DRONE SECURITY WHITE PAPER

Version 3.0

DJI

DJI is a global technology company known as the world's leading civilian drone manufacturer. We began operations in 2006 as a resource for remote controlled model aircraft hobbyists and pioneered the widespread adoption of ready-to-fly recreational drones. Today our solutions serve professionals, enterprises, and government agencies around the world.

DJI's innovative technology has become the preferred platform in a wide range of industries, including agriculture, construction, energy, media, and public safety. DJI's open architecture has created a marketplace for third parties to provide additional hardware payloads, software systems, and mobile apps, which enable the world's innovators to develop solutions for a variety of pursuits.

DJI Drone Security White Paper

This paper outlines key systems in our drones and the security measures DJI has implemented to bolster security, enhance privacy controls, and protect the integrity of user data. It has been updated to reflect additional security improvements and new product developments, in line with our longstanding commitment to drone safety and security.

CONTENTS

DJI Mavic 3 Pro Cine

INTRODUCTION

DJI technologies enabled the widespread adoption of ready-to-fly recreational drones, which today serve professionals, enterprises, and government agencies around the world. People choose DJI because our drones have an unparalleled mix of ease-of-use, reliability, and accessibility – and we have demonstrated a commitment to safety and security long before rules or regulations required us to do so.

Our approach to drone and data security is guided by the following core principles:

Transparency & Education

We remain open and transparent about our security and data practices and will continue to make it easier for our users to understand our data management and system security protocols through informational materials such as this security white paper, the DJI Trust Center and ongoing dialogue with our partners and dealers.

Give Users Control

No flight logs, images or videos are synced with DJI servers unless the user chooses to do so. We believe that users should have control over their data, and as such continue to expand the privacy controls built into our drones. For example, consumer drone users can easily manage their privacy preferences via their flight app's settings, and they can activate "Local Data Mode" to sever the connection between their flight app and the internet (akin to flying offline). In doing so, the app will close all data services and prevent sharing of data, even inadvertently. Enterprise drone users have additional security modes and controls including the ability to add a non-decryptable security code, wipe data at an instant, fly and update their drone completely offline or choose to use a third-party software alternative. [See Chapter: *Data Security & Privacy Controls*]

Independent Validation

We perform third-party audits regularly to validate our drone security and data privacy practices. Since 2017, international cybersecurity firms and experts, including Booz Allen Hamilton, FTI Consulting, KIVU, and more, have conducted thorough independent assessments of our products procured off-the-shelf. The findings consistently validate our alignment with industry best practices and ability to effectively protect user data. [See Chapter*: Security Audits & Certifications*]

Community Collaboration

We engage with experts, enthusiasts, and other members of the drone community to hear their suggestions on how to further strengthen our systems. We were the first drone maker to introduce a Bug Bounty Program in 2017 and the program continues to encourage security researchers to responsibly detect and report potential vulnerabilities. [See Chapter: *Bug Bounty Program*]

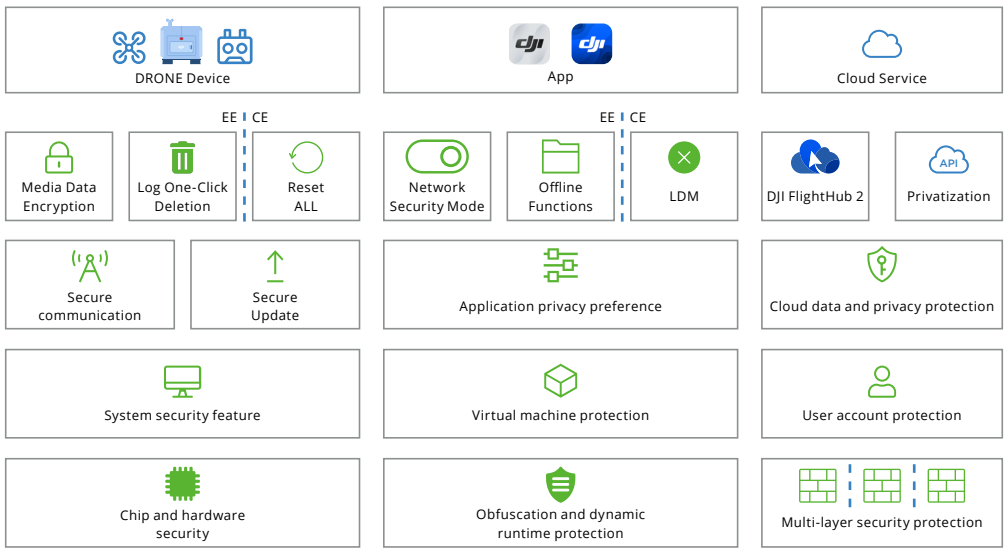
This white paper covers the following components of a DJI drone system (see Figure 1) and outlines the security and privacy protocols built into the product:

- **Device security:** Employment of Trusted Execution Environment (TEE) and FIPS-certified DJI Core Crypto Engine for strong chip and hardware security
- **Application security:** Introduces DJI's approach to securing the flight applications that operate the drones, as well as covers SDK and open source information
- **Data security & privacy controls:** Drone data shared with DJI is TLS-protected and any personal data shared by users (i.e. name or email address for account registration) is further secured with AES-256 encryption in storage. Drone data shared with DJI outside of China is housed in U.S.-based cloud servers, with the exception of Agras drone data which is stored in servers based in the U.S., Japan or Europe (depending on which region the customer is based in).
- **Communication security:** Lists the protocols and security considerations for device interconnection between the drone, its remote controller, cloud infrastructure and mobile device (where applicable)
- **Cloud security:** Outlines DJI's options for storing and managing data on different types of cloud architecture
- **Security audits & certifications:** Summarizes third-party audits conducted in the U.S. and Europe, and lists key certifications including FIPS 140-2 and ISO 27001
- **Bug Bounty Program:** Information on DJI's long standing program, bug submissions and reporting process

We hope you find this paper an informative resource that thoroughly details how DJI secures its drones across its components, as well as clarifies the types of data that are - and are not - collected.

We will continue to advocate for the development of a clear technology-based industry standard for drone security that all drone manufacturers would need to adhere to. This will improve overall drone and data security and benefit the industry as a whole.

Figure 1: System Overview



EE: Enterprise Grade Edition CE: Consumer Grade Edition

Matrice 350 RTK

DJI DRONES: CLASS LEADING PROTECTION

	Security Features	Consumer	Enterprise		Agriculture
Typical Solution		DJI Mavic 3 DJI Fly	DJI Mavic 3 Enterprise DJI Pilot 2 DJI FlightHub 2	Matrice 30 series DJI Dock DJI FlightHub 2	T60 DJI Agras
Device	Trusted Execution Environment	√	√	√	√
	Secure Boot	√	√	√	√
	Secure Update	√	√	√	√
	Device Certificate	√	√	√	√
	Log Export Encryption	√	√	√	√
	Log One-Click Deletion		√	√	
	SD Card Log Encryption	N/A	N/A	√	√
	Media Data Encryption		√	√	
	Reset All	√			
	Communication Security	√	√	√	√
	Quick Connect & Transfer	√			
App	Application Hardening	√	√	N/A	√
	Local Resource Encryption	√	√	N/A	√
	Network Security Mode	LDM mode only	√	N/A	
	Offline Firmware Update		√	N/A	
	Offline GEO Zone Unlocking		√	N/A	
	Offline Map		√	N/A	
Cloud	Secure Communication via TLS	√	√	√	√
	Multi-Layer Cloud Security Protection	√	√	√	√
	Storage Encryption for Personal Data	√	√	√	√
	Cloud API		√	√	

DJI Dock 2

DEVICE SECURITY

Chips and hardware security is the foundation of drone system security. DJI products adopt best practice technologies such as Trusted Execution Environment (TEE), secure engine and key management, Replay Protected Memory Block (RPMB)-based secure storage, secure boot, access control, system partition protection, and other technologies to ensure sufficient user protection for data, communication, and property (see Figure 2).

CHIPS AND HARDWARE SECURITY

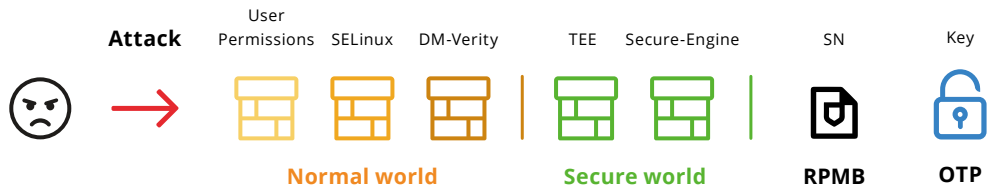
TRUSTED EXECUTION ENVIRONMENT (TEE)

Most DJI products use the ARM® Cortex®-A series processor, which supports ARM® TrustZone® technology. This is a type of Trusted Execution Environment (TEE) technology, which divides the processor into a secure world (running a secure OS and trusted applications) and a normal world (running the rich OS).

In TrustZone®, multiple security functions are implemented such as authentication and authorization, secure storage, key management, firmware decryption, and firmware verification. TrustZone® provides a secure environment based on hardware isolation to protect the confidentiality and integrity of sensitive data and the proper execution of core code.

Sensitive information such as device keys, certificates, and ID requires special protection. This sensitive information can only be accessed or modified by TrustZone® authorized trusted applications, and TrustZone® provides secure storage and integrity checking mechanisms for this information. At the same time, TrustZone® can be used to encrypt user information such as the user flight logs in the normal world to ensure the confidentiality of data.

Figure 2: Device Security Infrastructure



SECURE ENGINE AND KEY MANAGEMENT

DJI drones adopt the FIPS-certified [1] DJI Core Crypto Engine and the ARM® CryptoCell® series secure engine to ensure industry-recognized security in both hardware design and cryptographic algorithm implementation.

A secure engine operates in a secure environment of a device and can access and use keys in the One Time Program (OTP) area. The functions of the secure engine include a cryptographic algorithm acceleration module, key management module, and a true random number generator.

The root keys will be injected into the OTP to ensure confidentiality. When the keys are transmitted, a unique secret key is used for encryption for every single DJI product, and the corresponding decryption is performed in TEE. After the key is written, it can only be accessed by the secure engine, and the software cannot access it, thus ensuring the confidentiality of the key.

Meanwhile, DJI selects a compliant algorithm, key strength, and usage based on NIST recommendations (https://www.keylength.com/en/compare), as shown in the table below.

Algorithm	Strength	NIST Recommendation	Usage
AES	128 bits & 256 bits	2030	Encryption
RSA	2048 bits & 3072 bits	2030	Signature
ECC	256 bits	2030	Authentication
ECDSA	256 bits	2030	Signature
SHA	256 bits	2030	Digest

The key is the most important parameter on the device and lays the foundation of device security. Key confidentiality is closely related to functions such as data encryption, communication security, and firmware verification. Thus, DJI treats the security of the key in generation, transmission, injection, and access seriously.

The introduction of the hardware secure engine prevents the key from exposure to the normal world, ensuring the security of the key when the system is running.

[1] FIPS 140-2 Consolidated Validation Certificate (November 2022): https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/November%202022_051222_0640_signed.pdf

RPMB-BASED SECURE STORAGE

Replay Protected Memory Block (RPMB) is a secure area of the device's storage which uses a combination of signing and reply protection mechanisms to ensure that data can only be accessible to TEE and prevent unauthorized access. DJI products use RPMB to store sensitive data such as serial numbers, identity verification information, and security configurations.

DEVICE UNIQUE SERIAL NUMBER

The serial number (SN) is a unique identifier for the device and is widely used in authentication and identification. The serial number of DJI products is stored in RPMB, which effectively prevents forgery to clone the device, thereby avoiding the risk caused by the user being impersonated.

DEVICE CERTIFICATES

DJI products use X.509 format certificate, with each certificate bound to the drone’s SN. These device certificates are mainly used for device authentication and access control in services such as 4G enhanced transmission and device connection to the cloud. For a list of products with device certificates, see the Appendix.

DEBUG CHANNEL DISABLED

When DJI products are shipped from the factory, the Joint Test Action Group (JTAG), serial port, and other debugging methods are disabled, avoiding the risk of an attacker acquiring and modifying the firmware through the debug interface. This enhances the security of the firmware, and safeguards against drone compromise and user data breach.

FIRMWARE SECURITY

This section outlines the firmware security features of DJI drones.

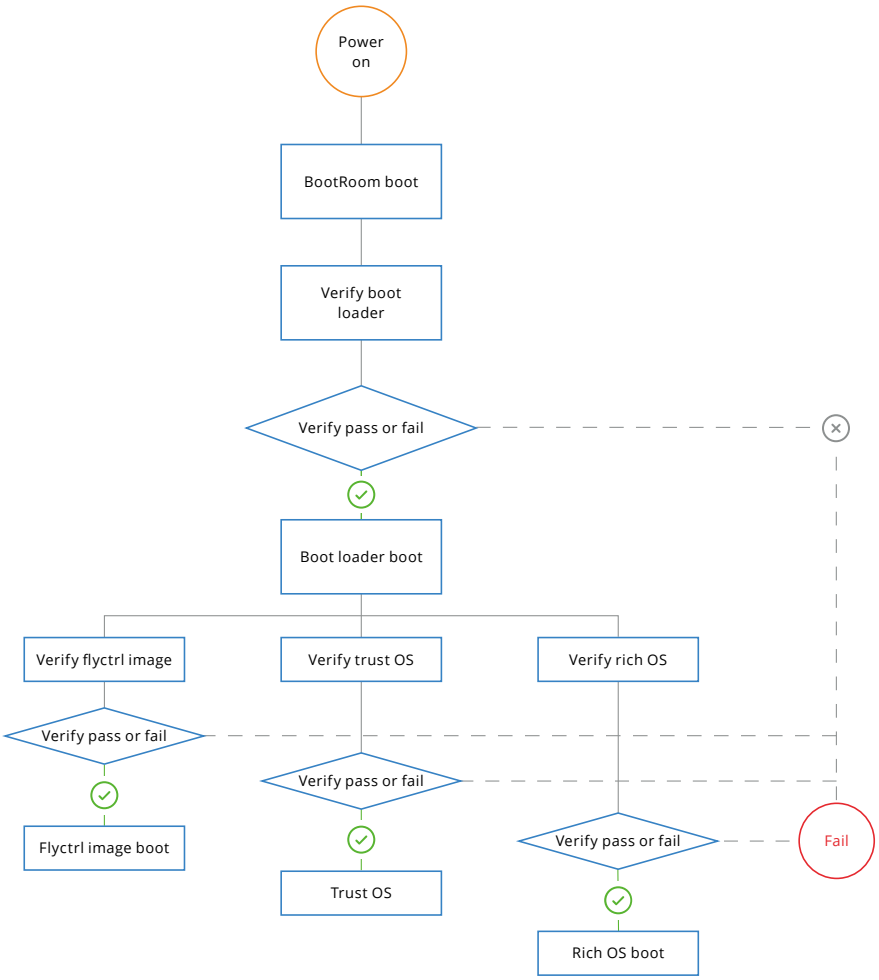
SECURE BOOT

For every step in the boot process, the firmware is encrypted and signed by DJI to ensure its confidentiality and integrity. The firmware can only run after it is verified and decrypted. The firmware includes boot loaders, kernels, secure operating systems, flight control firmware, and others.

After the device is powered on, the processor executes the BootROM code, which is stored in the on-chip read-only memory. This piece of code was burned into the chip during manufacturing and cannot be tampered with. BootROM will verify the secondary boot loader stored in the flash memory. After successful verification, the firmware will be decrypted and loaded. The boot loader verifies and loads the flight control firmware, secure operating system, and Linux kernel. The firmware of each level in the boot chain must be verified by the upper-level firmware (see Figure 3).

This secure boot chain ensures the integrity of the drone's software system. Failure in any verification step during the boot process indicates the possibility of accidental or malicious tampering, resulting in the termination of the boot process. See the Appendix for models that support secure boot (the implementation of secure boot can vary slightly from product to product).

Figure 3: Secure boot chain



DM-VERITY

DM-Verity is the technology used to protect the partition integrity in Android, employing a hash tree structure to map the data of the entire system partition. The hash tree will be signed. During the boot process, the public key is used to verify the integrity of the hash tree. Next, the applications and the software library are read from the system partition and compared against the hash tree. Any failure during verification will result in the termination of the boot process.

The system partition contains many system-level applications and software libraries, providing basic functions such as flight, navigation, image transmission, and data storage for the drone. Tampering of the system partition indicates malicious damage of the drone's basic functions, which affects the system security and data security of the drone. Therefore, DM-Verity plays a major role in ensuring the security of users' property and data. See the Appendix for models that support DM-Verity.

SE-LINUX

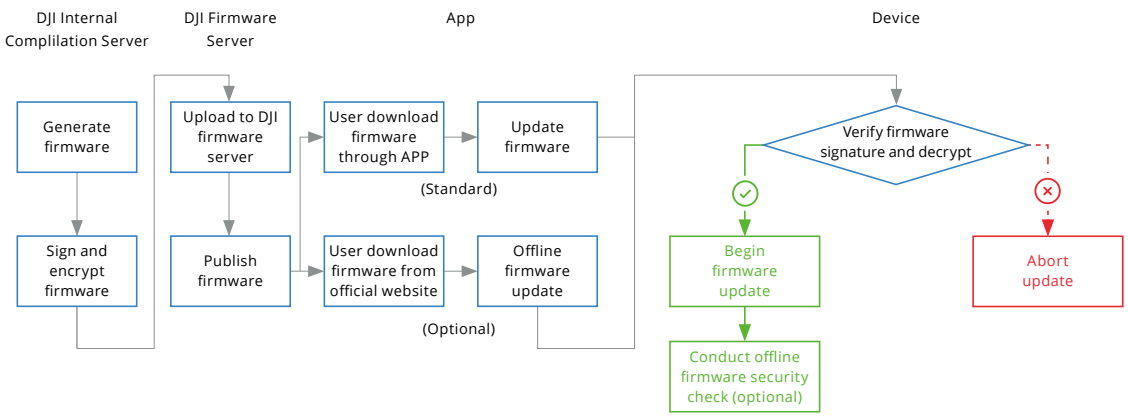
SELinux controls access to all resources such as processes, operations, and files, ensuring that there is no violation of access control policies in the system. The access control policies are stored in the root file system and protected by the device's secure boot to avoid tampering by a third party. See the Appendix for models that support SELinux.

SECURE UPDATE

DJI drones support remote system updates for new feature releases, bugs fixes, and security vulnerability patches. The update package will be signed and encrypted by DJI before it is released. The drone decrypts and verifies the signature of the update package, and begins the update once verification is complete. The update system also supports a hardware-based anti-rollback mechanism to prevent users from rolling back to vulnerable firmware versions (see Figure 4).

The secure update solution effectively prevents the installation and execution of malware on the DJI drone, ensuring the reliability of the drone software.

Figure 4: Secure Update



SYSTEM SECURITY HARDENING

Security hardening helps systems effectively identify and guard against malicious activities and improves system availability and integrity.

DJI drones adopt the following common system security hardening mechanisms:

- **Address space layout randomization:** During program code compilation, use the compilation parameter -pie -fPIE to enable address space layout randomization.
- **Stack overflow protection:** During program code compilation, use the compilation parameter -fstack-protector to enable stack overflow protection.
- **Strip debug symbols:** During program code compilation, use the strip command to delete debug symbols, thereby increasing the difficulty of reverse analysis.
- **Service and port minimization:** Based on the principle of least privilege, high-risk services and ports such as File Transfer Protocol (FTP), Secure Shell (SSH), Telnet, Hypertext Transfer Protocol (HTTP), and Android Debug Bridge (ADB) are disabled by default on DJI products to protect system security.

LOG SECURITY

LOG EXPORT ENCRYPTION

Users can export flight logs and device logs through the DJI Assistant 2 app or DJI Pilot 2. The exported logs are usually used to locate, analyze, and assess causes for system failures. Log exports are initiated by the user, and the drone encrypts them with an AES algorithm.

Since the device logs stored in the drone record the running information of the system, encrypting the exported device logs can increase the difficulty for any potential attacker to understand the system, thereby improving security. Encrypting the exported flight logs also protects the user's flight data.

LOG ONE-CLICK DELETION

Enterprise drones support the log one-click deletion function where users can tap "Clear All Device Data" in DJI Pilot 2 to delete the following logs:

- **Drone logs:** Logs stored on drones, including all flight logs and device logs.
- **Payload logs:** Logs stored in the payload module (DJI official payloads).
- **Remote controller logs:** Logs stored in the remote controller, including flight records, brief flight records of DJI Pilot 2, local media data, and flight route files.

See the Appendix for models that support this function.

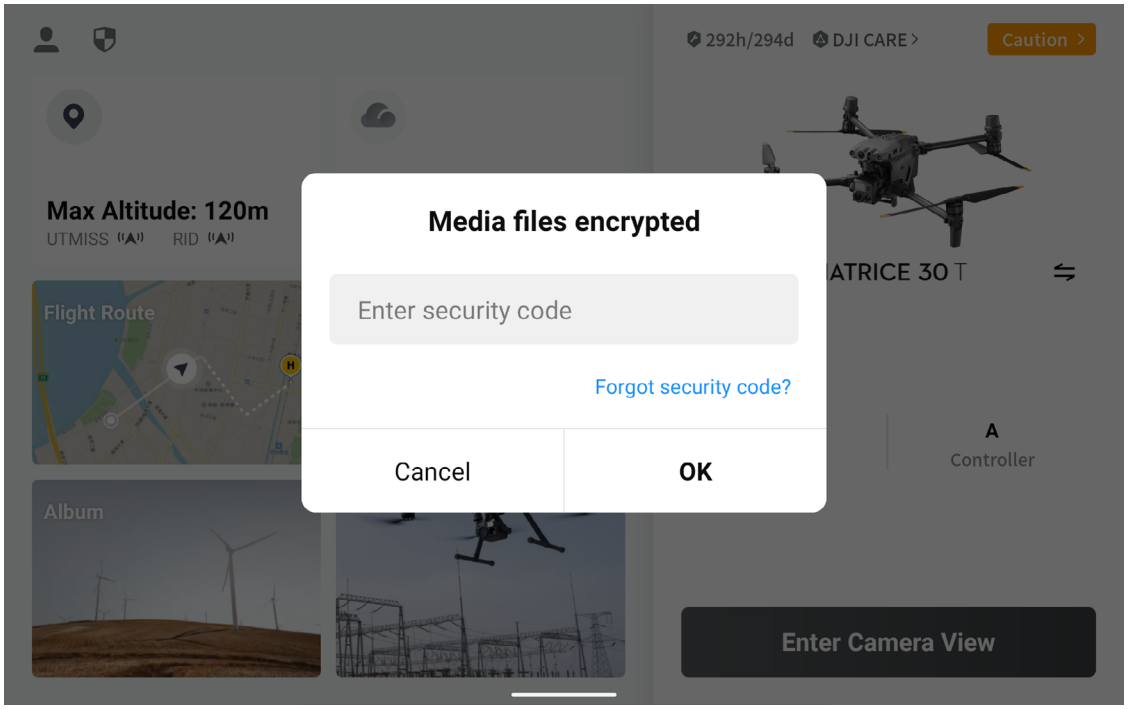
SD CARD LOG ENCRYPTION

SD cards are detachable, and logs stored on an SD card can be easily accessed. Therefore, DJI implemented AES-128 encryption for logs stored on SD cards which helps protect user information and flight data. See the Appendix for models that support this function.

MEDIA DATA ENCRYPTION

If media data encryption function is enabled, users' media data is encrypted for storage.

Figure 5: Media Data Encryption



Enterprise drone operators can encrypt their media data by simply accessing their DJI Pilot 2 app settings (“Data and Privacy” -> “Security Code”) and setting a secure code (password). The employed encryption algorithm is AES-256-XTS and the encryption key is generated randomly and protected by the secure code set by the user. DJI does not store this secure code. Thus if a user forgets the secure code, content on the storage device cannot be restored. See the Appendix for models that support this function.

Users can access encrypted media data on a drone using one of the following two methods:

- **DJI Pilot 2 app:** Enter the correct secure code in the DJI Pilot 2 app to access the media data
- **DJI Decrypt Tool on PC:** Take the storage device out of the drone and connect the storage device to a computer where DJI Decrypt Tool is installed. Enter the correct secure code in the software to view the media data.

Media data encryption can effectively prevent an unauthorized third party from accessing user's media data.

RESET ALL

The reset all function fully clears users' personal data and settings. The reset all function has two levels:

- **Reset all settings:** Reset camera, flight controller, and gimbal parameters.
- **Clear all data:** In addition to resetting all settings, this also formats storage space and clears drone logs.

Users can choose a level according to their preferences. See the Appendix for models that support this function.

PHYSICAL SECURITY

Physical security refers to security measures that protect physical assets and property from unauthorized parties, theft, damage, or loss. This is used in DJI's remote drone operations solution (Drone docks) which provides functions, such as route planning, flight task execution, and remote retrieval of real-time operation information, to adapt to user needs in scenarios such as infrastructure inspection and emergency response.

Drone docks are often deployed in sparsely populated areas. The remote drone operations solution provides CCTV video surveillance which enables dock operators to view real-time videos feeds on the cloud to ensure the safety of their devices.

DJI RC-N1

APPLICATION SECURITY

DJI application software includes DJI Fly series, DJI Pilot series, DJI Agras series, and other software which plays a central role in interacting with drones, displaying the image taken by the drone, controlling the drone, editing images, providing user registration and login, and interacting with cloud services. Therefore, the app is the main component in the drone system.

DJI applications support Android and iOS mobile platforms, as well as Windows and Mac computer systems. This chapter will introduce the DJI application hardening methods on different platforms.

As well as cover the various kinds of SDKs. Users can customize their own applications according to individual needs. These SDKs can be utilized either independently or in conjunction with one another to satisfy diversified needs.

APPLICATION HARDENING

The application runs on users' devices. As there are many computing platforms available, individual security structures vary considerably. This presents an issue where the app is running within an environment that has the potential to be insufficiently secure, creating the risk of user data theft by third-party programs. DJI has analyzed the different platforms and has provided different application hardening strategies for each platform.

ANDROID APPLICATION HARDENING

DECOMPILATION PROTECTION

By obfuscating and packing the code, attackers are not able to understand business logic by decompiling the code (communication logic, encryption logic, and drone control logic). For the most important and user-related code, the more secure virtual machine protection technology is implemented. The original executable code is converted into a secure and customized bytecode and run on the virtual machine engine, greatly increasing the difficulty of reverse attacks.

DYNAMIC LIBRARY ENCRYPTION PROTECTION

The dynamic library is developed in C/C++ language, which is less susceptible to reverse analysis. Protection for the dynamic library includes:

- Assembly code compression and encryption protection
- Dynamic library executable and linkable format (ELF) information protection
- Dynamic library encryption
- Dynamically code clearance after decryption

DYNAMIC RUNTIME PROTECTION

The dynamic defense technology provided by security hardening is based on anti-debugging protection. At the same time, it monitors key functions and links, protects Android applications at runtime by means of polling and active detection. The methods include:

- Proactively checking and protecting key processes of the system through the monitoring mechanism to prevent attackers from debugging the app;
- Performing anti-hook checks on key functions by means of polling;
- Preventing dynamic debugging and dynamic injection attacks by monitoring common debugging methods and features of injection tools;
- Replacing and hiding key module logic functions to prevent them from being hooked.

LOCAL RESOURCE PROTECTION

A data encryption mechanism is implemented in the Android file system layer, effectively protecting all file read and write operations, including flight records, shared preferences, databases, and application logs.

INTEGRITY PROTECTION

All contents of the app installation packages are cross-checked, and the verification data and the verification code are encrypted, enabling timely identification of apps as official. When an app is detected as unofficial or tampered with, the app will be prompted to quit, and malicious information such as illegal advertisements and Trojans will be prevented from harming the user.

IOS APPLICATION HARDENING

The hardware and software of iOS devices are highly integrated, with strong built-in security protection. All apps need to be reviewed by the App Store before release. When a security vulnerability occurs in the system, the iOS System can be updated in time to effectively reduce the risk of compromise. Based on the security protection of the iOS system, DJI apps have added the following protection measures:

- In the app development process, code logic is obfuscated by adding redundant sensitive words and business logic;
- In the runtime, the entries of important keys and methods are written to the global pointers by a thread, and other logic obtains the sensitive data or call critical methods via global points, making it challenging to perform reverse analysis;
- Sensitive commands protection is implemented in the underlying modules that communicate with the drone;
- White-box cryptography is applied to the keys and login credentials used in the app (e.g., user center, flight limit, flight records).

PC APPLICATION HARDENING

DJI implements the hardening of computer applications mainly using third-party software. Like the hardening of a mobile device app, the hardening of a computer application consists of shelling, anti-debugging, and similar technologies:

- Packing binary files and adding anti-debugging features to increase reverse engineering difficulty;
- Signing binary files to avoid third-party distributing tampered applications;
- Obfuscating key and passwords associated with aircraft interactions and implementing key code virtual machine protection, etc., to avoid leaking sensitive information.

The front end code and important data are protected in the following ways:

- The front end is obfuscated and encrypted to prevent source code from being leaked and exploited;
- Key credential parameters are encrypted and sensitive key data is pulled from the client instead of being stored locally to the front end to reduce the risk of sensitive key information being captured and utilized;
- WebSockets over SSL/TLS (WSS) and HTTPS are enforced between clients and servers, avoiding man-in-the-middle attack and network sniffers.

DJI SDK SECURITY

DJI produces several SDKs including Mobile SDK, Onboard SDK, Payload SDK, and DJI Edge SDK. This section will first briefly explain the basic purpose of each SDK, then describe the data types, internet connections, and open source information involved in each SDK in detail.

DJI MOBILE SDK

By using the Mobile SDK (MSDK), developers can build iOS and Android applications that interface wirelessly with drones. The MSDK creates a customized mobile app to unlock the potential of the aerial platform that helps realize developers' innovations.

When developers use DJI MSDK to develop applications, or users use applications developed by DJI MSDK, the following functions will trigger network interactions:

Function	Description	Optional
SDK Registration and Activation	When developing an app via the MSDK for the first time, or when the user runs an app developed by the MSDK for the first time, the MSDK will connect to a DJI server for activation. In this process, MSDK will only sync system information (such as operational platform version, SDK version, etc.), no user personal information will be uploaded.	No
Firmware Update Check	When the user connects a device to an app developed by the MSDK, the latest firmware information will be pulled by the MSDK from the server and the user will be prompted to update.	Yes
GEO Zone Database Update	When the user connects a device to an app developed by the MSDK, the latest GEO Zone database will be pulled by the MSDK from the server to help the user fly in accordance with local laws and regulations.	Yes
Country Code	The current user's country code will be obtained. This information will mainly be used to set up the remote controller's frequency band.	Yes
User Experience Information	When the user uses an app developed by the MSDK, the MSDK will record API calling status to optimize and improve functionality. Recorded statistics only include API calling status and do not contain any personal information. If the user turns off user experience information in the privacy settings of the app, then this data will not be uploaded.	Yes
DJI User Center	(Optional) When the developer calls the DJI User Center related API in the MSDK, communication with the DJI User Center server will be established.	Yes
Third-Party Network RTK Service	(Optional) When the developer calls the API in the MSDK that interacts with a third-party network RTK service, communication with the third-party network RTK service will be established.	Yes

Considering some agencies require high standards for privacy, Local Data Mode (LDM) is available in DJI MSDK. Developers can equip apps with LDM mode. When LDM mode is enabled, network links will be cut off. Please note, for both normal apps and LDM-equipped apps, apps must complete the SDK registration and activation. Activation only needs to be completed when using the app for the first time. For LDM-equipped apps, after the activation is completed, users can enable the LDM to cut off all network links of the app.

DJI ONBOARD SDK

DJI Onboard SDK (OSDK) helps to build automated drone applications for supported DJI enterprise grade aerial devices as well as the A3 and N3 Flight controllers.

While OSDK has been integrated into the DJI Payload SDK offering, we maintain the following information as there are some operators who may continue to use the original OSDK function.

When developing applications based on the OSDK, developers need to apply for an ID and its corresponding key on the DJI Developer Website (developer.dji.com/onboard-sdk/). First time users use the applications developed by the OSDK, they need to enter the ID and the key applied by the developer for activation. A network connection is required when activating for the first time. After successful activation, the flight control module will record the ID and subsequent activation can be performed offline until the ID is erased by the flight control module.

When using the flight control API through the OSDK, relevant flight commands and flight statuses will be recorded by the flight logs. During the activation process, the flight control module will also record the user ID into the flight logs. The user can actively export the flight logs using DJI Assistant 2, and the exported flight logs will be encrypted.

Part of the DJI OSDK code uses open source. Refer to the following links for more information:

– github.com/dji-sdk/Onboard-SDK

– github.com/dji-sdk/Onboard-SDK-ROS

– github.com/dji-sdk/Onboard-SDK-Resources

DJI PAYLOAD SDK

DJI Payload SDK (PSDK) enables third-party manufacturers to develop application- specified payloads that seamlessly integrate with DJI flight platform. Using the PSDK, payloads can access the battery, wireless communication link, drone status and status information (GNSS, attitude, time and date), as well as various APIs that are closely integrated with DJI MSDK, DJI Pilot 2, and DJI OSDK.

Developers first need to register a DJI PSDK enterprise account, which is used to bind the application developed by DJI PSDK with the DJI SKYPORT adapter. After the binding is completed and the third-party payload is connected, communication between the payload and the aircraft will be transmitted through the adapter.

A log is automatically generated during the use of the PSDK, mainly recording commands and errors related to PSDK functions. The log does not include user personal data, and can be exported by users according to their needs, while not being uploaded automatically.

A log is automatically generated during the use of SKYPORT, mainly recording information such as CPU usage, interface bandwidth, device type, power supply voltage, and activation status. Users can manually export logs according to their own needs while not be uploading automatically.

During the use of PSDK, the following functions may trigger network interaction:

Function	Description	Optional
PSDK binding with SKYPORT	When developers develop an app via the PSDK, the app needs to be bound with DJI SKYPORT. During the process, the SKYPORT adapter will verify information such as user account, product name, and product ID with the server through DJI Assistant 2.	No
PSDK unbinding with SKYPORT	PSDK applications can also be unbound from DJI SKYPORT. During the process, the SKYPORT adapter will also verify information such as user account, product name, and product ID with server through DJI Assistant 2.	No
User experience data	This data mainly records the usage time of each PSDK function, version information, developer information, GNSS location information after reducing accuracy (reduce accuracy to a 5-10 km radius), etc. Users can turn off the authorization of user experience data upload through the “Privacy Settings” tab in the app or DJI Assistant 2.	Yes

DJI EDGE SDK

Developers can use DJI Edge SDK (ESDK) to develop edge computing applications for the remote drone operations solution (Drone docks). Third-party edge computing boxes developed based on ESDK can interact with drone docks and cloud APIs, and can access drone liveview data and media files. This way, different edge computing devices can be developed to meet various requirements in industries, such as image preprocessing, image compression, AI-based object recognition, and AI-based defect detection.

To ensure data security on edge computing nodes, an RSA public-private key pair will be generated when the edge computing box is deployed. The public key is stored in the secure area of the drone docks, whereas the private key is protected by the edge computing box. The public-private key pair enables mutual authentication and communication encryption between the drone docks and the edge computing box.

The following table describes the types of data that the DJI Pilot 2 app collects when the app is used to deploy the edge computing box:

Function	Description	Optional
ESDK-based Dock Binding Data	When developers develop ESDK-based apps, they use the DJI Pilot 2 app to bind the edge computing box with DJI Dock. In the binding process, information such as the product name, product ID, Dock SN (de-identified), and edge computing box SN (de-identifed) will be recorded. Users can disable the upload of data generated in the binding process through Privacy Settings in the app or DJI Assistant 2.	Yes
User experience data	The data mainly includes the usage time of each ESDK function, version information, and developer information. Users can disable the upload of user experience data through Privacy Settings in the app or DJI Assistant 2.	Yes

DJI RC Pro

DATA SECURITY & PRIVACY CONTROLS

This chapter outlines the different types of data that can be collected, processed and stored by a drone. This chapter will also highlight other types of data that DJI may collect (for example, to fulfill a customer order on the DJI Store, or provide after sales and repair services), as well as the security protocols and privacy controls that are built into DJI drones to help protect the integrity and privacy of the user and their data.

TYPES OF DRONE DATA

Data is generated, processed, and stored during the use of the drone. The specific data types and detailed descriptions are as follows:

Data type	Description	Storage location	Usage
Flight logs	Sensor data, GNSS information, and user control data during flight	Onboard storage or SD card	User can export logs by using related applications such as DJI Assistant 2. The onboard storage log will be encrypted by the export process on the drone while SD card stored log will be encrypted during log storage process.
Live flight status	Environmental information and real-time information of the drone during flight, such as current altitude, latitude and longitude, power voltage, etc..	User's mobile device or remote controller	When a drone is in use, the drone transmits its encrypted data to the user's mobile device. The data will not be synchronized to the cloud without user authorization.

Device logs	Device logs is generated during the operation of the drone to locate and solve a system bug, such as crash stacks, error and warning message.	Onboard storage or SD card	User can export logs by using related applications such as DJI Assistant 2. The onboard storage log will be encrypted by the export process on the drone while SD card stored log will be encrypted during log storage process.
Media data	Photos or videos taken by the user	Onboard storage or SD card	If media data encryption function is enabled, a secure code is required to access media data.
Update package	Drone system firmware	Onboard storage	The firmware is encrypted and signed by DJI and transmitted to the drone via the app or DJI Assistant 2.
GEO Zone Database	Specific flight area which include Restricted Zones, Authorization Zones, Warning Zones, Enhanced Warning Zones, and Altitude Zones	Onboard storage	When the user triggers a GEO Zone Database update, the database is transmitted from the app to the drone. The GEO Zone database is protected using a combination of encryption and signing.
GEO Zone unlocking data	Data required for GEO Zone unlocking function such as unlock license.	Onboard storage	When the user initiates GEO Zone unlocking, GEO Zone unlocking data is transmitted from the app to the drone. GEO Zone unlocking data is protected using a combination of encryption and signing.

DATA WALKTHROUGH & USER PRIVACY CONTROLS

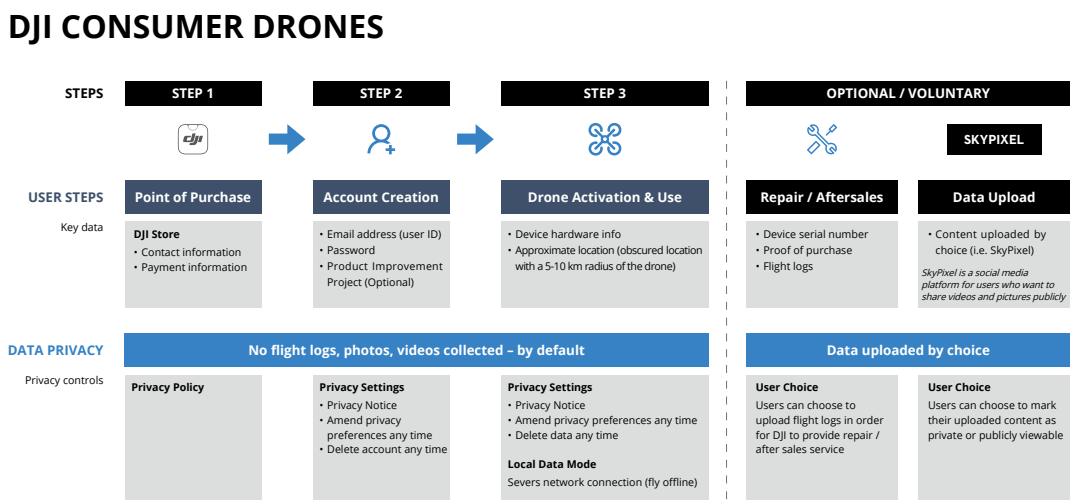
This section outlines the process of setting up a drone for the first time, highlighting the relevant data requests and available privacy controls for the user at each stage.

DJI FLY

The DJI Fly applications interact directly with consumer drone systems. They carry out drone system communication, interactive control, real-time live display, user information management, image editing, and content sharing.

The flight app communicates clearly to users what data can be collected (including what is optional) from point of purchase to drone activation. No flight logs, images or videos are shared with DJI without user consent (see Figure 6).

Figure 6: Consumer drone data walkthrough



When launching the app for the first time with a new drone, the app will prompt the user to confirm which items of information will be collected. The user can change their preferences at any time by simply toggling the “on” or “off” authorizations of the specified item in the “Privacy Settings” tab of the “Settings” page of the application at any time.

The following table lists the information and specific content that the app may collect:

User info	Content and usage	User authorization time	Opt-Out (If LDM Off)
Approximate Location	This information is an obscured location (with a radius of 5-10km as the obfuscation) of your DJI device and mobile device. This information is used to provide the server with the approximate location of the user to request and refresh the latest GEO zones.	When the app is started for the first time, a pop-up window will appear for user authorization.	No
DJI Device Hardware Information	This information includes the product serial number of the DJI device you paired with the app and the serial number of the flight controller, gimbal, camera, and battery. This information is used for device activation and device-related requests such as DJI Care.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
DJI Device GNSS Information	This information is the location of the DJI device you paired with this app. This information will be provided to the third party map framework to display the real-time location of your device on the map. The map interface will appear in the function of finding the aircraft, the map function of the flight interface, and the function of location album.	When the app is started for the first time, a pop-up window will appear for user authorization	Yes
User Behavior Logs	Including de-identified product usage data such as usage frequency. This information is used for statistical analysis to improve user experience.	In the pop-up window that appears when the app is started for the first time, select DJI Product Improvement Project, and then select Contributor. This is optional.	Yes

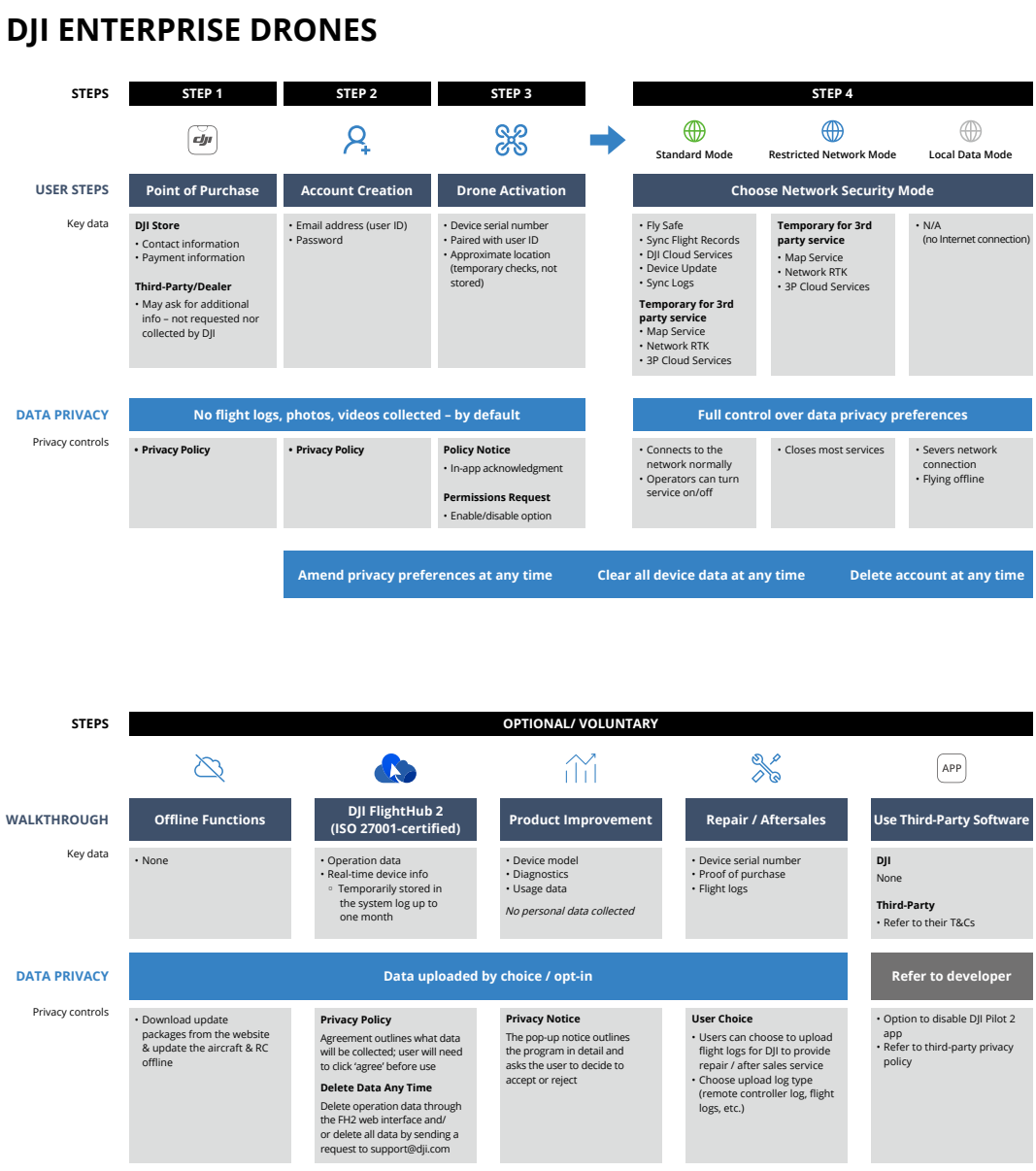
Flight Records	Flight data generated by the app and flight system in real time including: - Flight status such as position trajectory & aircraft attitude information - Device status such as camera & gimbal status, battery status, remote control & image transmission status, visual & sensory system status - Flight related information such as route, mileage, location and time Users can synchronize historical flight data to the cloud and between different devices for backups	When the user chooses to upload	Yes
Videos/ Photos	Photos/videos taken by users for sharing	When the user chooses to upload	Yes

Any data communicated between the DJI Fly series app and the cloud server are encapsulated and transmitted through the HTTPS protocol to ensure its security. Users can also choose to enable the Local Data Mode (LDM) function - which severs the communication between the app and the server - at any time.

DJI PILOT 2

DJI Pilot 2 is an application that interacts directly with enterprise drone systems. It carries out drone system communication, interactive control, real-time display image transmission, user information management, and intelligent tasks. It provides customers with various software features for industrial drone applications. In addition to inheriting the security features of consumer applications, DJI Pilot 2 expands security and privacy functions to meet enterprise user needs.

Figure 7: Enterprise drone data walkthrough



Similar to the consumer flight apps, users are able to instruct DJI Pilot 2 on what data it can and cannot collect (see table below). When DJI Pilot 2 loads on a new device for the first time, a pop-up window will appear to prompt the user to confirm what information can be collected. Users can amend their preferences at any time by simply enabling or disabling authorization for specific items via the Data and Privacy Settings tab of the Settings screen of the app.

Network Service	Description	Standard Mode	Restricted Network Mode	Local Data Mode
Map	Maptiler map access Aircraft or remote control position on the map	Optional	Optional	Disabled
Third-Party Livestreaming	GB/T 28181 RTMP	Optional	Optional	Disabled
Device Update	Firmware update notification, push, or installation	Optional	Disabled	Disabled
Activation	Drone and payload activation	Enabled	Disabled	Disabled
Flight Academy	Instructions for using the device	Enabled	Disabled	Disabled
DJI Care	Service plan for DJI enterprise drones	Enabled	Disabled	Disabled
Enhanced Transmission	4G enhanced transmission [2]	Enabled	Disabled	Disabled
FlySafe	GEO Zone database update Unlock license download	Enabled	Disabled	Disabled
Sync Logs	Sync DJI device logs to DJI servers	Optional	Disabled	Disabled

[2] At the time of writing, 4G enhanced transmission is only supported in the Chinese Mainland. Please visit page 44 for more information

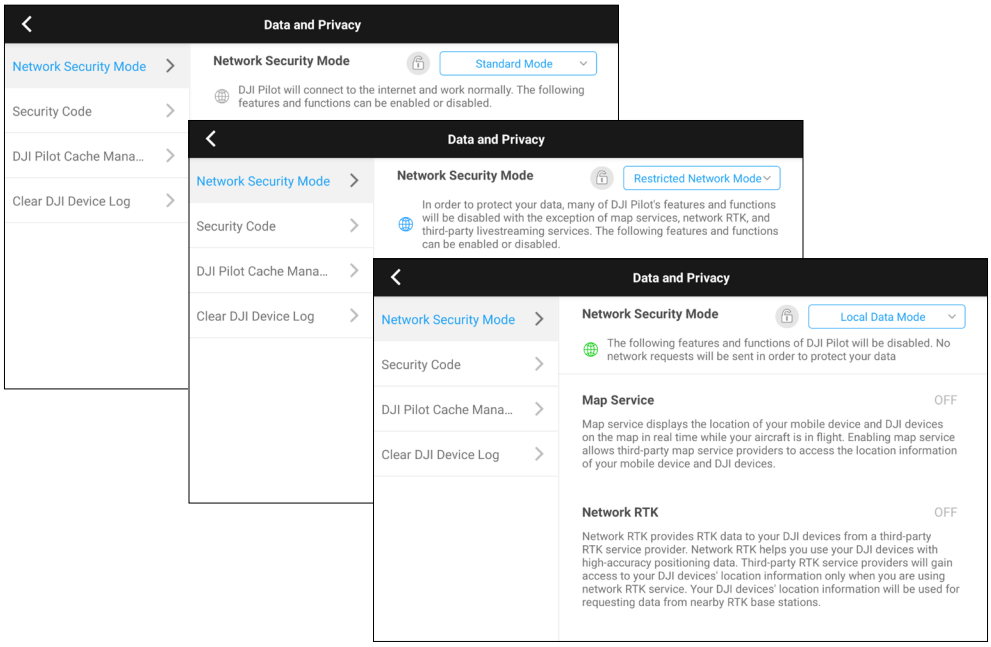
Sync Flight Records	Flight records synchronization aims to provide users with a convenient tool for synchronizing flight records of DJI devices. The app synchronizes information to the DJI server only when users actively upload flight records. The following information will be synchronized: - Account information - Device serial number (SN) - location information - Flight information such as flight path and flight time and speed - Device status such as sensor data	Optional	Disabled	Disabled
DJI FlightHub 2	Connection to DJI FlightHub 2, supporting functions such as live streaming, device management, device status display, point line and area, cloud-based mapping, media file libraries, and flight route libraries	Optional	Disabled	Disabled
DJI Product Improvement Project	Collecting and sending de-identified device diagnostics and usage data	Optional	Disabled	Disabled

DJI Pilot 2 provides users with enhanced controls, including network security mode, media data encryption, log one-click deletion, offline firmware update, offline GEO Zone unlocking, and offline map.

NETWORK SECURITY MODES

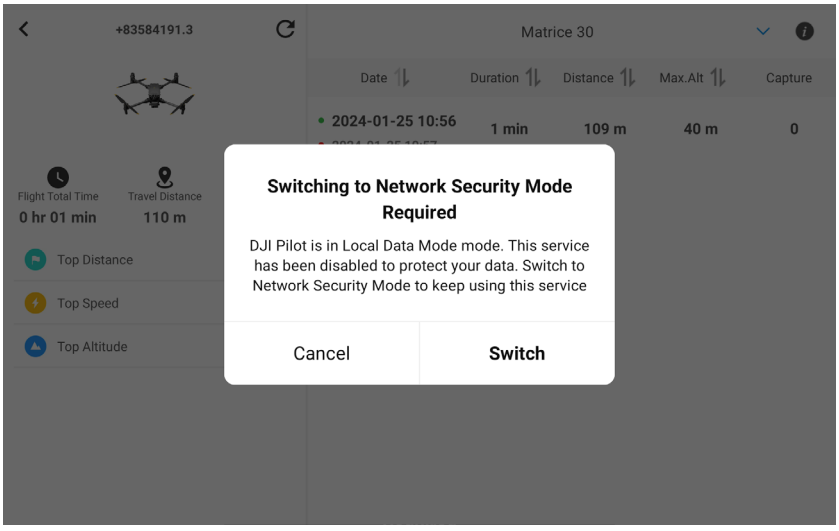
Users can choose from a range of network security modes:

Figure 8: Network Security Modes



- **Standard Mode:** App will connect to the network and you can turn a service on or off according to your needs.
- **Restricted Network Mode:** App will close most data services. It will still support maps, network RTK and custom livestream functions.
- **Local Data Mode (LDM):** App will close all data services and will not send any network requests. While in Local Data Mode, it is impossible for a user to sync their data even accidentally with DJI. If they attempt to do so, they will receive the following message:

Figure 9: Network Security Mode Alert



OFFLINE FUNCTIONS

DJI Pilot 2 provides various offline functions where the remote controller does not need to be connected to the internet:

- **Offline maps & offline firmware updates:** Users can import offline map data from MapTiler through the DJI Pilot 2 app. Download the latest map and/or firmware from the official website, add it to an SD card and update the drone while remaining offline. Users can download firmware and conduct a security check before uploading the firmware update offline to their drones via an SD card
- **Offline GEO Zone unlocking:** DJI Pilot 2 provides the offline GEO Zone unlocking function to enterprise operators. See the appendix for models that support this function. To use the function, perform the following steps:
  - After the unlocking application is approved, visit the FlySafe official website to download the required files for unlocking.
  - Import the files to an SD card, and insert the SD card into the remote controller. Power on the drone and the remote controller to link the drone with the remote controller.
  - Start the DJI Pilot 2 app. In the GEO Zone Unlocking module, select the files in the SD card to unlock the drone.

ADDITIONAL DATA PRIVACY CONTROLS

In addition to the settings that each user toggles immediately upon app launch, there are additional layers of security DJI users may wish to enable:

- **Media Data Encryption:** As stated in an earlier section, users are able to protect their data locally by requiring a secure code to be entered before anyone can access content saved locally on the SD card, such as photos or video content. This effectively prevents a third party from accessing the media data on a storage device without permissions when the device is lost. This code is also not accessible by DJI.
- **Cache Management:** Users are able to clear their cache at any time. In addition, DJI allows users to select specific cache clearing options. This allows users to retain certain cached data if it is needed for a specific mission while still removing other cached data.
- **Log One-Click Deletion:** As described in the "LOG SECURITY" section, users can tap Clear All Device Data in DJI Pilot 2 to delete the drone logs, payload logs, and remote controller logs.

THIRD-PARTY SOFTWARE ALTERNATIVES

Users may prefer to use a range of alternative third-party software compatible with DJI devices. These third-party options can be downloaded onto the iPad or Android device and used as a separate app, without any interactions with DJI Pilot 2.

It is also possible to download third-party software and disable the DJI Pilot 2 altogether.

DJI AGRAS

DJI Agras is an app that directly interacts with agricultural drone systems. It provides users with abundant functions for using drones in the agricultural field, such as drone system communication, interactive control, real-time display of transmitted videos, user information management, and plant protection operation management.

When DJI Agras is connected to a new device for the first time, a pop-up window will appear to prompt the user to confirm whether each listed piece of information is authorized to be collected. During subsequent use, users can enable or disable authorization for specific items at any time on the Privacy Settings tab of the General Settings screen of the app.

The following table describes the information that may be collected by the app and the details of the information.

User Info	Content and Usage	User Authorization	Opt-Out
Approximate Location	This information is an obscured location (with a radius of 5-10 km as the obfuscation) of the DJI device. This information is used for maintaining normal functions in GEO zones.	When the app is started for the first time, a pop-up window will appear for user authorization	No
DJI Device GNSS Information	This information is the geolocation of the DJI device. This information is used for third-party map positioning. If permissions on this type of information are revoked, the task execution, real-time monitoring, and operation area statistics functions are also disabled.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
DJI Device Hardware information	This information is the SN of the DJI device that is linked with the app, including the SNs of the flight controller, gimbal, camera, and battery. This information is used for purposes such as device activation, login and registration, and API requests.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes

Real-Time Flight Data	This information includes real-time location data, account, flight status, and device status, enabling real-time viewing of the drone positions and quality supervision on the DJI Agras Management Platform.	When the app is started for the first time, a pop-up window will appear for user authorization	Yes
Flight Records	This information is the detailed flight data generated in real time, which allows users to view operation data playbacks and statistics.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
User Behavior Logs	If users opt into the Product Improvement Plan, the App will collect de-identified data including DJI device info: product models, firmware versions, and logs about device status and usage. The information is used to analyze product usage and status to improve product experience. Diagnostic and usage data: including device property data and product usage data. The data is used to analyze and improve product experience.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
DJI Device Logs	This information refers to the operation log files generated by the DJI device. The log files are used for product issue analysis in after-sales services.	When the user actively uploads	Yes

All communication data between DJI Agras and the cloud server is encapsulated and transmitted by using the HTTPS protocol to ensure communication security.

Drone data shared with DJI outside of China is housed in U.S.-based cloud servers, with the exception of Agras drone data which is stored in servers based in the U.S., Japan or Europe (depending on which region the customer is based in).

DJI ASSISTANT 2

The DJI Assistant 2 series software is a client software that interacts with DJI drones on Windows and Mac computer platforms. Key functions include firmware update, log export, camera calibration, flight simulator, and DJI device parameter settings.

The communication between DJI Assistant 2 and the DJI device uses the USB virtual serial port, while the communication between it and the server uses the HTTPS protocol. The communication data between different processes of the application is AES encrypted, which enhances the security of data communication.

When using the DJI Assistant 2 software, the following information will be obtained to ensure that all functions are working properly. See table below for more information.

When using the software for the first time, a prompt will appear to confirm data access authorization for the software. After using it for the first time, the user can change the authorization settings at any time in the Settings page at the top right of the software.

User Info	Content and Usage	User Authorization Time	Opt-Out
DJI Device Serial Number	This information refers to the SN of the DJI device linked to the app, and is used for product improvement. [3]	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
Payload SDK Information	This information includes product IDs and the license information, and is used by Payload Software Development Kit (PSDK) developers to collect tracking data for product improvement. [4]	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
Onboard SDK Information	This information mainly includes the app ID, and is used by Onboard Software Development Kit (OSDK) developers to collect tracking data. [5]	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes
User Experience Information	This information is used in the product improvement project and will prompt the user to choose whether to participate after using it for the first time. The information includes the user's preferences for the application UI interface and drone operation, and helps DJI improve products and services by automatically sending diagnostic and usage data every day. The information recorded is de-identified.	When the app is started for the first time, a pop-up window will appear for user authorization.	Yes

[3] This will not be collected from DJI Assistant 2 upon updating to v2.1.21 (consumer series) and V2.1.13 (enterprise series)

[4] Ibid

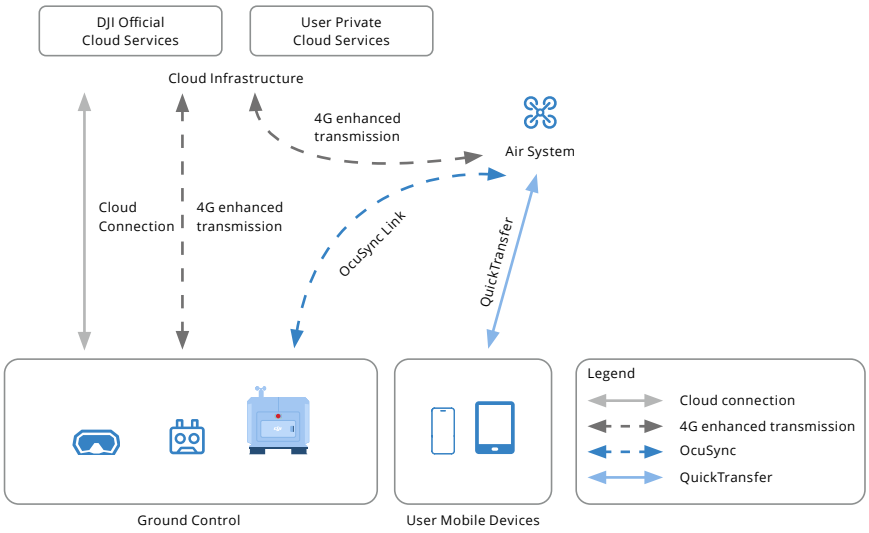
[5] Ibid

Matrice 350 RTK + DJI RC Plus

COMMUNICATION SECURITY

DJI provides a secure environment for device interconnection to protect data from illegal access, tampering, and corruption during transmission. There are four primary systems involved in the DJI device interconnection architecture (see Figure 10):

Figure 10: DJI Device Interconnection Architecture



1. **Air system:** Consists of DJI drone products which can establish connections to ground control devices, user mobile devices, and cloud infrastructure.

2. **Ground control:** Controls the air system and receives an encoded stream of data from the air system. Currently, DJI has the following ground control devices:
   - **Remote controllers:** Supports control over air system devices including flight control, payload control, and transmission control.
   - **DJI Goggles:** Provides an immersive flight experience. With the goggles receiving drone liveview data and a motion controller, users can truly experience a first-person perspective.
   - **Remote drone operations solution:** Serves as the supporting infrastructure DJI launched for drones, providing functions such as drone takeoff and landing, charging, task distribution, and flight control to adapt to user needs in scenarios such as infrastructure inspection and emergency response.

3. **Cloud infrastructure:** Provides drones with services such as media data sharing, data storage, and remote management, playing an important role in supporting modern drone management.
   - **DJI official cloud services:** The infrastructure which DJI products and services rely on, including DJI Service, SkyPixel, and DJI FlightHub 2.
   - **User private cloud services:** Third-party cloud services that can be accessed by certain DJI products to enhance data confidentiality for enterprise users.

4. **User mobile devices:** Certain DJI products can connect to user mobile devices such as mobile phones and tablets to allow users to quickly download media data from their drones.

There are three main types of links in DJI device interconnection:

- **Transmission link:** Used for transmitting control and payload data between the air system and the ground control. DJI currently supports two types of transmission links: OcuSync links and 4G enhanced transmission links.
- **Cloud connection link:** Used for communication between the air system, the ground control, and the cloud infrastructure. DJI products currently support connection to DJI official cloud services as well as user private cloud services.
- **QuickTransfer link:** Used for communication between user mobile devices and the air system, allowing quick access to media data on drones and improving user experience. Currently, QuickTransfer links are used mainly on consumer drones.

OCUSYNC COMMUNICATION SECURITY

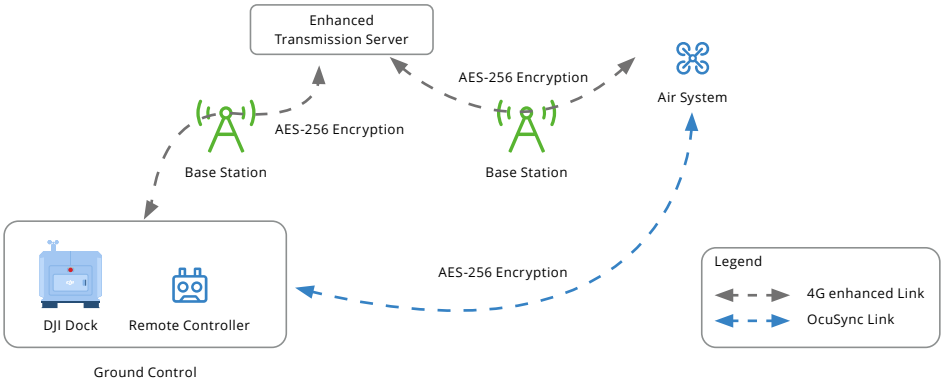
OcuSync is a proprietary DJI protocol with built-in security features. The OcuSync communication solution is widely used in DJI drone products. The link is encrypted by the AES-256 algorithm. Each time a device powers on, a random and different session key is generated for accessing the encrypted data, ensuring a unique encryption key for each use.

The OcuSync communication mechanism effectively protects users against communication hijacking, man-in-the-middle attacks, replay attacks, and communication eavesdropping by technologies such as secure key negotiation and communication encryption.

4G ENHANCED TRANSMISSION LINK SECURITY

DJI products can support 4G enhanced transmission (see Figure 11). Provided that 4G communication is enabled, when the air system and the ground control are linking, an OcuSync link is established first for data exchange between the air system and the ground control. After data exchange is complete, a 4G link can be established. When the 4G link is established, the air system and the ground control perform mutual authentication based on the previously exchanged data to avoid unauthorized access or incorrect connections. The 4G enhanced transmission link uses the AES-256 algorithm to encrypt data. A random and different session key is generated for accessing the encrypted data, ensuring a unique encryption key for each use. The exchange of session keys is encrypted using keys derived from the linking information between the air system and the ground control.

Figure 11: Link Composition of 4G Enhanced Transmission



When 4G links are used for communication, the air system and the ground control communicate through the enhanced transmission server. When a device connects to the enhanced transmission server, mutual authentication is required. Each air system device has its unique device certificate and private key. The private key is encrypted and will be used only in TrustZone®. Two-way authentication can effectively prevent unauthorized devices from accessing the enhanced transmission server to avoid further unauthorized access to the air system.

The 4G enhanced communication solution effectively protects users against near-field and remote communication hijacking, man-in-the-middle attacks, replay attacks, and communication eavesdropping through secure key negotiation, mutual authentication between devices and communication encryption technologies, and security protection for private keys in the device side using TrustZone® technology.

In the 4G enhanced transmission solution, session keys are saved and used only on air system devices and ground control devices, and the enhanced transmission server cannot temper or decrypt the transmitted data, thus ensuring the security of user data. In addition, DJI provides a 4G private deployment service for users who have higher requirements for data security. Users can deploy a private enhanced transmission service to ensure the security of their data. Click developer.dji.com to learn more.

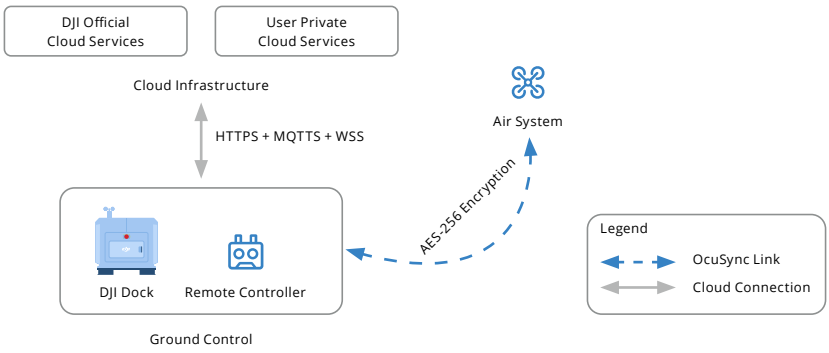
At the time of writing, 4G enhanced transmission is only supported in the Chinese Mainland. It will be available internationally [6] in 2024.

CLOUD CONNECTION LINK SECURITY

DJI OFFICIAL CLOUD SERVICES

DJI official cloud services for drone products include DJI Service, SkyPixel, and DJI FlightHub 2. Devices can establish cloud connection links to access the cloud infrastructure and use the services provided by DJI such as media data sharing and data storage. The ground control serves as a relay and connects to both the air system and the cloud infrastructure, forming a complete cloud connection link (see Figure 12).

Figure 12: Cloud Connection Link



During the process of establishing a cloud connection link, the ground control first connects to the air system through an OcuSync link and then establishes a Transport Layer Security (TLS) link to the cloud infrastructure. To ensure the security of the cloud connection link, the TLS link uses TLS 1.2 or later. After the previous steps are complete, the air system device calculates an authentication token in the trusted zone and uploads the token to the cloud. This authentication token is bound to the air system device SN. The cloud uses the authentication token to verify the identity of the air system device. After the identity verification is successful, links are established between the air system, the ground control, and the cloud infrastructure.

[6] The list of countries will be published on DJI's website

With TLS-based mutual authentication, OcuSync link encryption, and authentication token-based security mechanism, cloud connection links can defend against common attacks such as communication hijacking, man-in-the-middle attacks, replay attacks, and communication eavesdropping.

USER PRIVATE CLOUD SERVICES

Third-party vendors can develop cloud services similar to DJI FlightHub 2 as instructed in the Cloud API documentation and have seamless interaction with DJI products. Click developer.dji.com to learn more about private deployment.

This allows more flexible cloud infrastructure construction for users. See the appendix for models that support integration with private clouds. Such links to private cloud services have the same security level as links to DJI official cloud services, both adopting TSL 1.2 or later.

QUICKTRANSFER SECURITY

Consumer drones and their corresponding DJI Fly apps support QuickTransfer. They enable users to quickly download media files from the drone after they are captured. When connecting for the first time, the DJI Fly app scans nearby DJI devices through the Bluetooth of the mobile phone.

After discovering the DJI device and tapping to connect to the device, authentication will be initiated on the corresponding device. The user needs to manually press the corresponding button on the drone to complete the authentication. After the authentication is completed, the mobile phone will obtain the Wi-Fi SSID and password of the drone through Bluetooth, and the UUID of the mobile phone will be recorded in the whitelist of the drone. Next, the mobile phone will connect to the device via Wi-Fi and the user can download the media files on the device. When connecting the next time, the locally cached Wi-Fi SSID and password can be used to quickly connect to the drone.

The drone will verify whether the mobile phone UUID is in the whitelist to prevent unauthorized access. If the drone and the mobile phone have been connected through the remote controller before, the UUID of the mobile phone will also be added to the drone's whitelist for quick access the following time. Wi-Fi and Bluetooth connections are only used to quickly export media data and will not be used to control the aircraft. See the Appendix for models that support this function.

DJI Inspire 3

CLOUD SECURITY

DJI provides users with a variety of cloud services to enrich product features. This section explains how DJI provides robust security for cloud services and cloud storage.

USER ACCOUNT SECURITY

All DJI applications deploy an integrated account system, including online store, forum, drone activation, and DJI Care services. Other applications perform account operation via embedded web pages, OAuth, and relevant API.

DJI currently adopts the following methods to protect the security of user accounts:

- **Account Center Risk Management System:** This system detects malicious behaviors, including abnormal login, collision attack, and malicious registration. For example, image verification will be required if an account is logged in at a location which is not included on the commonly used location list.
- **Traffic Limit:** To prevent sites from receiving a high volume of malicious requests, the user center sets the traffic limits and blacklists any malicious IP.
- **User Information Encryption:** Encrypts user's key information in the database and encrypts network traffics with HTTPS.

SERVER SECURITY

This section demonstrates the server security of DJI from four aspects: host security, internet application security, operation security, business continuity and disaster recovery.

HOST SECURITY

DJI internet services are primarily deployed onto the cloud, so the security of services is closely linked to cloud providers. DJI employs Amazon AWS and Alibaba Cloud as cloud service providers, which are known for their security qualifications and high reliability [7]. AWS has certifications of compliance with ISO 27001/27017/27018, and Alibaba Cloud has certifications of compliance with ISO 27001/27017/27018, CSA STAR certification, and SOC (Service Organizational Control) independent audits.

- For information regarding AWS security, refer to the following link: aws.amazon.com/security/
- For information regarding Alibaba Cloud Security, refer to the following link: alibabacloud.com/trust-center/compliance

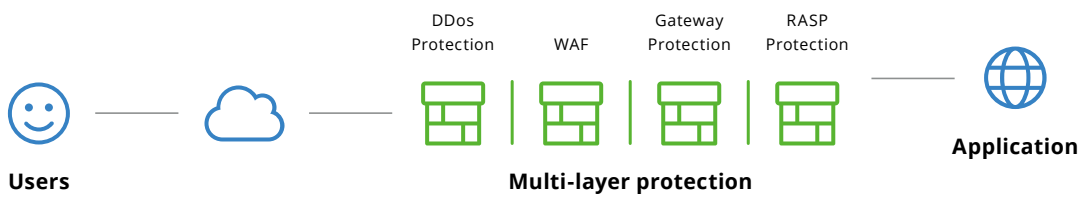
In addition, DJI has taken the following measures to ensure host security:

- DJI performs log security checks and scans to promptly discover and handle common vulnerabilities.
- The security operations team carries out periodic penetration tests for DJI cloud services.
- Intrusion detection systems are deployed on the server to promptly troubleshoot and handle exceptions.
- All R&D terminals are installed with antivirus products, where the virus databases are updated every day and vulnerability scans are conducted on critical system components each week.

INTERNET APPLICATION SECURITY

In most cases, network requests will pass through multiple layers of security protections designed by DJI before reaching backend services, including traffic cleaning for anti-DDoS, a web application firewall (WAF), and runtime application self-protection (RASP) (see Figure 13).

Figure 13: Multi-layer security [8]



[7] Consumer and enterprise drone data shared with DJI outside of China is stored on U.S.-based AWS servers. Photos or videos showcased on the public SkyPixel social media sharing platform are stored on U.S.-based Alibaba Cloud servers. Consumer drone users would have to opt-in to share this data as flight logs, videos and images are not shared by default on DJI drone platforms. Please see page 30 for more information.

[8] RASP Protection does not apply to FlightHub 2

DJI performs penetration testing and code analysis against online applications on a regular basis. Additionally, the codes for drone-related applications will be rigorously audited by security professionals to ensure security. If vulnerabilities are detected during inspection, a developer team will fix them immediately.

OPERATION SECURITY

Server-end operation security is maintained and operated by a professional operating team at DJI. DJI's operation team follows the best practices of resource management and authorization management recommended by Amazon AWS and Alibaba Cloud and observes the principles of Need-to-Know and minimum authorization. Host and system permissions are rigorously allocated and controlled. In the meantime, operations performed on the server-end are limited by strict standard operation procedure (SOP).

The DJI operation and maintenance management team is ISO 27001-certified and continues to obtain the certification validity. The ISO 27001 certification provides DJI customers with independent verification of information security management capabilities.

BUSINESS CONTINUITY AND DISASTER RECOVERY

To ensure the availability of DJI services, DJI has established a comprehensive service monitoring mechanism to promptly identify system availability issues. In addition, failure drills will be performed on DJI cloud services to improve the fault tolerance and restorability of the system. As for disaster recovery, the databases of DJI cloud services can be restored from backups created within the last 30 days and allow data to be restored to any time point in the last 7 days.

CLOUD SERVICES AND DATA SECURITY

DJI has formulated "Personal Data Protection Specifications" according to corresponding laws and regulations to regulate the data storage of every application. DJI's data transmission is encrypted to prevent malicious parties from obtaining it.

These practices are specified below:

- The data communication between browsers and servers uses a TLSv1.2 or after protocol;
- The data communication between mobile applications and servers uses a TLSv1.2 or after protocol.

Drone data shared with DJI outside of China is housed in U.S.-based cloud servers, with the exception of Agras drone data which is stored in servers based in the U.S., Japan or Europe (depending on which region the customer is based in).

DJI SERVICE

DJI Service provides most of the backend interfaces for DJI application software like DJI Fly, DJI Pilot series, and DJI Agras series, including device activation service, flight records synchronization service.

To delete all the data on DJI Service, contact support@dji.com. Refer to the DJI privacy policy at www.dji.com/policy for more information.

DJI SKYPIXEL

DJI SkyPixel is an aerial photography community that allows users to upload and share photos and videos taken by DJI products and third-party cameras. It also provides photo and video uploading as well as sharing functions for DJI apps.

With the user's consent, the data stored in DJI SkyPixel is as follows:

- Gender, country, username: This information is used for profile page display, provided by the user and is not mandatory. DJI will not perform authenticity verification.
- User-uploaded images and videos: This data includes the photos and videos that users upload to DJI SkyPixel which can be marked as publicly viewable or private.

To prevent the hacking of data in batches, DJI restricts the request frequency on the relevant interfaces.

User-uploaded content which is marked as private can be accessed only by specified authorized employees (i.e., operations administrator and content viewer). To prevent the user's images or videos from leaking, we have strict access restrictions on user data. Users cannot be identified by the uploaded file name because the uploaded resources have file names generated by random strings. Rather than the original, the app and web page displays cropped and compressed images.

Uses can delete uploaded photos and videos with the delete button. Users can delete all of their data by contacting support@dji.com. Refer to the DJI privacy policy at www.dji.com/policy for more information.

DJI FLIGHTHUB 2

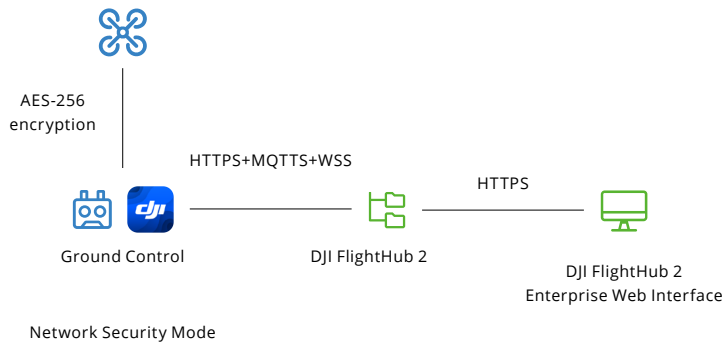
DJI FlightHub 2 is a cloud-based aircraft task management platform. It provides functions such as team and devices management, media file management, route library management, and flight route library management.

DJI FlightHub 2 supports multiple aircraft models (see the appendix for models that support DJI FlightHub 2) and it allows users to plan flight routes through the cloud and perform flight tasks using DJI Dock or DJI Pilot 2 APP (see Figure 14). In addition, DJI FlightHub 2 makes remote access to real-time operational information possible and improves team productivity and efficiency. The information communicated between DJI FlightHub 2 and devices includes:

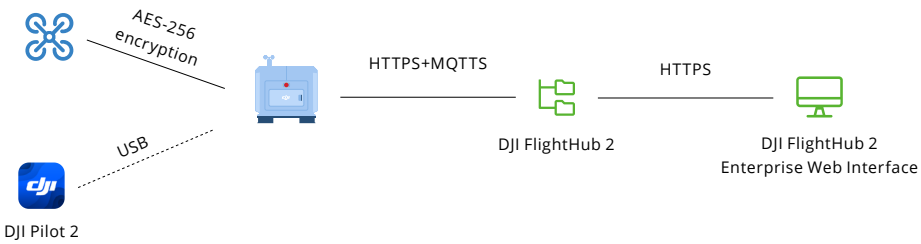
- Real-time device information, such as drone SN, transmission signal strength, latitude, longitude, livestreams from aircraft camera or payload
- Operation data such as media file, flight routes

Just like DJI FlightHub, the HTTPS, MQTTs, and WSS protocols and the anti-hotlinking mechanism are used to ensure the security between DJI FlightHub 2 and an app or a device.

Figure 14 DJI FlightHub 2 User Case



User case 1: Using FH2 with DJI Pilot 2 APP



User case 2: Using FH2 with DJI Dock

IDENTITY AUTHENTICATION AND ACCESS CONTROL

DJI FlightHub 2 uses a unified account for identity authentication, and the system adopts a role-based access control (RBAC) mechanism. In RBAC, access permissions are associated with roles. A user can obtain the permissions associated with a role by assuming the role. In DJI FlightHub 2, roles are divided based on two dimensions:

- Organization dimension: Roles in this dimension are mainly responsible for organization management, such as member management, device management, and organization project management.
- Project dimension: Roles in this dimension serve for projects and are mainly responsible for project permission management.

The two dimensions are independent of each other, so as to provide fine-grained permission management, data access control, and enhanced collaboration capabilities across multiple organizations. The following table describes all the roles in DJI FlightHub 2.

Dimension	Role	Permission
Organization	Super administrator	Manages the organizational life cycle and owns all the permissions of an organization. An organization must have at least one super administrator.
	Organization administrator	Manages members, devices, and projects within the organization
	Device maintainer	Manages all devices within the organization
	Member	Views project information, adds devices, and exits the organization
	Temporary member	Has limited operation permissions within the joined project
Project	Project administrator	Manages the project lifecycle and owns all project permissions. A project must have at least one project administrator.
	Member	Has limited operation permissions within the project.

DATA ENCRYPTION AND PRIVACY PROTECTION

To ensure data security, DJI FlightHub 2 implements security measures throughout the data management lifecycle which includes data collection, transmission, storage, and destruction. These security measures include, but are not limited to: access control, data classification, log auditing, watermarking, transmission encryption, and storage encryption.

DJI FlightHub 2 follows the principle of least privilege, and only processes user information on an as-needed basis. DJI will only access user information from DJI FlightHub 2 with user permission.

DJI FH2 stores data generated within China separately from data generated internationally. FH2 data from users within China is stored in China-based servers. FH2 data from other regions are stored in U.S. servers. The reliability of user data is ensured through a highly reliable distributed storage service. In terms of data encryption, storage encryption measures are provided for sensitive personal data. Global static encryption is also enabled by default for the whole database.

DJI FlightHub 2 uses standard encryption protocols to ensure data transmission security. DJI FlightHub 2's web interface communicates with the DJI FlightHub 2 server by using the HTTPS protocol. In addition, DJI Dock communicates with the DJI FlightHub 2 server by using MQTT with TLS.

AUDITABILITY AND COMPLIANCE OF DATA OPERATIONS

When a user requests assistance from the cloud platform due to technical or other reasons, DJI FlightHub 2 will operate on the data within the authorization scope of the user, and all operations will be logged.


Flycart 30

GEOFENCE SECURITY PROGRAM

FLIGHT RESTRICTION SYSTEM PROTECTION

The flight restriction system includes a GEO Zone database and flight control functions. The GEO Zone database stores geographic coordinate information, such as Restricted zones (such as airports), Altitude zones, and Authorization zones. Fight control function decides whether the drone can fly into a specific area and whether to apply certain restriction policies based on the GNSS information of the drone and the GEO Zone database.

To maintain a consistently reliable geofence system, the GEO Zone database and flight control functions must be protected. DJI signs the database to ensure the integrity of corresponding information.

Simultaneously, the security of flight control functions is gradually strengthened. The latest flight control functions perform signature verification in a trusted execution environment, which significantly improves the overall security of the system.

The flight restriction system analyzes the GNSS information from the GNSS module on the aircraft and the database stored in the aircraft, does not require networking, and does not upload the user's GNSS information. The GNSS information sent from the GNSS module is signed to prevent man-in-the-middle attacks and GNSS module replacement. If the app has network access during flight, an approximate location of mobile device (reduce accuracy to 5–10 km radius) will be used to check whether there is a temporary GEO Zone database in this area.

UNLOCKING SYSTEM PROTECTION

When necessary, a user can apply to unlock a GEO Zone. After the user submits an application, the corresponding certificate will be signed and can be downloaded to the aircraft by the user. The flight restriction system performs signature verification on the certificate and compares it with the GNSS Information and device SN to determine whether to unlock the flight restriction. Go to www.dji.com/flysafe for more information on Fly Safe.

In public safety scenarios, relevant enterprises or organizations need to operate in the long term without restrictions. In view of this, DJI launched the Qualified Entities Program (QEP). The enterprises or organizations can join the QEP and obtain a longer unlocking duration. The minimum unlocking duration is five calendar years. Currently, the QEP is available only in North America, Canada, and Europe.

DJI Mavic 3 + DJI RC-N1

SECURITY AUDITS & CERTIFICATIONS

Our data security practices have been validated by multiple federal agencies as well as independent private sector firms – since 2017. The agencies independently procure DJI products off-the-shelf and conduct a thorough technical investigation.

An overview of the audits and their findings are outlined below.

ISO 27001 CERTIFICATION FOR DJI FLIGHTHUB 2 (2023)

DJI FlightHub 2 has obtained ISO 27001 certification, issued by the British Standards Institution (BSI), which proves that the design, development, and operational services (such as risk management, security controls, and continuous improvement) of DJI FlightHub 2 comply with the information security management standards.

FIPS 140-2 CERTIFICATION (2022)

FIPS 140-2 is a security standard issued by the U.S. government for cryptographic modules. In 2022, the DJI Core Crypto Engine obtained the NIST FIPS 140-2 CMVP Level 1 certification, which proves that DJI meets the rigorous security standards in design and implementation and provides a high level of protection for sensitive data and communication. The engine is a firmware hybrid cryptographic module which provides foundational security services for the entire platform, including cryptography, key management, platform identity, secure boot, and secure Life Cycle State (LCS).

Formally validated by the U.S. and Canadian Governments, FIPS 140-2 compliance has been widely adopted around the world in both governmental and non-governmental sectors as a practical security benchmark and realistic best practice. The standard ensures that the hardware validated meets specific security requirements.

DJI products are equipped with this secure engine, which indicates that the products have a high level of security and comply with industrial and regulatory security standards. Click here [9] to view the certificate details.

[9] https://www.dji.com/no/newsroom/news/dji-achieves-encryption-recognition-from-us-department-of-commerce

TÜV SÜD AUDIT (2022)

In 2022, TÜV SÜD conducted an audit of the following product portfolios of DJI: DJI consumer drones (DJI Air 2S, DJI Mini 2, and DJI Mavic 3) along with the DJI Fly app (for iOS and Android) and a DJI industrial-grade drone (DJI Matrice 300 RTK) along with the DJI Pilot app (for Android). The audit reports issued by TÜV SÜD confirm that the preceding product portfolios meet the requirements of NIST IR 8259 and ETSI EN 303645 standards in terms of network security and privacy protection.

Click here [10] for more information.

BOOZ ALLEN HAMILTON - UAS COE AUDIT (2020)

Cybersecurity firm Booz Allen Hamilton, on behalf of PrecisionHawk's Unmanned Aerial Intelligence Technology Center of Excellence (UAS CoE), conducted risk assessment testing and analysis of three DJI commercial drone products: Mavic Pro GE, Matrice 600 Pro GE, and Mavic 2 Enterprise.

Click here [11] for more information.

FTI SECURITY AUDIT (2020)

FTI Consulting (FTI), a global leader in cybersecurity, conducted an independent review and validation of Local Data Mode and DJI's drone products through a source code review of DJI applications as well as a hardware cybersecurity review of devices. The audit found that when Local Data Mode was enabled, no data generated by the drone or application was sent externally to infrastructure operated by any third party, including DJI, validating DJI's assertions about the utility and function of the feature.

Click here [12] for more information.

U.S. Department of Interior (2019)

The U.S. Department of the Interior (DOI) conducted thorough tests and evaluations on the DJI government-grade (GE) version of drones: Matrice 600 Pro and Mavic Pro.

Click here [13] for more information.

[10] https://www.dji.com/newsroom/news/new-independent-audit-of-select-dji-products-successfully-tests-against-national-cybersecurity-and-privacy-protection-standards

[11] https://viewpoints.dji.com/blog/no-evidence-of-unexpected-data-transmission

[12] https://security.dji.com/news?newsId=case-9&lang=en_US

[13] https://www.dji.com/newsroom/news/us-federal-agency-validates-and-approves-dji-high-security-solution-for-government-drone-programs

KIVU SECURITY AUDIT (2018)

Kivu is a U.S.-based cybersecurity agency. In 2018, DJI released Kivu's independent report, which reviewed DJI's data security practices and concluded that DJI is capable of protecting users' personal data.

Click here [14] for more information.

DJI FLIGHTHUB SOC2 AUDIT (2017)

DJI FlightHub products have passed the SOC2 certification issued by the American Institute of Certified Public Accountants.

[14] https://security.dji.com/news?newsId=case-5&lang=en_US

DJI Air 3

DJI BUG BOUNTY PROGRAM

DJI has always been committed to improving the security of its products. While having established organizations, processes, and specifications to accomplish this, DJI has always adhered to and advocated for a culture of open cooperation, and has always valued collaboration with industry-leading security vendors and researchers.

In August 2017, DJI launched the Bug Bounty Program and invited security experts to identify potential security vulnerabilities on DJI platforms, which included servers, applications, and devices. This program is part of the company's continued efforts in strengthening its data security and implementing comprehensive privacy measures for customers. From August 2017 to January 2024, 296 information security experts have submitted reports regarding possible vulnerabilities within our platforms. Each report has been carefully reviewed and evaluated by our team. We have also resolved these issues, which has greatly improved the security and stability of our products and ensures better data protection for our customers.

In accordance with the DJI Bug Bounty Program Policy, over US$136,600 in cash and DJI credits have been awarded to security experts. From 2020 to 2024, we have also organized a wide range of events. In order to express our gratitude for the significant contributions from the security researchers and white-hat hackers, we doubled some of the rewards as a token of our appreciation. In 2021, DJI participated in Bug Bounty campaigns together with other security response centers and attracted more researchers as a result.

Drones have provided tremendous changes and benefits to various industries around the world. Keeping them secure will require continued investments and collaboration with the data security research community.

If you'd like to participate, please contact us at bugbounty@dji.com


MINI 4 PRO

DJI PRIVACY POLICY

DJI has explicit policies regarding user personal data protection and encourages users to read and confirm these policies when they use DJI's devices, computer software, and cloud services.

For more information about privacy policies, visit www.dji.com/policy

DJI Mavic 3 Enterprise

CONCLUSION

Drones have rapidly become a valuable tool for professional use, and users who work with high-security information demand the same type of strong security precautions for drones and drone data as they do for every other technology in their toolbox. The preceding pages of this white paper demonstrate how DJI has embraced that challenge, and how we will continue to test, validate and improve our data security protocols.

DJI has earned its leadership role in the industry by relentlessly innovating the features that define modern drones. Customers choose DJI products because our systems provide stable, reliable, flexible and highly capable aerial data collection, and they have made clear they want the data security protections necessary to let them continue using DJI systems.

We have detailed our commitment to responsible data stewardship because we recognize how important it is for our customers. We hope our work to set high data standards can once again become a standard for the entire drone industry, encouraging strong protections and a deep-seated commitment to treating customer data with the respect it deserves.

We invite you to visit the DJI Trust Center to stay updated with the latest information and announcements. We also welcome your input on how to continue enhancing and improving data protection.

Please contact us at datasecurity@dji.com with your questions, comments and suggestions.

DJI Mavic 3 Classic

APPENDIX

- **Models that support device certificates:** Mavic 3 series, Air 3, Mini 3 Pro, Mini 4 series, Avata, Inspire 3, Matrice 30 series, Mavic 3 Enterprise series, Mavic 3M, Matrice 350 RTK, Matrice 3TD/3D, the remote drone operations solution, FlyCart 30, T60/T25P, T50/T25, T40/T20P

- **Models that support secure boot:** Phantom 4 RTK, Mavic 3 series, Air 3, Mini 2 SE, Mini 3 series, Mini 4 series, Inspire 3, Mavic 3 Enterprise series, Mavic 3M, Mavic 2 Enterprise Advanced, Matrice 30 series, Matrice 350 RTK, Matrice 3TD/3D, the remote drone operations solution, FlyCart 30, T60/T25P, T50/T25, and T40/T50P

- **Models that support DM-Verity:** Mavic 3 series, Air 3, Mini 2 SE, Mini 3 series, Mini 4 series, Inspire 3, Mavic 3 Enterprise series, Mavic 2 Enterprise Advanced, Mavic 3M, Matrice 30 series, Matrice 350 RTK, Matrice 3TD/3D, FlyCart 30, T60/T25P, T50/T25, and T40/T50P

- **Models that support SELinux:** Mavic 3 series, Air 3, Mini 2 SE, Mini 3 series, Mini 4 series, Inspire 3, Mavic 3 Enterprise series, Mavic 2 Enterprise Advanced, Mavic 3M, Matrice 30 series, Matrice 350 RTK, Matrice 3TD/3D, FlyCart 30, T60/T25P, T50/T25, and T40/T50P

- **Models that support log one-click deletion:** Matrice 350 RTK, Matrice 30 series, Matrice 3TD/3D, Mavic 3 Enterprise series, Mavic 3M, and Inspire 3

- **Models that support SD card log encryption:** Inspire 3, Matrice 30 series, Matrice 350 RTK, T60/T25P, T50/T25, T40/T20P, and FlyCart 30

- **Models that support media data encryption:** Matrice 30 series and Mavic 3 Enterprise series

- **Models that support the reset all function:** Mavic 3 series, Mini 3 series, Mini 4 series, Avata, and Air 3

- **Models that support 4G enhanced transmission:** Mavic 3 series, Mini 3 Pro, Mini 4 series, Air 3, Inspire 3, Mavic 3 Enterprise series, Mavic 3M, Matrice 30 series, Matrice 3TD/3D, Matrice 350 RTK, T60/T25P, FlyCart 30, and the remote drone operations solution

- **Models that support integration with DJI FlightHub 2:** Matrice 350 RTK, Matrice 3TD/3D, Matrice 30 series, Mavic 3 Enterprise series, Mavic 3M, and the remote drone operations solution

- **Models that support integration with DJI FlightHub 2 on private clouds:** Matrice 350 RTK, Matrice 30 series, Matrice 3TD/3D, Mavic 3 Enterprise series, Mavic 3M, and the remote drone operations solution

- **Models that support QuickTransfer:** Mini 3, Mini 3 Pro, Mini 4 series, Air 3, Mavic 3, Mavic 3 Classic, and Mavic 3 Pro

- **Models that support offline GEO Zone unlocking:** Mavic 3 Enterprise series, Mavic 3M, Matrice 30 series, FlyCart 30, Matrice 3TD/3D, and Matrice 350 RTK

This white paper does not cover the following EOL products:

- **Consumer drones:** Mavic 2, Mavic Pro series, Air 2S, Air, Mini SE, Mini 2, Mavic Mini, Inspire 2, Inspire 1 series, DJI FPV series, Spark, Phantom 4 Pro series, and Phantom 4 Advanced

- **Industrial-grade drones:** Matrice 300 RTK

- **Agricultural drones:** T16, T20, and T30

DJI Avata

GLOSSARY

Abbreviations	Full Name
AES	Advanced Encryption Standard
API	Application Programming Interface
APP	Application
AWS	Amazon Web Services
CBC	Cipher Block Chaining
CSA STAR	Cloud Security Alliance, Security, Trust, Assurance & Risk
DDoS	Distributed denial-of-service
DM-Verity	Device Mapper Verity
DOI	U.S. Department of the Interior
DTS	Data Transfer Service
ECC	Elliptic Curve Cryptography
ELF	Executable and Linkable
HTTPS	Hypertext Transfer Protocol Secure
ISO	International Organization for Standardization
JTAG	joint Test Action Group
LAN	Local Area Network
LDM	Local Data Mode
MQTT	Message Queuing Telemetry Transport
MQTTS	Message Queuing Telemetry Transport with TLS
MSDK	Mobile Software Development Kit
OSDK	Onboard Software Development Kit

OTP	One Time Program
PoLP	Principle of Least Privilege
PSDK	Payload Software Development Kit
QEP	Quailed Entities Program
RASP	Runtime application self-protection
RC	Remote controller
ROM	Read-only memory
RPMB	Reply Protect Memory Block
RSA	Rivest-Shamir-Adleman
RTMP	Real Time Messaging Protocol
SD Card	Secure Digital Memory Card
SDK	Software Development Kit
SELinux	Security-Enhanced Linux
SHA	Secure Hash Algorithm
SN	Serial Number
SOP	Standard Operation Procedure
SSD	Solid-state drive
TEE	Trusted Execution Environment
WAF	Web Application Firewall
WPA	Wi-Fi Protected Access
WSS	WebSockets over SSL/TLS

security.dji.com/data