修改 PIN 碼以保障資訊安全，修改後需牢記，遺忘無法找回。

補充：每次登錄輸入 PIN 碼或修改 PIN 碼時，軟體會提示：請按設備 OK 鍵確認，這時只要點按藍牙硬體 D-Key 上的【OK】鍵即可。

4. 登錄成功，APP 自動與當前硬體綁定，後續僅該硬體可登錄，包括主設備和輔設備。解綁規則：僅卸載 APP 後綁定關係解除，卸載重裝 APP 後可重新綁定新的硬體。

重要：切換一套設備中的主設備或輔設備登錄時，需在登錄選擇設備的介面長按已保存的設備”D-Key xxx”，根據介面提示刪除該設備，刪除後可再嘗試連接一套設備中的另一個設備。



3 底部導航與板塊佈局

軟體底部固定 3 個導航入口，雲交互置於中間位置：

1. **【檔】**：本機檔案、安全區、雲空間
2. **【雲交互】**：加密聊天、好友、群組
3. **【基本設定】**：通訊錄、個人記事本、系統設置



4【檔】板塊——加密存儲

入口：底部導航 → **【檔】**

包含三個平行同級頁面：**本機檔案** → **安全區** → **雲空間**

4.1 本機檔案

- 展示手機本地全部普通檔，等同於手機自帶的系統檔管理。
- 內置**檔棧**：記錄已移入安全區、導出、分享加密包、接收解密後的檔。
- 支持長按檔：單選 / 多選、分享、刪除、移入安全區。

4.2 安全區（核心加密區）

- APP 自動生成的獨立加密存儲空間，僅藍牙硬體驗證通過可訪問。
- 支持存入：圖片、音視頻、文檔、壓縮包等所有檔格式。

- 操作：長按檔後可選擇明文導出、密文導出、刪除、分享加密、移動、重命名、一鍵上傳雲空間。
- 安全特性：不被系統相冊、播放器掃描，不對外暴露。



4.3 雲空間——加密雲端備份

4.3.1 登錄與使用規則

- 默認不啟動、不聯網，點擊後自動觸發 PIN 碼登錄。
- 未開通 / 已過期：按鈕置灰，顯示前往充值入口（跳轉網頁）。
- 登錄成功展示：雲端檔列表、已用空間、到期時間。

4.3.2 核心功能

- 唯一數據來源：僅安全區檔可上傳。
- 唯一下載目標：僅下載回到安全區。
- 支持操作：單選 / 多選 / 一鍵全選、上傳、一鍵還原、刪除。
- 檔衝突處理：提示跳過 / 覆蓋 / 重命名。
- 新手機還原：自動恢復原目錄結構與檔案名。
- 數據保留：免費試用 1 個月，到期未續費保留 1 個月後清空。
- 雲空間僅與安全區互通，不支持本地普通檔直接上傳。



5 【雲交互】板塊——加密通訊

入口：底部導航 中間位置 → 【雲交互】

功能介紹：雲交互為所有 D-Zone 用戶提供了加密即時通訊功能，以用戶手中 **D-key ID** 為唯一身份標識，無需註冊即可匿名聊天，所有聊天內容均通過 D-key 硬體加密，僅聊天交互的雙方可以解密查看，平臺及任何其他人士完全無訪問許可權，雲交互聊天記錄後臺不存儲，僅臨時緩存，已讀即清理，極致保障用戶的隱私安全。

5.1 好友與群組管理

- 打開雲交互直接顯示好友 / 群組列表。
- 添加好友：按 D-Key ID 或軟體內通訊錄添加，需對方同意。
- 支持功能：本地備註名、本地自定義頭像、拉黑防騷擾。
- 快捷導入：可從 D-Zone 已有的雲備份中一鍵還原雲交互的通訊錄。
- 群組管理：可在群組中查看、添加群友等。

5.2 聊天功能

- 支持發送：文字、檔、語音（不支持語音/視頻通話）。
- 檔選擇：可從本機或安全區選取。

- 消息存儲：手機本地獨立開闢雲交互安全區加密存儲。
- 記錄備份：可選擇一鍵雲備份將本地所有聊天記錄加密備份至雲端，備份後可還原至本地。
- 消息狀態：已讀統一顯示已送達；發送失敗標紅 / 顯示感嘆號。
- 消息管理：單條刪除、一鍵清空、文字 / 檔可轉發，語音不可轉發。
- 未讀提示：紅點 + 數字角標（APP 圖示、雲交互入口、會話列表）。
- 消息通知：APP 後臺橫幅推送。



6 【通訊錄】板塊（置於基本設定板塊內）

入口：底部導航 → 【基本設定】 → 【通訊錄】

功能介紹：管理 D-Key ID 好友資訊，主要用於安全區檔分享加密時選擇要指定分享的好友，以及用於雲交互聊天中好友的添加，支持“導出/導入”，可將通訊錄導出保存至手機指定路徑。

- 添加好友：輸入對方 D-Key ID（需從好友處獲取）、設置昵稱、分組（家人 / 同事等），點擊確認即可添加（無需對方同意）。
- 分組管理：自定義添加、編輯、刪除分組。
- D-Key ID 獲取：可在【基本設定】介面頂端查看自己的 D-Key ID，長按可複製
- 好友管理：查看 D-Key ID、修改昵稱、修改分組、刪除好友。
- 通訊錄備份（導入和匯出）：匯出是指將通訊錄匯出至【檔案棧】或【D-Key 設備】進行存儲備份，導入是

指將已備份的通訊錄檔案修復至當前軟件通訊錄清單中



7 【基本設定】板塊

入口：底部導航 → 【基本設定】

- 查看 D-Key ID：查看本人已綁定設備的 D-Key ID（長按可複製）。
- 個人記事本：編輯並加密存儲關鍵資訊（如隱私資訊、帳號密碼等），支持上傳最多 9 張圖片。保存後自動加密，僅連接藍牙硬體可查看/編輯。
- 設備類型查看：查看當前登錄 D-Key 設備類型，如主設備/輔設備。
- 其他設置：修改 APP 顯示語言、修改設備 PIN 碼、檢查版本更新、退出登錄、一鍵刪除所有安全區資料等。



8 加密、解密、分享與雲備份

8.1 加密操作

- 檔加密：移入安全區自動加密。
- 記事本加密：保存即加密。
- 雲交互消息：本地硬體加密存儲。

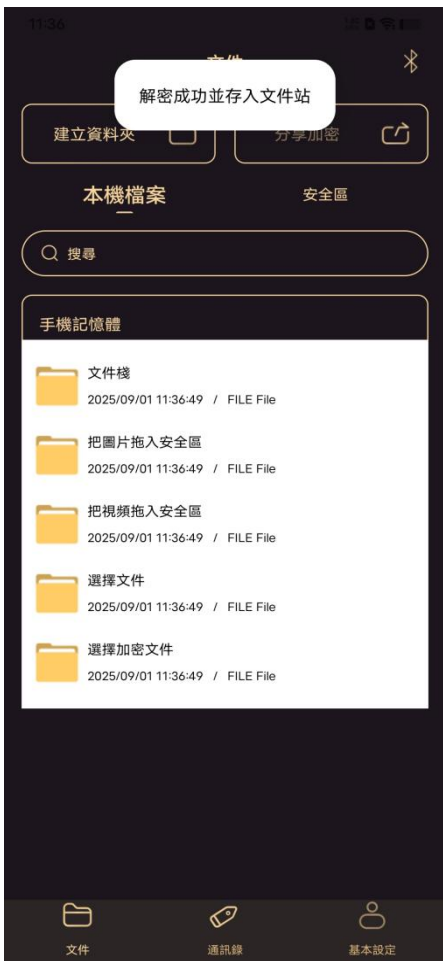
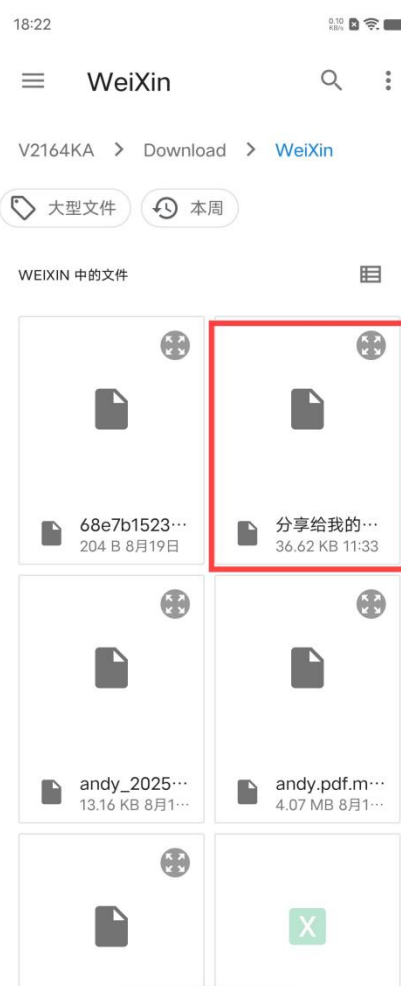
8.2 解密操作

- 安全區檔解密（明文導出）
 - › 路徑：【檔】→【安全區】→長按選中加密檔→點擊【明文導出】。
 - › 說明：解密後的普通檔自動存放至【檔棧】，可正常查看/使用。



• 好友分享的加密檔解密

- 前提：需將收到的加密檔下載至手機本地。
- 路徑：【檔】→【本機檔案】→【選擇加密檔】→找到並點擊該收到的分享檔。
- 說明：僅限對收到的好友指定加密分享給你的檔解密，並使用綁定的 D-Key 硬體可解密成功，解密後文件顯示在【檔棧】，非指定加密分享給你的檔無法解密。



- **雲交互內消息解密：**登錄雲交互後接收方自動解密，本地保存記錄。
- **雲空間內檔解密：**登錄雲空間後需對雲空間內檔操作還原至安全區才能解密查看。

8.3 檔分享

- **普通分享：**

＞ 路徑：**【檔】**→**【本機檔案】**→**【檔棧】**→長按選中普通/加密檔（支持 單選/多選）→點擊介面底 端**【分享】**。

＞ 操作：選擇分享媒介（如微信、郵箱等），發送給目標接收者。

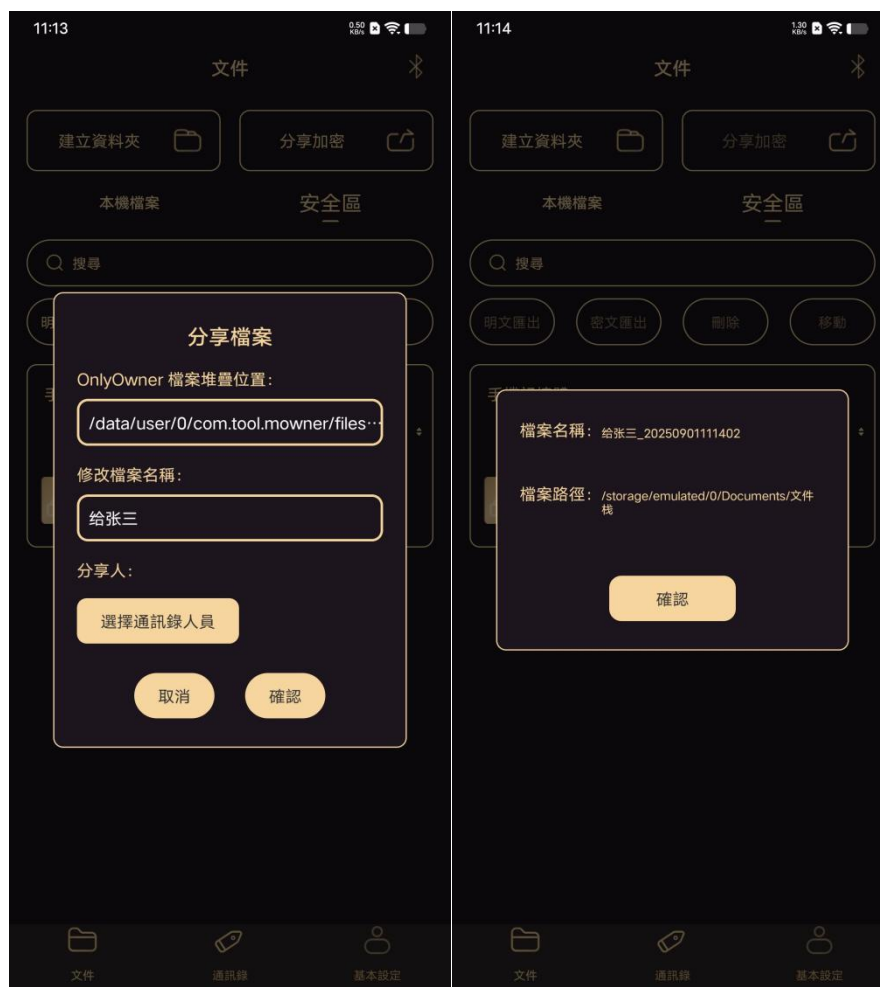
- **加密分享：**

需先生成“加密分享包”，再通過普通分享發送，具體步驟：

1. 生成加密分享包：

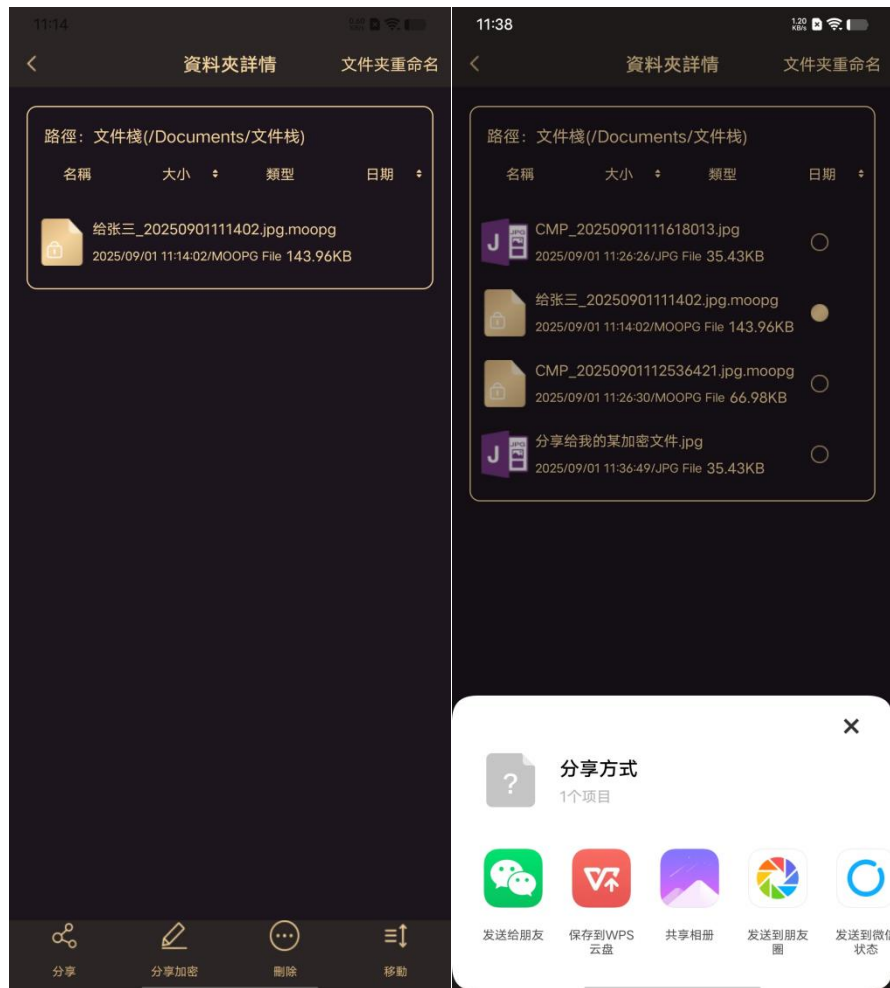
＞ 路徑：**【檔】**→**【本機檔案】**→**【檔棧】**→長按選中需分享的檔→點擊**【分享機密】**。

＞ 操作：重命名分享檔，從通訊錄中選擇目標好友（支持單個、多個好友或按分組選擇），點擊“確認生成”；生成的加密包自動存放至**【檔棧】**。



2. 發送加密包：

＞ 路徑：找到【檔棧】中的加密包→長按→點擊【分享】→選擇媒介發送給好友。



• 分享檔管理

＞ 路徑：【基本設定】→【分享檔案記錄】。

＞ 功能：可查看所有“收到的加密分享檔”和“加密分享出去的檔”，支持直接 點擊查看。

8.4 雲備份與還原

- 雲備份：安全區檔 → 單選 / 多選 / 一鍵上傳至雲空間。
- 雲還原：雲空間檔 → 一鍵還原至安全區原目錄。
- 備份說明：雲交互中的聊天記錄需單獨由雲交互中一鍵雲備份保存和還原。

9 雲空間收費規則與權益說明

9.1 付費功能——雲空間

- 身份依據：硬體 D-Key ID 唯一帳號體系。
- 試用政策：新用戶免費試用 1 個月。
- 續費方式：統一網頁端充值，APP 內 僅展示狀態，過期或空間不足時介面顯示前往充值入口（跳轉網頁）。
- 過期規則：按鈕置灰，不可上傳，檔保留 1 個月後清空。

9.2 付費功能——雲交互

- **開通雲空間 = 自動開通雲交互**，與雲空間**共用帳號與權益**，不單獨售賣。
- 試用政策：免費試用權益與雲空間等同。
- 過期規則：**僅可接收消息，無法發送消息**。
- 發送提示：向未付費用戶發消息時，提示 “對方為非授權用戶”。

10 注意事項

1. 更新安全：APP 更新（應用市場或 APK 包更新）不會導致用戶數據丟失、損壞或無法解密。
2. 登錄安全：雲空間、雲交互每次使用需單獨 PIN 碼登錄。
3. 隱私保護：安全區、雲交互檔不會在系統相冊、播放器中顯示。
4. 防誤刪：手機清理軟體請勿刪除 D-Zone 相關目錄，避免加密檔丟失。
5. 硬體依賴：所有加密、解密、登錄操作均需綁定的 D-Key 藍牙硬體，PIN 碼遺忘無法找回，硬體丟失或損壞將無法訪問數據。
6. 傳輸安全：藍牙設備連接時，所有通信數據均經過加密處理，保障傳輸過程安全。
7. 檔備份：建議定期通過【雲空間】備份和【安全區】的“明文導出”或“密文導出”功能備份重要檔，防止意外刪除或丟失。

11 常見問題提示

1. 雲空間無法登錄？檢查藍牙連接、PIN 碼、網路、服務是否過期。
2. 雲消息發不出去？檢查權益是否過期、對方是否非授權、網路是否正常。
3. 檔解密失敗？僅綁定的 D-Key 硬體可解密。
4. 雲空間檔丟失？雲空間權益過期超過 1 個月系統自動清空。
5. 其他使用過程中問題，歡迎隨時聯繫官網溝通：<https://www.onlyownerhk.com/>

D-Zone Mobile Security App User Manual V2.0

Update date: May 26, 2026

Catalogue

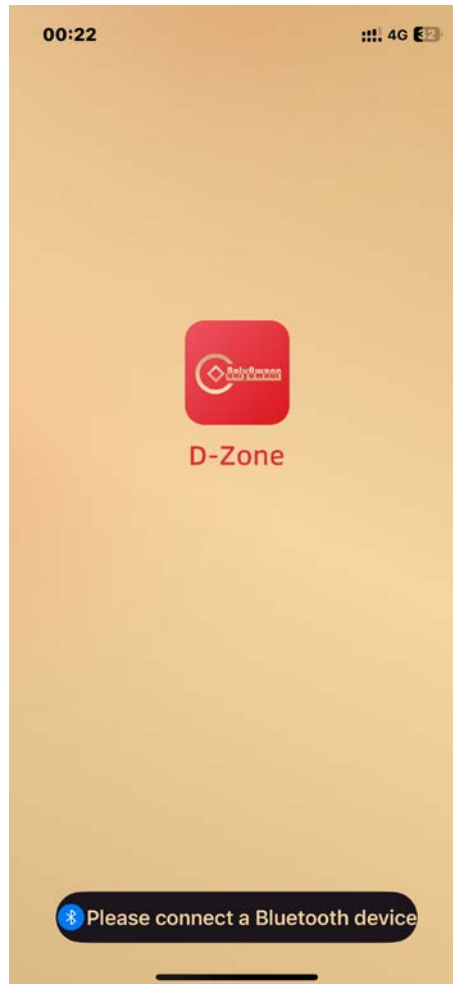
2 Installation and Login	18
2.1 Installation Instructions	18
Download the update address: https://onlyownerhk.com/ft-code-21.html	18
2.2 Login and Bluetooth Device Binding	18
3 Bottom Navigation and Section Layout	19
1. [Files]: Local Files, Secure Zone, Cloud Storage	19
2. [Cloud Interaction]: Encrypted chats, friends, groups	19
3. [Basic Settings]: Contacts, Personal Notebook, System Settings	19
4[Section]Section — Cryptographic Storage	20
4.1 Local File	20
4.2 Security Zone (Core Encryption Zone)	20
4.3 Cloud Storage - encrypted cloud backup	21
4.3.1 Login and Usage Rules	21
4.3.2 Core Functions	21
5 [Cloud Interaction]Section — encrypted communication	22
5.1 Friend and Group Management	22
5.2 Chat Function	22
6 [Contact List] section (located within the Basic Settings section)	23
7 [Basic Settings]Section	24
8 Encryption, decryption, sharing, and cloud backup	25
8.1 Encryption Operation	25
8.2 Decryption Operation	25
8.3 File Sharing	28
8.4 Cloud Backup and Restoration	29
9 Cloud Storage Pricing Rules and Benefits Description	29
9.1 Paid Features - Cloud Storage	29
9.2 Paid Features - Cloud Interaction	30
10 Precautions	30
11 Frequently Asked Questions	30

1 About the D-Zone

D-Zone is a decentralized mobile data encryption and secure communication application that requires no registration or authentication. It must be used in conjunction with the dedicated Bluetooth hardware D-Key, where the D-key ID serves as the unique identity identifier. All data is encrypted using hardware-based encryption protocols and stored in ciphertext format both locally and in the cloud, ensuring maximum user privacy protection. The application primarily offers three integrated security capabilities: D-Zone is a decentralized mobile data encryption and secure communication application that requires no registration or authentication. It must be used in conjunction with the dedicated Bluetooth hardware D-Key, where the D-key ID serves as the unique identity identifier. All data is encrypted using hardware-based encryption protocols and stored in ciphertext format both locally and in the cloud, ensuring maximum user privacy protection. The application primarily offers three integrated security capabilities: D-Zone is a decentralized mobile data encryption and secure communication application that requires no registration or authentication. It must be used in conjunction with the dedicated Bluetooth hardware D-Key, where the D-key ID serves as the unique identity identifier. All data is encrypted using hardware-based encryption protocols and stored in ciphertext format both locally and in the cloud, ensuring maximum user privacy protection. The application primarily offers three integrated security capabilities:

- Safe Zone: Local privacy files are encrypted for storage and sharing
- Cloud Space: Secure Zone File Encryption for Cloud Backup/ restoration
- Cloud Interaction: Hardware-level encrypted text 文件/voice message chats

Important: The D-Key device comes with two hardware components upon factory delivery—one primary device and one secondary device. Both devices share the same encryption space to address the issue of being unable to recover encrypted files stored on a phone if only one device is lost. The main differences are as follows: After logging in, the primary device supports all functions of the D-Zone software; after logging in, the secondary device only has decryption and viewing capabilities, including access to contacts and ability to decrypt and view all encrypted shared files as well as encrypted files in cloud interactions or cloud storage.



2 Installation and Login

2.1 Installation Instructions

- Support System: Compatible with Android and iOS. This app is available for download on mainstream domestic app stores (iOS, App Store, Huawei App Market) and international app stores (iOS, Google Play). Huawei smartphones support the HarmonyOS system (not the pure HarmonyOS version).
- APK installation method: Download and install the APK

Download the update address: <https://onlyownerhk.com/ft-code-21.html>

2.2 Login and Bluetooth Device Binding

To log in, complete the four steps: "Bluetooth connection → Device selection → PIN verification → Device binding." The detailed process is as follows:

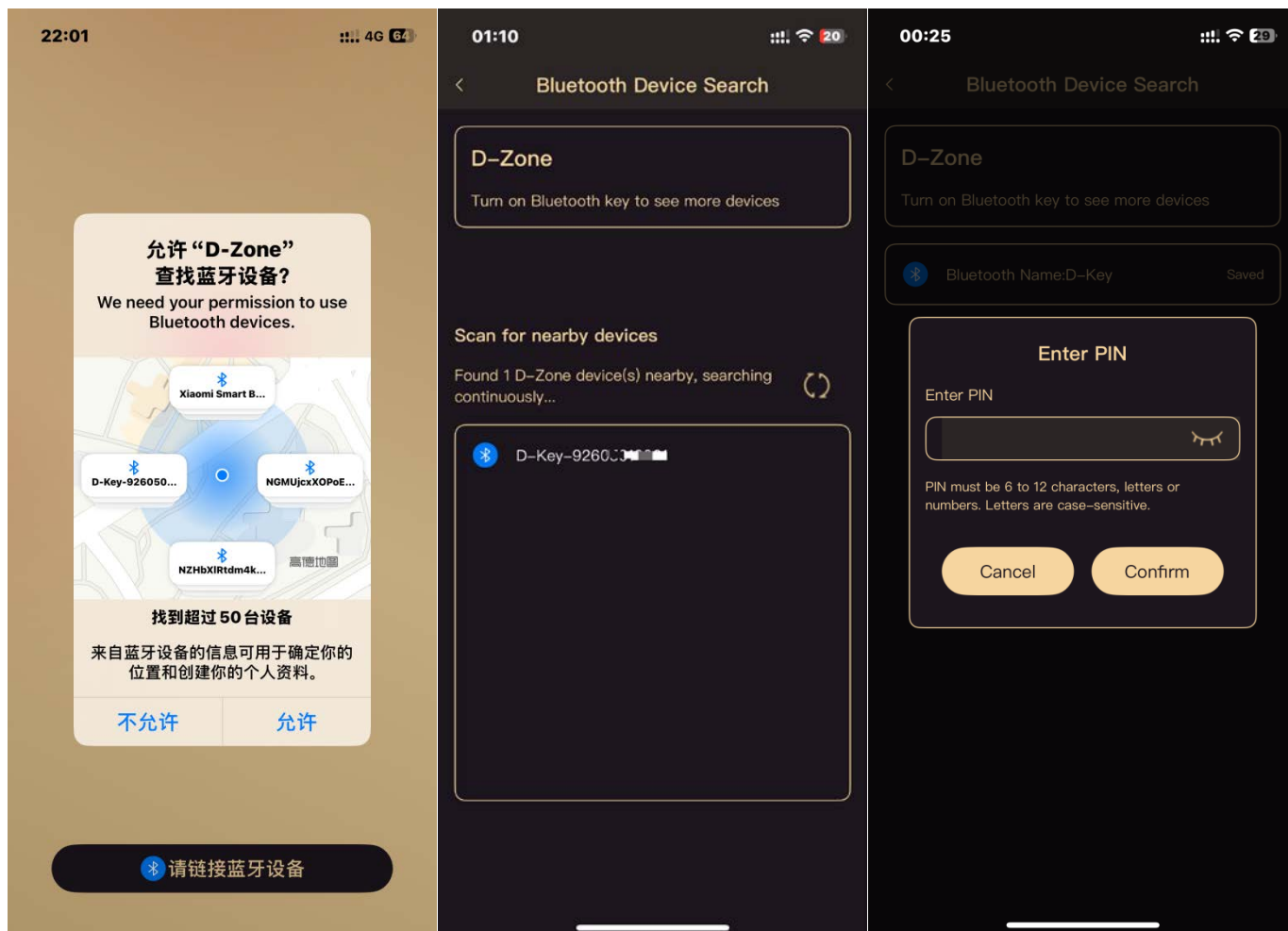
1. Open the app, tap [Connect Bluetooth Device], and grant access to Bluetooth, location, and file permissions.
2. Press the [OK] key on the Bluetooth hardware's "D-Key" to activate the Bluetooth device (the device will automatically enter Bluetooth pairing mode upon activation). Maintain a distance of ≤ 1 meter between the phone and the hardware.
3. In the device list, select [D-Key xxx] (where xxx is the hardware ID), then enter the initial PIN: 123456. Note: The initial PIN will automatically prompt you to change it upon login. After modification, you may adjust the PIN again in the

app settings for enhanced security—remember this PIN, as forgetting it cannot be recovered.

Additional note: Each time you enter or change your PIN code upon login, the software will prompt you to confirm by pressing the device's OK button. Simply press the [OK] button on the Bluetooth hardware's D-key at this point.

4. Login successful. The app automatically binds to the current hardware, and only this hardware—both the primary and secondary devices—can be logged in afterward. Unbinding rule: The binding is removed only after uninstalling the app; you can bind a new hardware device after reinstalling the app.

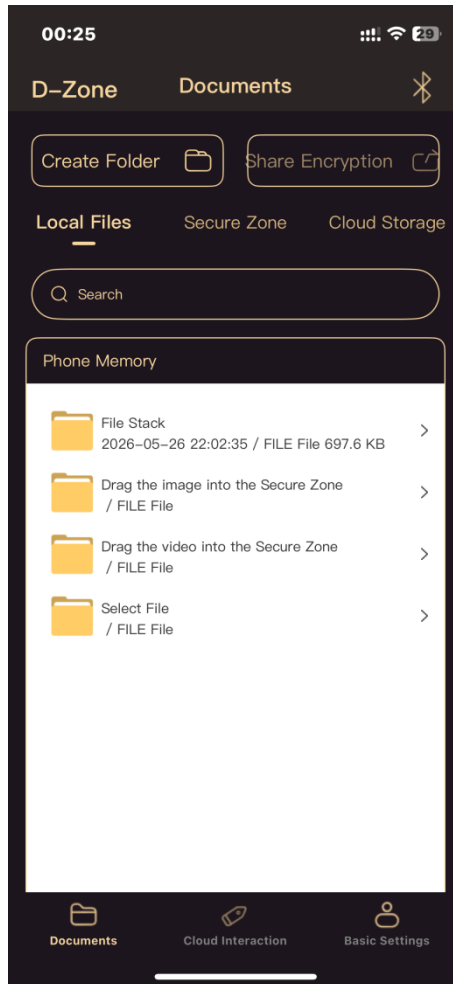
Important: When logging in to switch between the primary and secondary devices in a configuration, long-press the saved device "D-Key xxx" in the device selection interface and follow the prompts to delete it. After deletion, you may attempt connecting to another device in the same configuration.



3 Bottom Navigation and Section Layout

The software features three navigation entries at the bottom, with cloud interaction positioned in the center:

1. [Files]: Local Files, Secure Zone, Cloud Storage
2. [Cloud Interaction]: Encrypted chats, friends, groups
3. [Basic Settings]: Contacts, Personal Notebook, System Settings



4[Section]Section — Cryptographic Storage

Entry: Bottom Navigation → [File]

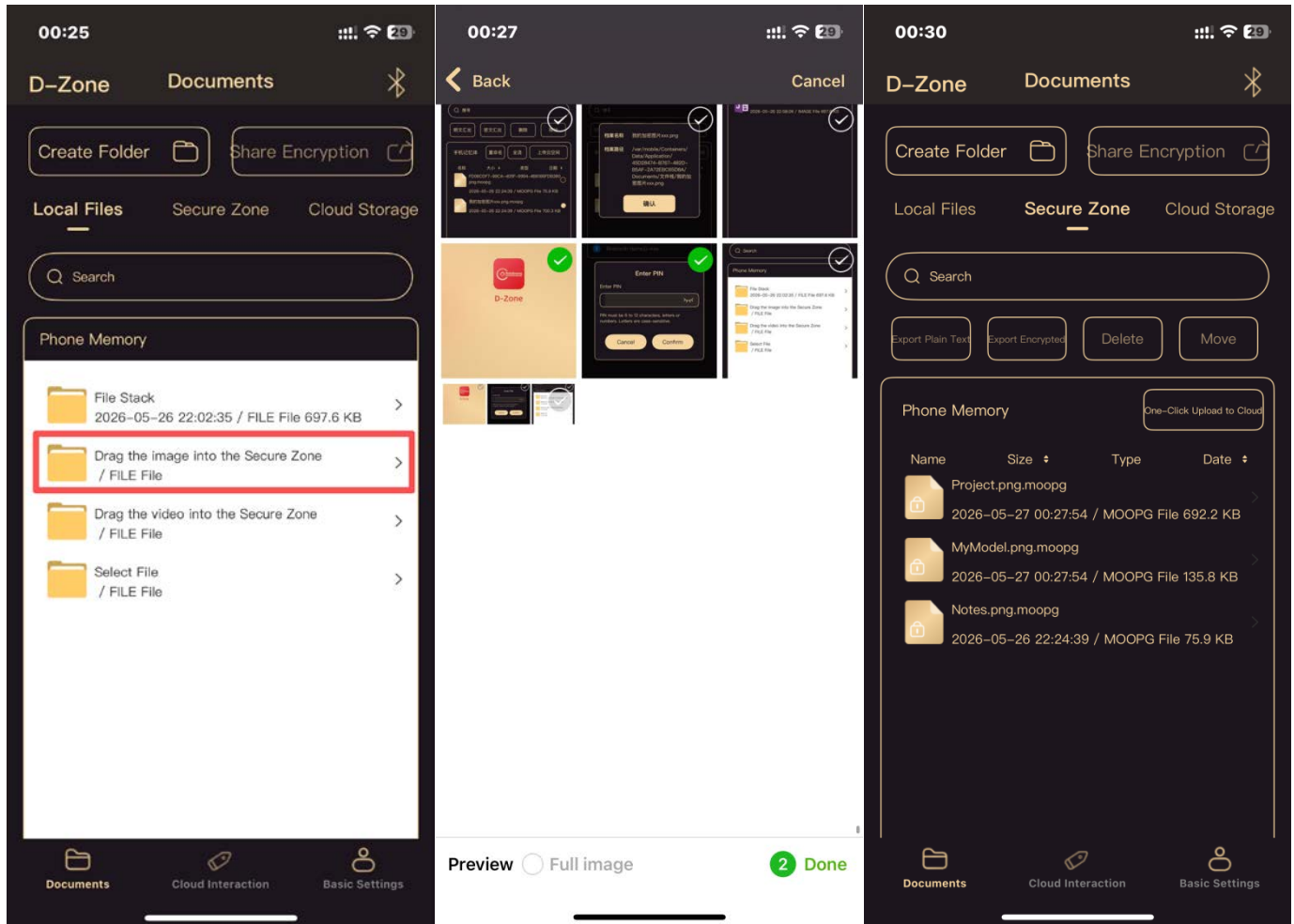
Consists of three parallel pages: Local Files → Secure Area → Cloud Space

4.1 Local File

- Show all local standard files on the phone, equivalent to the built-in system file management.
- Built-in file stack: Records files moved to the secure zone, exported, shared encrypted packages, and received decrypted files.
- Support long-press options: Single selection/Multiple selections, Share, Delete, Move to secure area.

4.2 Security Zone (Core Encryption Zone)

- The APP automatically generates an independent encrypted storage space accessible only after successful Bluetooth hardware authentication.
- Supports saving: images, audio and video, documents, compressed files, and all other file formats.
- Operation: Long press the button to select Plain Text Export, ciphertext Export, Delete, Share Encrypted File, Move, Renamed, or One-Click Upload to Cloud Storage.
- Security features: Not scanned by the system album or player, and not exposed externally.



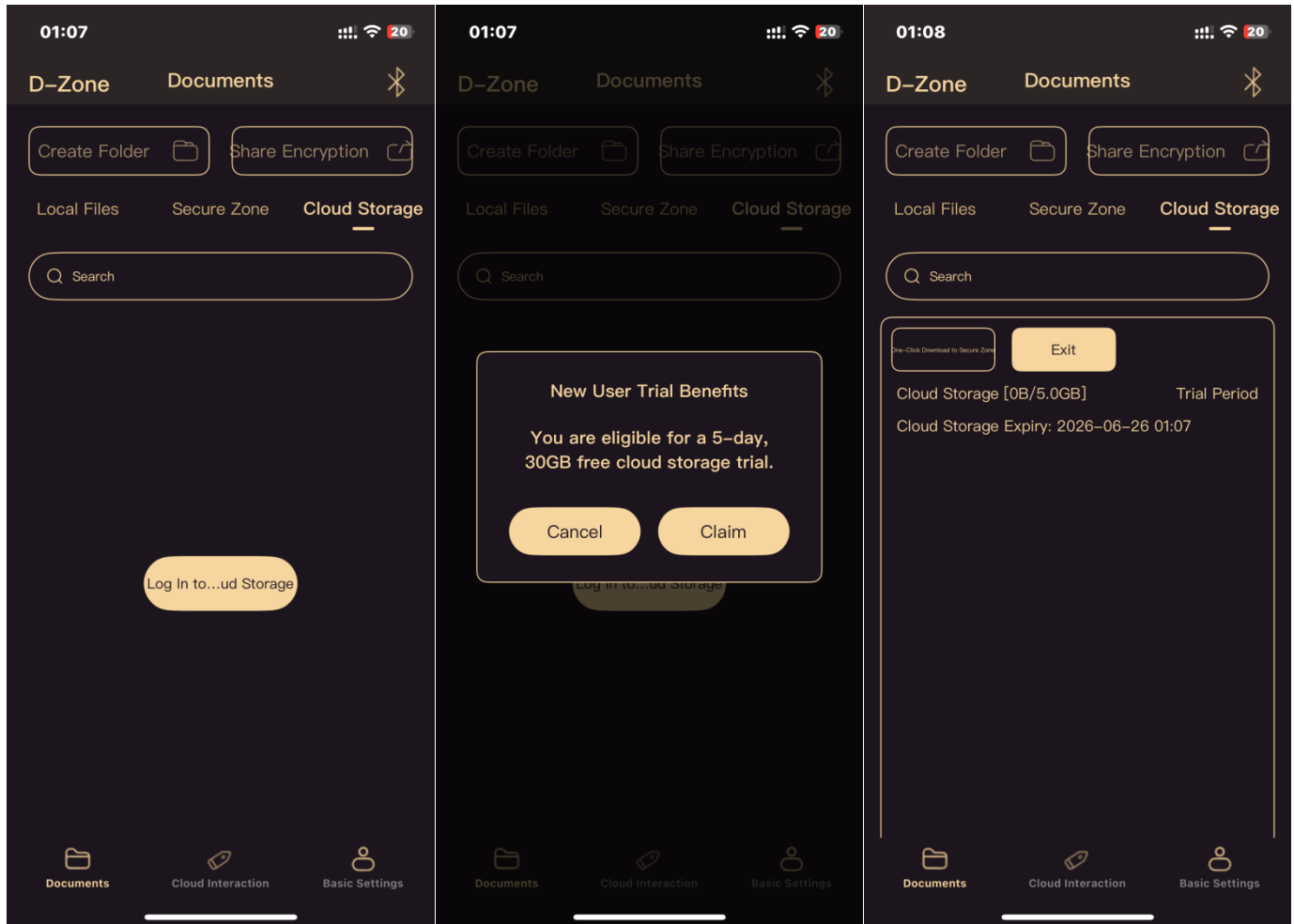
4.3 Cloud Storage – encrypted cloud backup

4.3.1 Login and Usage Rules

- It does not start or connect to the network by default; clicking it automatically triggers PIN-based login.
- Unactivated/ expired: The button turns gray and displays the recharge portal (redirects to a webpage).
- Successful login display: cloud file list, used space, and expiration time.

4.3.2 Core Functions

- Single data source: Only the secure zone file can be uploaded.
- Only download target: Download only to the secure area.
- Supported operations: Single selection / Multiple selection / One-click selection, Upload, One-click restore, Delete.
- File conflict resolution: Skip / Overwrite / Renamed.
- New phone restoration: automatically restore the original directory structure and file names.
- Data retention: Free trial for 1 month. If not renewed upon expiration, the data will be deleted after 1 month.
- Cloud storage only communicates with the secure zone and does not support direct uploads of local regular files.



5 [Cloud Interaction]Section — encrypted communication

Entry: Bottom Navigation, Middle Position → [Cloud Interaction]

Feature Overview: Cloud Interaction provides all D-Zone users with encrypted real-time communication. Using the D-key ID as the unique identity identifier, users can engage in anonymous chats without registration. All chat content is encrypted via D-key hardware and accessible only to the communicating parties; neither the platform nor third parties have access. Chat records are not stored on the backend but temporarily cached and automatically deleted upon read confirmation, ensuring maximum user privacy protection.

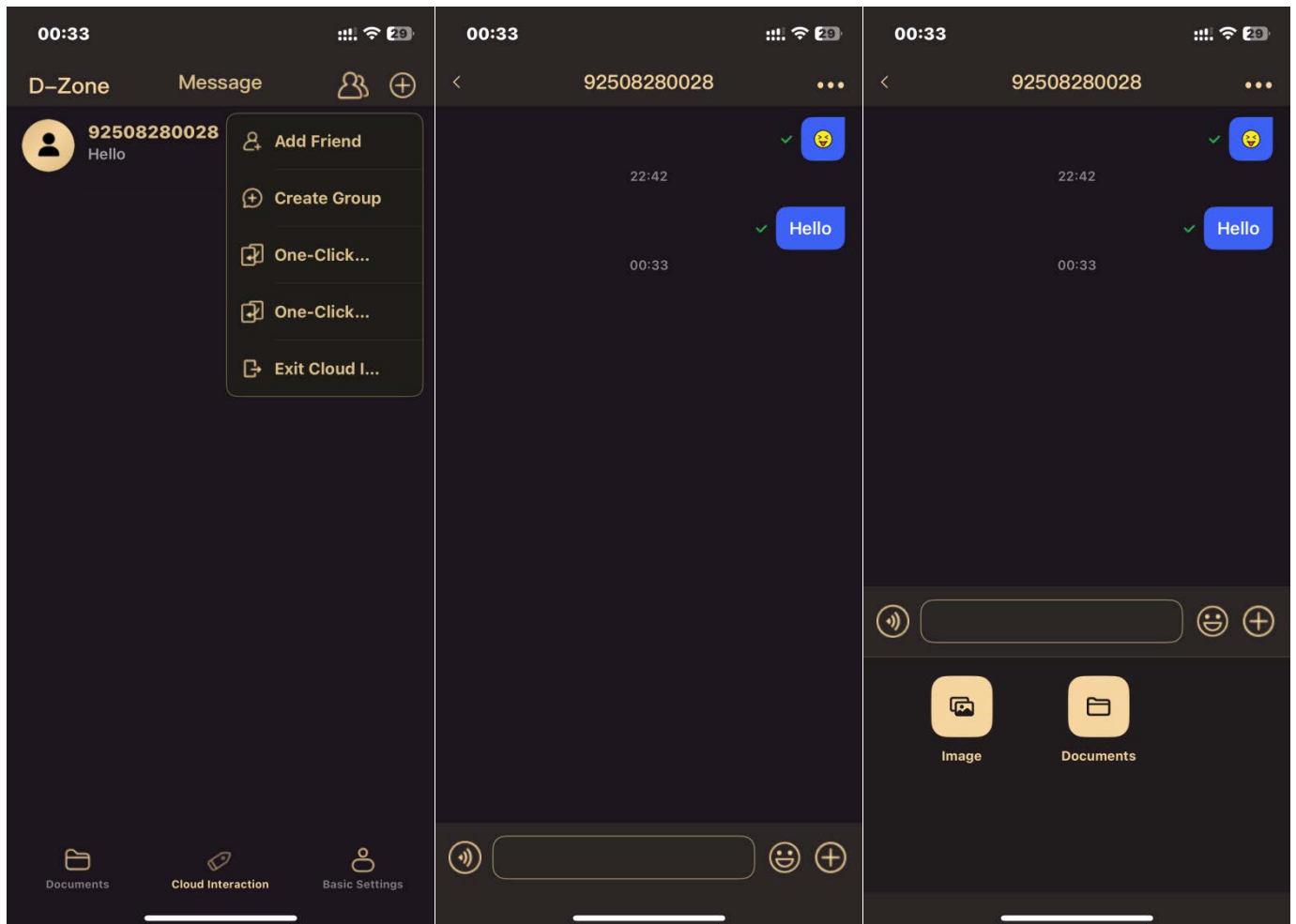
5.1 Friend and Group Management

- Open Cloud Interaction to directly display the list of friends/groups.
- Add friend: Add by D-Key ID or the app's contact list; consent is required.
- Support features: Local note name, local custom profile picture, block and anti-harassment.
- Quick Import: Restore contacts from cloud interactions with one click using existing cloud backups in D-Zone.
- Group Management: View and add group members within the group.

5.2 Chat Function

- Supports sending: text, files, and voice (voice/video calls are not supported).
- Option selection: You can choose from this device or the secure area.

- **Message Storage:** A dedicated encrypted security zone for cloud interaction is established locally on the smartphone.
- **Record Backup:** You can use one-click cloud backup to encrypt and store all local chat records in the cloud, and restore them locally afterward.
- **Message status:** Read uniformly displayed as delivered; failed send marked in red or displayed with an exclamation mark.
- **Message Management:** Delete individual messages, clear all at once, forward text and files; voice messages cannot be forwarded.
- **Unread notification:** red dot + number label (APP interface, cloud interaction entry, conversation list).
- **Message notification:** Banner push in the app background.



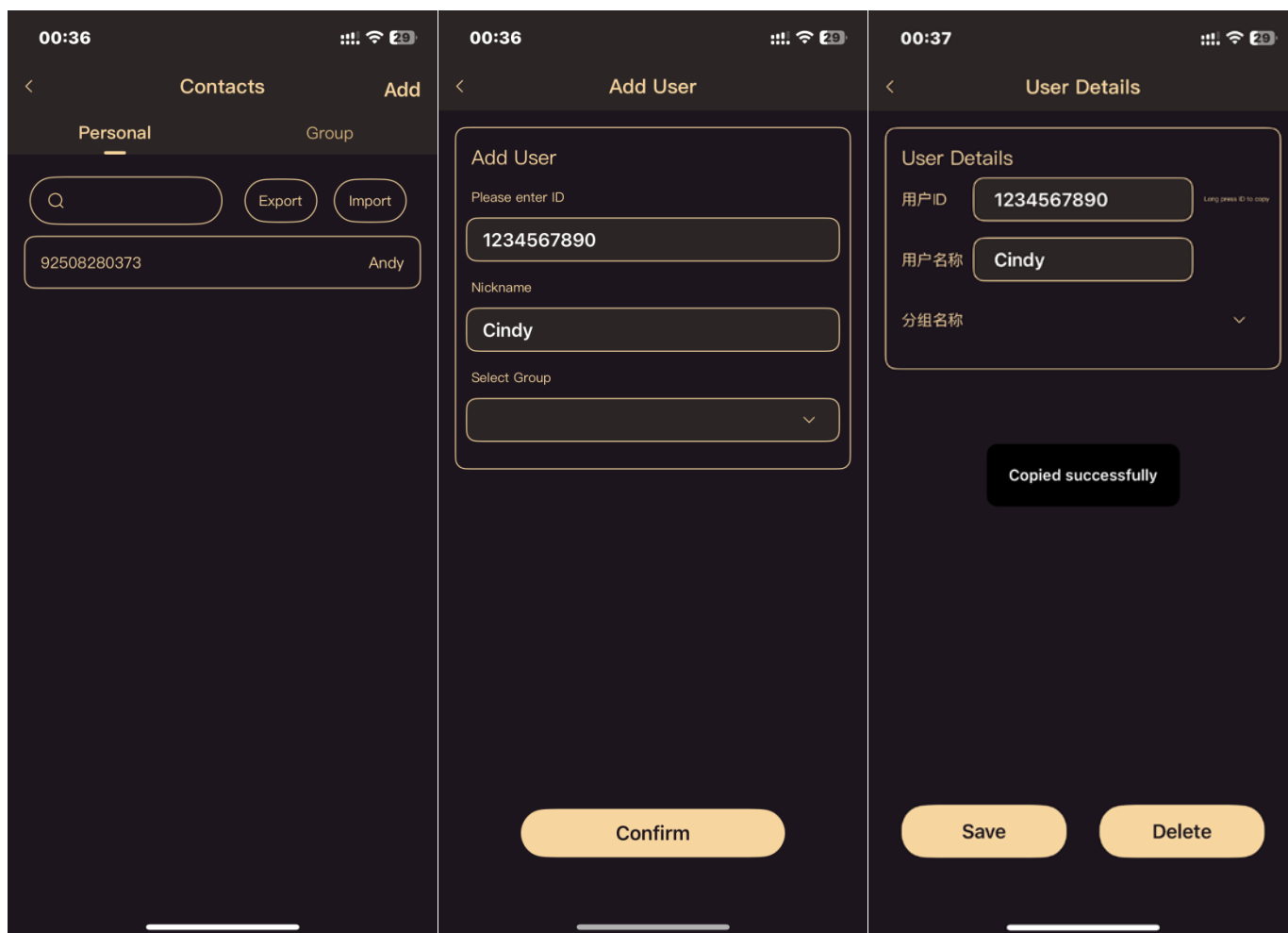
6 [Contact List] section (located within the Basic Settings section)

Entry: Bottom Navigation → [Basic Settings] → [Contact List]

Feature Description: Manage D-Key ID friend information. It is primarily used to select friends for sharing during secure zone file encryption and to add friends in cloud-based interactive chats. The feature supports "Export/Import," allowing you to save contacts to a specified path on your phone.

- **Add friend:** Enter the recipient's D-Key ID (obtainable from friends), set a nickname, group them (family/colleagues, etc.), and click Confirm to add (no consent required).
- **Group Management:** Customize adding, editing, and deleting groups.
- **D-Key ID retrieval:** You can view your D-Key ID at the top of the [Basic Settings] interface. Long press to copy it.

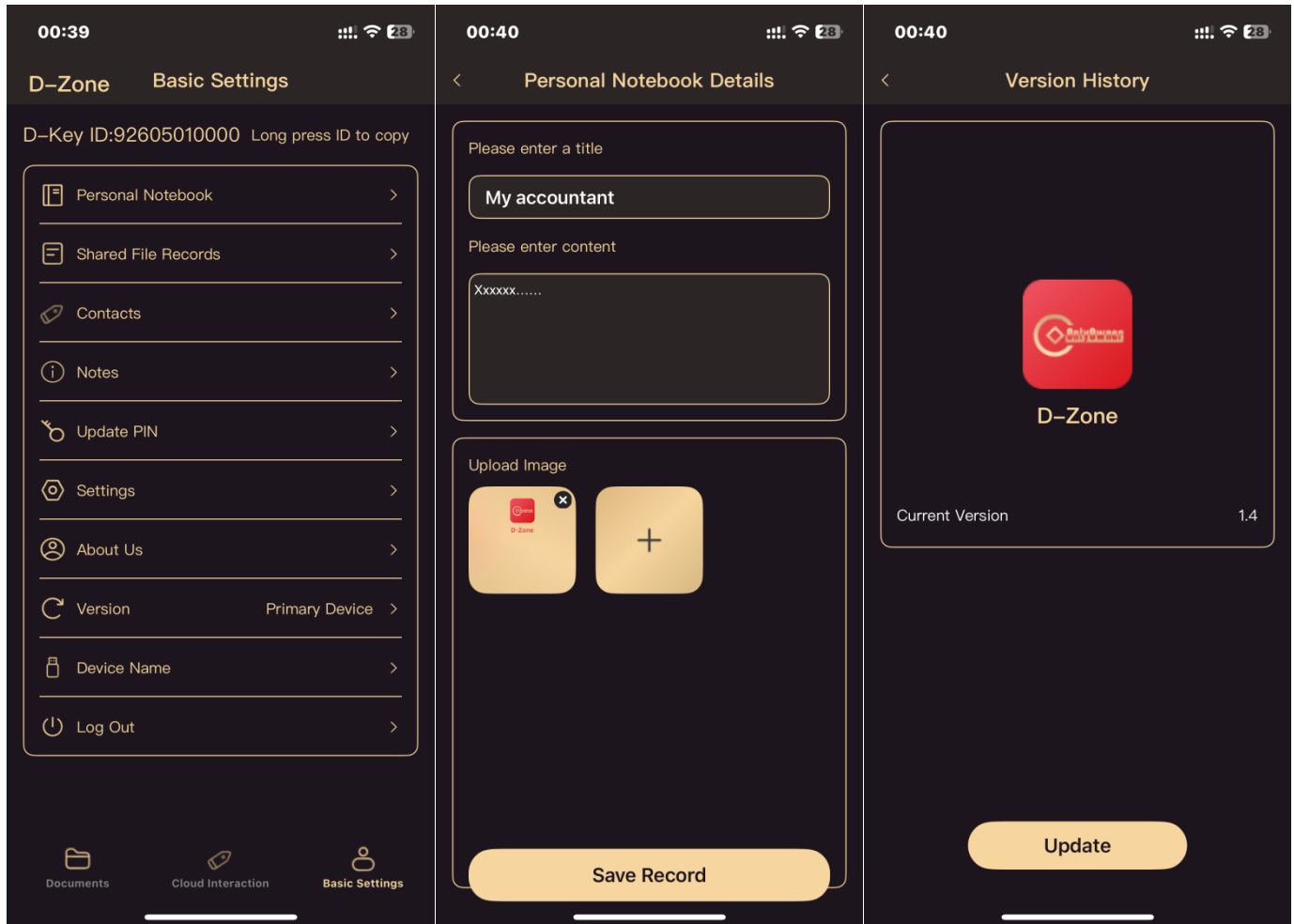
- Friend Management: View D-Key ID, Change nickname, Change group, Delete friend.
- Contact list backup (import and export): Exporting involves saving the contact list to the [File Stack] or [D-Key Device] for backup, while importing means restoring the backed-up contact file to the current software contact list.



7 [Basic Settings]Section

Entry: Bottom Navigation → [Basic Settings]

- View D-Key ID: View the D-Key ID of your bound devices (long press to copy).
- Personal Notebook: Edit and securely store critical information (such as private data, account passwords, etc.), with support for uploading up to 9 images. It automatically encrypts after saving and can only be viewed or edited when connected to Bluetooth hardware.
- Device Type View: Check the current logged-in D-Key device type, such as primary device or secondary device.
- Other settings: Change the app display language, modify the device PIN code, check for version updates, log out, and delete all security zone data with one click.



8 Encryption, decryption, sharing, and cloud backup

8.1 Encryption Operation

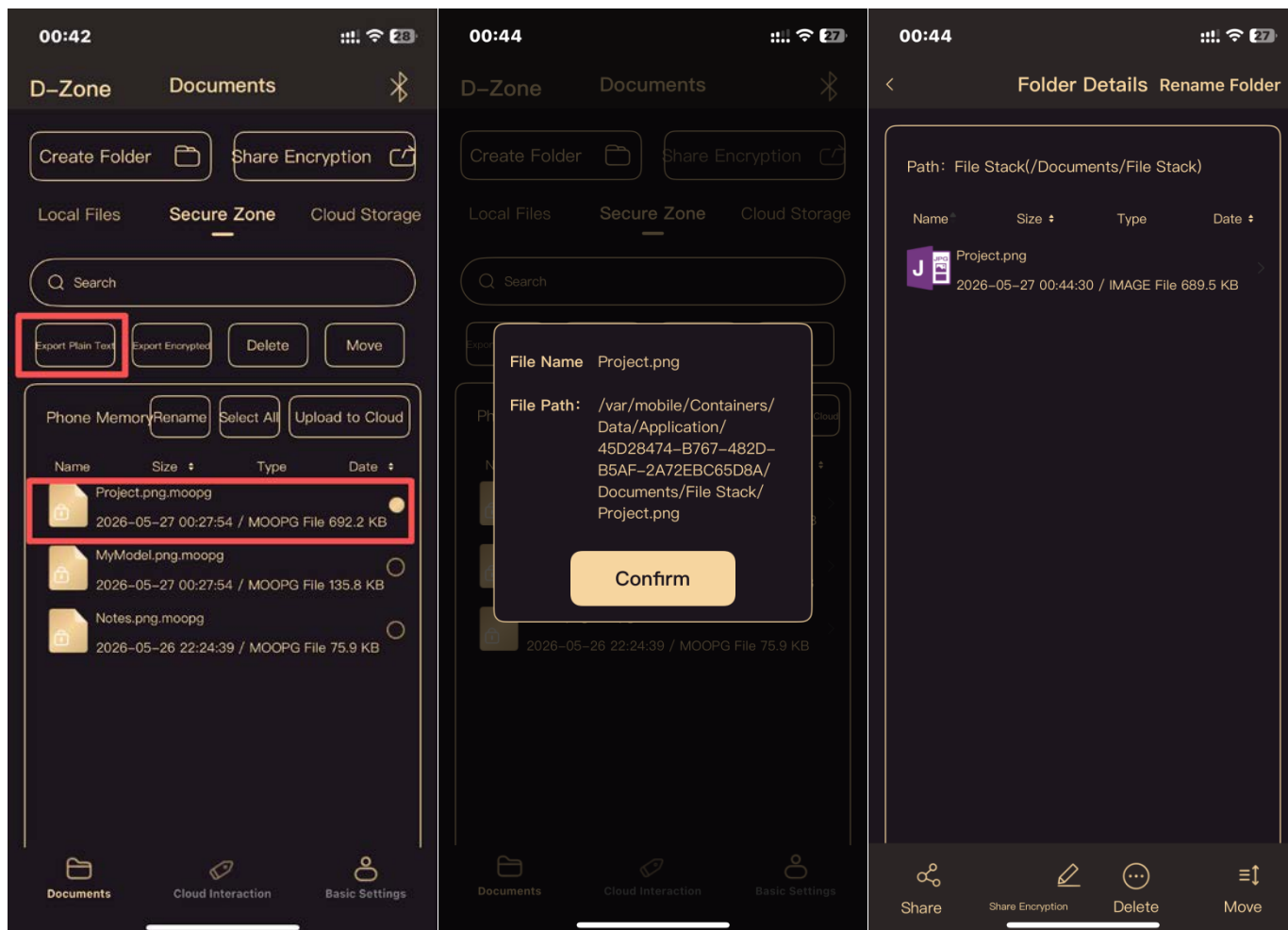
- File encryption: Auto-encrypt when moved to the secure zone.
- Notebook encryption: encrypted when saved.
- Cloud interactive message: locally encrypted storage on hardware.

8.2 Decryption Operation

- **decrypt in secure zone (export as plaintext)**

Path: [File] → [Security Zone] → Long-press to select the encrypted file → Click [Export Plain Text].

Note: The decrypted regular file is automatically saved to the [File Stack] and can be viewed or used normally.

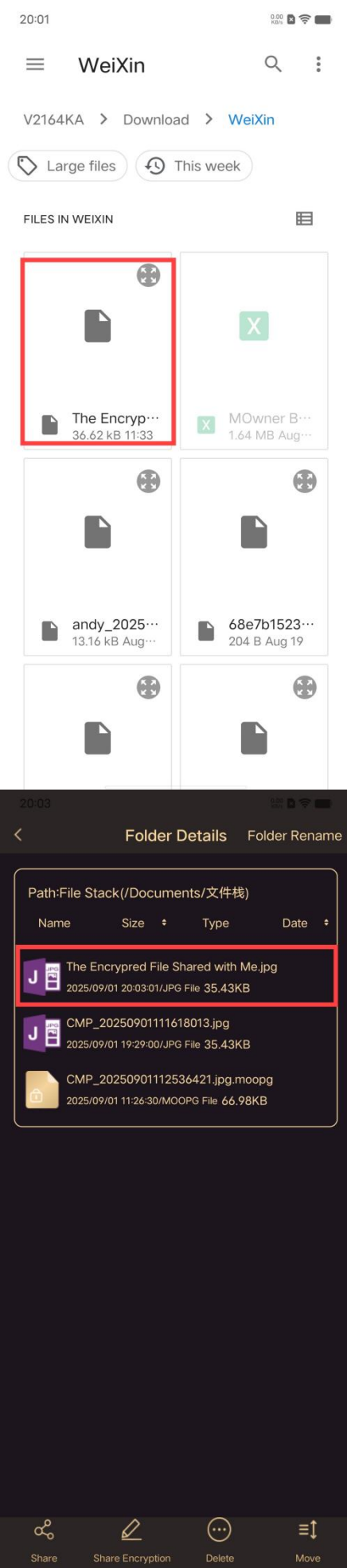
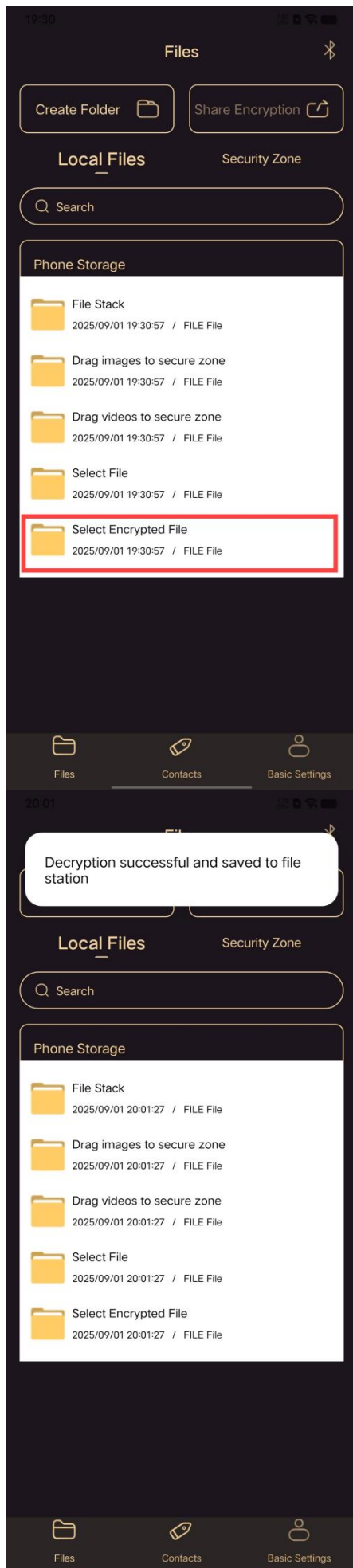


- **Decrypt the encrypted file shared by a friend**

Prerequisite: Download the received encrypted file to your local phone.

Path: [File] → [Local Files] → [Select encrypted file] → Find and click the received shared file.

Note: Only decrypt files shared with you in encrypted format from specified friends using the bound D-Key hardware. decrypted files appear in [File Stack]; files not shared in encrypted format cannot be decrypted.



- Cloud Interaction message decryption: After logging into Cloud Interaction, the recipient automatically decrypts the message and saves the record locally.
- Decryption of internal cloud storage files: After logging in to the cloud storage, restore the files to the secure zone before decryption and viewing.

8.3 File Sharing

- **General Share:**

Path: [File] → [Local Files] → [File Stack] → Long-press to select a regular/encrypted file (supports single or more selection) → Click [Share] at the bottom of the interface.

Operation: Select a sharing medium (e.g., WeChat, email, etc.) and send it to the target recipient.

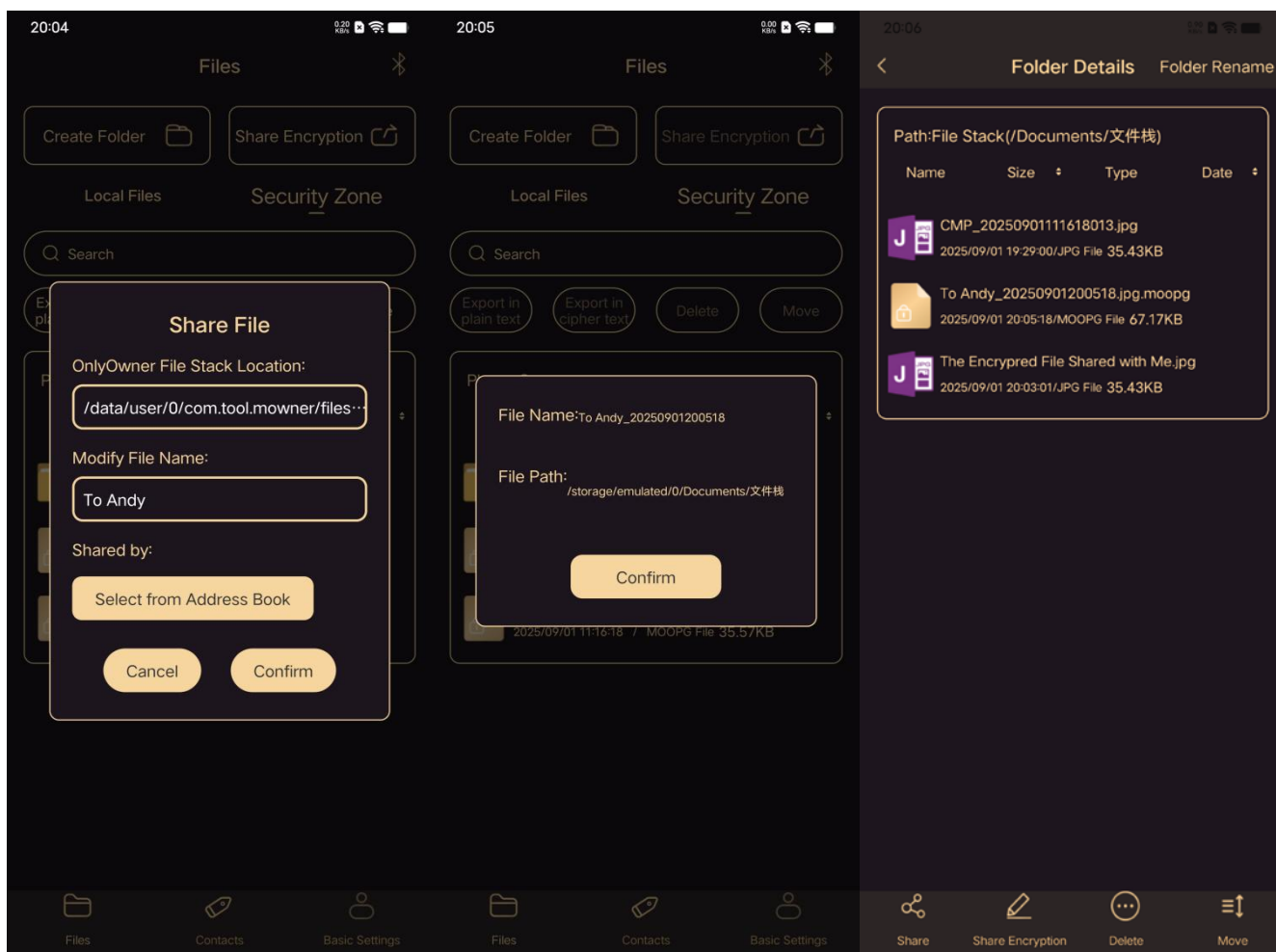
- **encrypted sharing:**

First, generate an encrypted sharing package, then send it via regular sharing. Steps:

1. Generate an encrypted sharing package:

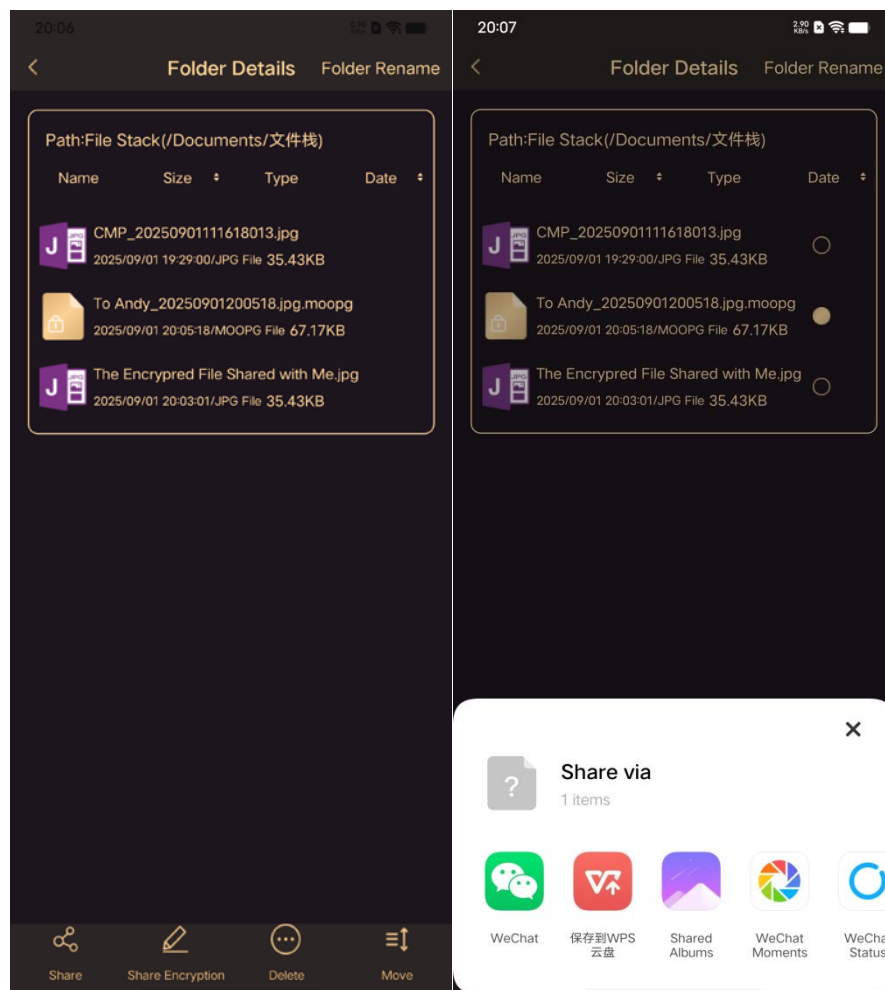
Path: [File] → [Local Files] → [File Stack] → Long-press the file to share → Click [Share Confidential].

Operation: Rename the shared file, select a target contact from the address book (supporting single, multiple contacts, or group selection), then click "Confirm Generation"; the encrypted package will be automatically saved to [File Stack].



2. Send the encrypted package:

Path: Find the encrypted file in [File Stack] → Long press → Click [Share] → Select a medium to send to friends.



- **Share File Management**

Path: [Basic Settings] → [Share File Records].

Function: View all "received encrypted shared files" and "shared encrypted files," with direct-click viewing support.

8.4 Cloud Backup and Restoration

- Cloud Backup: Secure Zone File → Single 选 / Multiple select / One-click upload to cloud storage.
- Cloud Restore: Cloud storage files → Restore with one click to the original directory in the secure zone.
- Backup Note: Chat records in Cloud Interaction must be backed up and restored separately using the one-click cloud backup feature.

9 Cloud Storage Pricing Rules and Benefits Description

9.1 Paid Features – Cloud Storage

- Identity basis: Unique account system based on hardware D-Key ID.

- Trial policy: New users get a free 1-month trial.
- Renewal method: Recharge via the unified web interface. The app only displays the status; when expiration or insufficient storage occurs, the interface shows a recharge option.
- Expiration rule: The button turns gray, preventing uploads; files are retained for one month before being deleted.

9.2 Paid Features – Cloud Interaction

- Enable Cloud Space = Auto activate cloud interaction, sharing accounts and benefits with Cloud Space without separate purchase.
- Trial Policy: The free trial benefits are equivalent to cloud storage.
- Expiration rule: Only receive messages; cannot send messages.
- Prompt: When sending a message to an unpaid user, display the message "The recipient is not authorized."

10 Precautions

1. Update Security: APP updates (via the App Store or APK package) will not result in loss, damage, or inability to decrypt user data.
2. Login Security: Cloud storage and cloud interactions require a separate PIN code for each login.
3. Privacy Protection: Secure zones and cloud interaction files will not appear in the system album or media player.
4. Error-proof deletion: Do not remove the D-Zone directory from your mobile cleanup software to prevent loss of encrypted files.
5. Hardware dependency: All encryption, decryption, and login operations require the bound D-Key Bluetooth hardware. If the PIN is forgotten and cannot be recovered, or if the hardware is lost or damaged, data access will be unavailable.
6. Transmission Security: During Bluetooth device connections, all communication data is encrypted to ensure secure transmission.
7. **File Backup: It is recommended to regularly back up important files using the "Plain Text Export" or "Ciphertext Export" features in [Cloud Space] and [Security Zone] to prevent accidental deletion or loss.**

11 Frequently Asked Questions

1. Cannot log in to the cloud storage?
Check the Bluetooth connection, PIN code, network, and whether the service has expired.
2. Can't send cloud message?
Check if the permissions have expired, if the recipient is not authorized, and if the network connection is normal.
3. decryption failed?
Only the bound D-Key hardware can decrypt.
4. Lost your cloud storage file?
The system automatically clears cloud storage data after the rights expire for more than one month.
5. For any other issues during use, please feel free to contact our official website: <https://www.onlyownerhk.com/>

傲然技術有限公司

使用者手冊