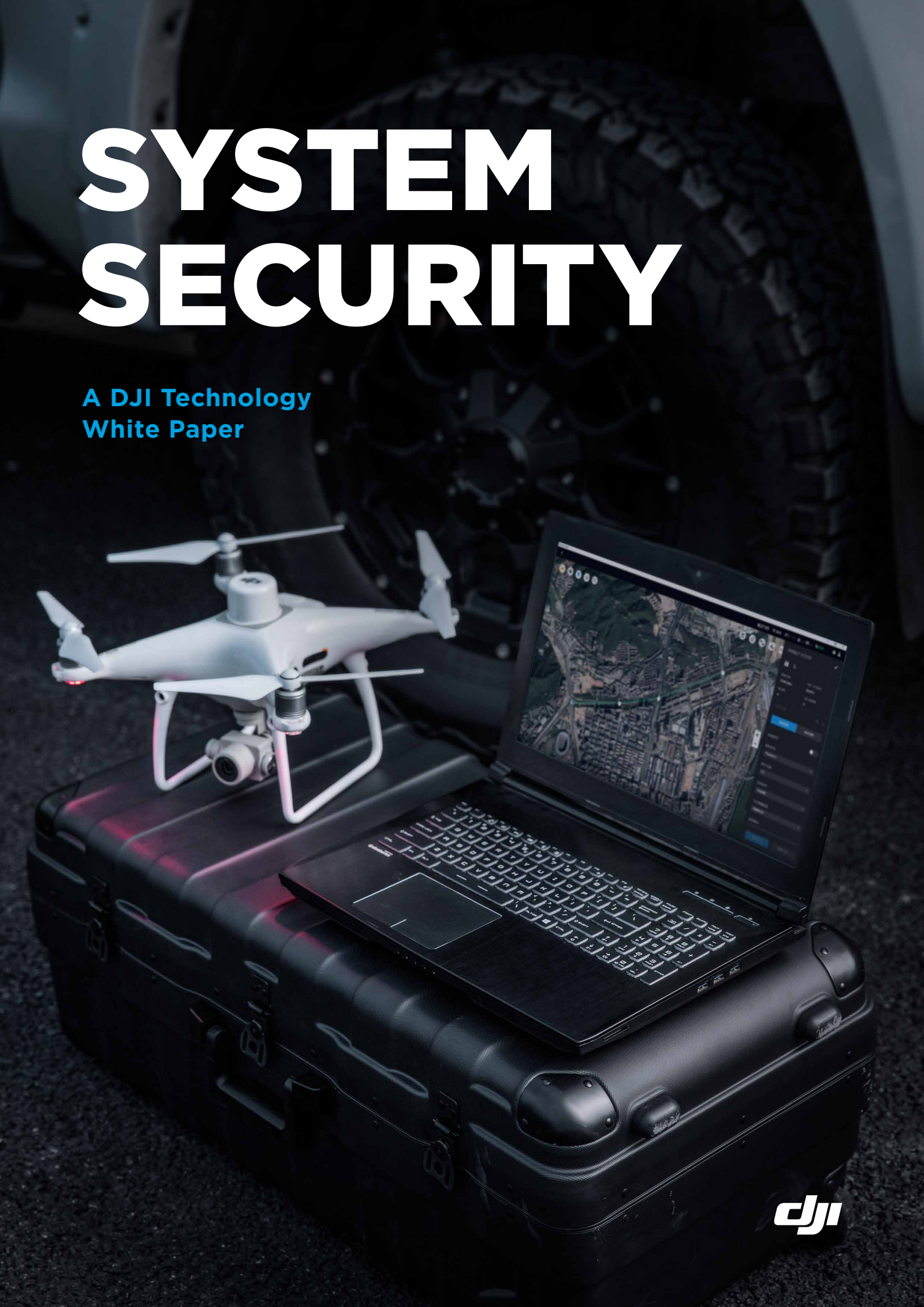
SYSTEM SECURITY

A DJI Technology
White Paper



DJI System Security

This paper outlines key systems in a drone and the security measures DJI has implemented to bolster security and protect the integrity of user data.

A DJI Technology White Paper
April 2020

security.dji.com/data

CONTENT

INTRODUCTION

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, we pioneered the widespread adoption of ready-to-fly recreational drones, and today our solutions serve professionals, enterprises and government agencies around the world.

DJI's innovative technology has become the preferred platform for aerial data collection in a wide range of industries, including agriculture, construction, energy, media and public safety. DJI's open architecture has enabled a flourishing marketplace of additional hardware payloads, software systems and mobile apps, which allow the world's innovators to develop creative solutions for a variety of pursuits.

As DJI has grown, we have worked hard to establish ourselves as the leader in many ways:

- Our thousands of engineers have led the technological development that makes the drone era possible. DJI invented the product category of highly capable off-the-shelf quadcopters, created camera stabilization systems for drone imagery, and enabled thermal imaging drone cameras for routine professional use.
- DJI has led the industry in developing safety systems to ensure drones remain a safe addition to the skies. DJI created the first geofence, knowledge testing and remote identification systems for consumer drones, long before legal or regulatory systems required them.
- As governments and businesses increasingly deploy drones on special and confidential missions, DJI is now leading the drone industry in developing standards for responsible and secure stewardship of this data.

As drone users have become increasingly aware of the unique ways in which drone data must be monitored and secured, DJI has enhanced its data security protections to meet these growing expectations. DJI established an internal Product Security Committee to manage cross-department security initiatives and oversee ongoing internal penetration testing programs, as well as established a successful Bug Bounty Program that rewards security researchers from around the world for responsibly disclosing potential security vulnerabilities. DJI also commissioned an independent cybersecurity study that confirmed DJI customers have control over their data, and that DJI does not access customer data unless customers choose to share it with us.

Now, DJI is leading the drone industry to look beyond particular data management issues and create a wider set of principles for how drone data should be managed and secured. This framework includes a three-fold commitment to our customers:

Transparency and education: DJI commits to defining the principles behind our data stewardship and help our customers understand how their data is generated, collected, managed, analyzed and stored.

Research and development: DJI commits to continuous investment in enhancing security protocols, cultivating a security-conscious culture and developing unique solutions for customers with the most rigorous data protection needs.

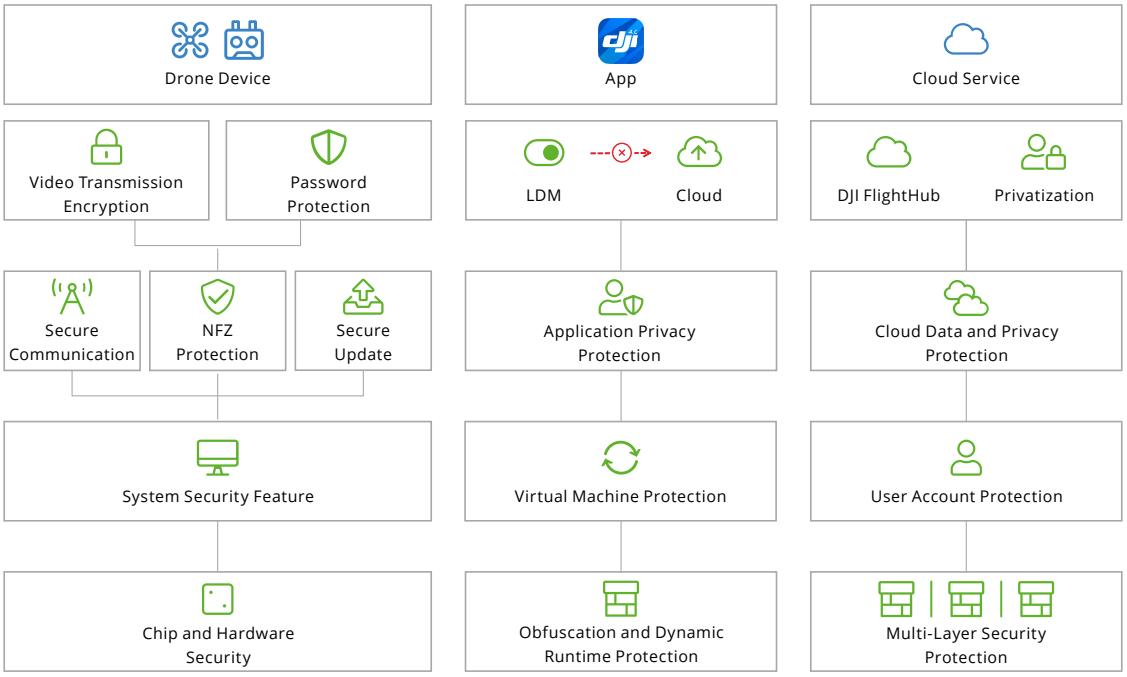
External validation: DJI commits to continue working with third parties to conduct independent audits and review of its product and system security.

This white paper is part of our commitment to ongoing transparency and education. It outlines the key systems in a drone system and identifies the security measures DJI has implemented to bolster security and protect the integrity of user data:

- Drone hardware, including aircraft, remote controllers, and viewing systems such as goggles.
- Communication systems, including protocols for connections between the drone and its remote controller.
- Applications, including mobile apps for operating drones and computer applications for processing and analyzing drone-collected data.
- Cloud services, including DJI's options for storing and managing data on different types of cloud architecture. Figure 1

We hope the discussion on the following pages provides helpful information about the details of how DJI systems handle data, and illuminates the care and scrutiny DJI applies to its stewardship of customer data.

Figure 1: System Overview



DEVICE SECURITY

Drones products face risks of security threats and attacks when used, such as static and dynamic code injection. The lack of relevant security design and infrastructure may make the drone system vulnerable to multiple attacks, such as user data theft, communication hijacking, sensitive information leakage, drone cloning, flight log theft, etc.

DJI drone systems adopts Trusted Execution Environment, secure engine and key management, secure boot, access control, system partition protection, and other technologies to raise the bar on security and ensure sufficient user protection for data, communication, and property. Figure 2

CHIP AND HARDWARE SECURITY

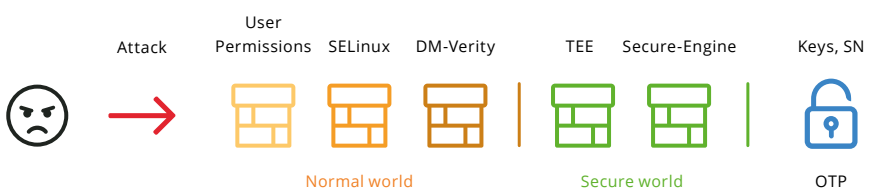
Chips and hardware security is the foundation of drone system security. It makes DJI's drones more secure and more reliable.

TRUSTED EXECUTION ENVIRONMENT (TEE)

Most DJI drone products use the ARM® Cortex®-A series processor, which supports ARM® TrustZone® technology. ARM® TrustZone® is a type of Trusted Execution Environment (TEE) technology. TrustZone® technology can divide the processor into a secure world (running a secure OS and trusted applications) and a normal world (running the rich OS). In Trust Zone® , 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 drone 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 normal world to ensure the confidentiality of data.

Figure 2: Device Security Infrastructure



SECURE ENGINE AND KEY MANAGEMENT

DJI drones adopt the ARM® CryptoCell series secure engine. The secure engine runs in the secure world of the drone and can access and use the key of 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 drone, 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. Following the cryptographic strength recommendation, the minimum key length and key usage are as follows: **keylength.com/en/compare**

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

The key is the most important parameter on the device side 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 transmission, injection, and access comprehensively. The introduction of the hardware secure engine prevents the key from exposure to normal world, ensuring the security of the key when the system is running.

DEVICE UNIQUE SERIAL NUMBER

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

DEBUG CHANNEL DISABLED

When the DJI drone is 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 is intended to describe the security features of the drone.

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 chip during manufacture 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. Figure 3

This secure boot chain ensures the integrity of the drone 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.

There are several DJI products that currently support secure boot (the implementation of secure boot can be slightly different for different products).

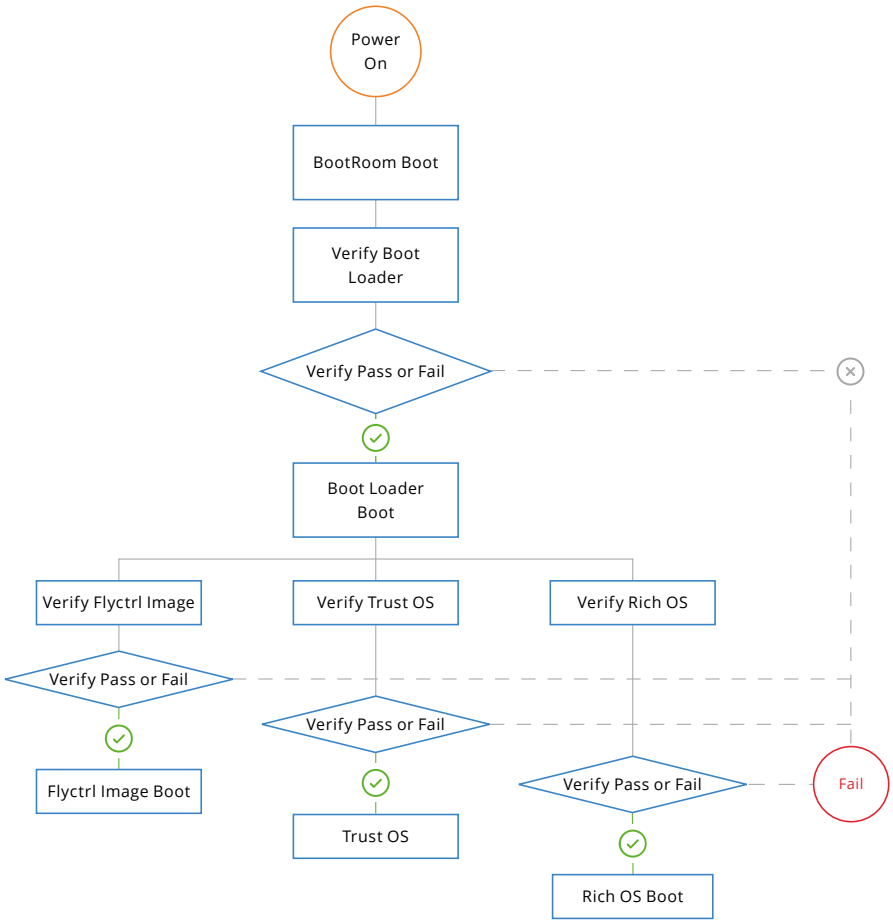
- Consumer: Inspire 2, Spark, Phantom 4 series, Mavic series
- Enterprise: M200 series, Mavic 2 Enterprise
- Government: Mavic Pro GE

DM-VERITY

Currently available in Mavic Air, Mavic 2, Mavic 2 Enterprise and Mavic Mini. 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. During the boot process, the public key is used to verify the integrity of the hash tree. Then 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.

Figure 3: Secure boot chain



SELINUX

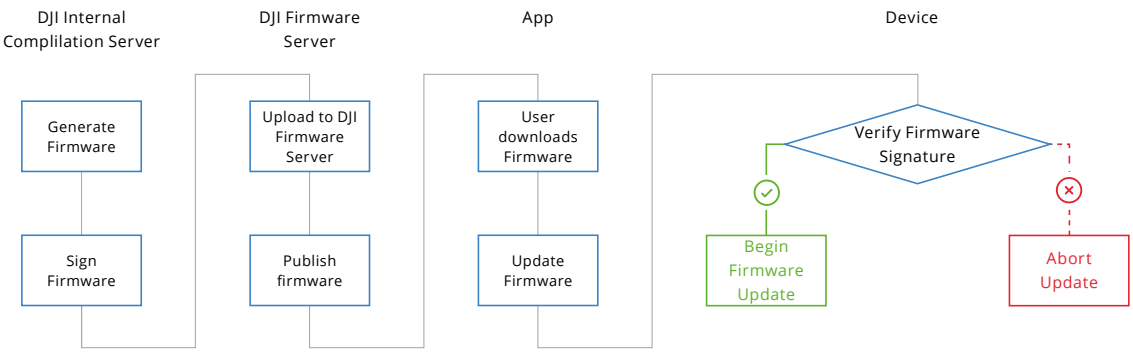
The Mavic 2 and Mavic 2 Enterprise DJI drone systems support SELinux, which controls access to all resources such as processes, operations, and files, ensuring that there is no violation of access control policies in the system. The access control policies are stored in the root file system and protected by the device's secure boot to avoid tampering by a third party.

SECURE UPDATE

DJI drones support remote system updates for new features release, bugs fix, 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. 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



DEVICE DATA SECURITY

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 log	Sensor data, GPS information, and user control data during flight.	Onboard storage	User can export flight logs through DJI Assistant 2, and the flight logs will be encrypted by the export process on the drone.
Live flight status	Environmental information and real-time information of the drone during flight, such as current altitude, latitude and longitude, power voltage, etc., and does not contain any user information.	Not stored	Live flight statuses transmitted to the app are encrypted by the drone when the drone is in operation.
Device log	Device log is generated during the operation of the drone to locate and solve a system bug	Onboard storage	User can export device logs through DJI Assistant 2, and the device logs will be encrypted by the export process on the drone.
Media data (onboard)	Photos or videos taken by the user	Onboard storage	If device password protection is enabled, a password is required to access onboard media data. Otherwise, users can access it through the app.
Media data (SD card or SSD)	Photos or videos taken by the user	SD or SSD	User accesses media data via physical connection only (i.e., card reader)
Update package	Drone system firmware	Onboard storage	The firmware is encrypted and signed by DJI, then transmitted to the drone via app or DJI Assistant 2.

LOG EXPORT ENCRYPTION

Users can export flight logs and device logs through DJI Assistant 2. The exported logs are usually used to locate, analyze, and assess causes for system failures. 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 the attacker to understand the system, thereby improving security. Encrypting the exported flight log also protects the user's flight data.

NO FLIGHT LOG

Flight logs are generated during the operation of a drone. As users in a governmental capacity require higher standards for data security and privacy, DJI has provided a "no flight log" feature, exclusive to DJI Government Edition drones. This feature disables flight logs recording while the drone is in use.

DEVICE PASSWORD PROTECTION

Users can apply password protection to drone media data and property. When the password protection function enabled, the password is required in the scenarios like powering up, setting transmission frequency and accessing the onboard media storage via computer or app. Currently, the Mavic 2 Enterprise drone supports this feature. Figure 5

The password protection function prevents unauthorized access to the drone's media data. For example, it helps protect the user's media data when the drone is not properly grounded or flies away.

Figure 5: Password protection

COMMUNI-CATION SECURITY

DJI attaches great importance to the security of the drone communication system. Currently, the communication transmission schemes used by DJI mainly include OcuSync and Wi-Fi. This chapter will introduce the security of these two solutions respectively.

OCUSYNC COMMUNICATION SECURITY

OcuSync is a proprietary DJI protocol with built-in security features. The OcuSync communication solution is widely used in drones such as Mavic 2, Matrice 200 V2, and Mavic 2 Enterprise. The control link is encrypted by the AES algorithm, and the session key used for encryption is generated by a random number generator every time the drone is powered on, ensuring a unique encryption key for each use. The Mavic 2 Enterprise and Matrice 200 V2 drones also support the video transmission encrypted by the AES 256 standard.

OcuSync's 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.

WI-FI COMMUNICATION SECURITY

DJI products that use Wi-Fi for image transmission are Mavic Air, Spark and Mavic Mini. The TCP/IP layer allows only a single authenticated legitimate client connection and communication at one same time. Other clients will be unable to connect to the device.

When a mobile device controls the drone directly, the universal standard wireless LAN protocol is used, and the standard protocol supports the WPA2-PSK encryption scheme.

When using a remote controller, a proprietary custom Wi-Fi protocol is used. The privately customized Wi-Fi protocol adds physical layer protection to the encryption. It only supports scanning and connection among DJI internal devices, and the connection key is randomly generated and updated for every use.

APPLICATION SECURITY

DJI application software includes DJI GO series, DJI Pilot series, DJI Assistant 2 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, and explain the application security settings and privacy settings in detail according to the types and functions of the application.

In addition to applications, DJI provides 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. The last section of this chapter will explain privacy security settings, open source status, and other details of SDKs.

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 increases 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 check and protect key processes of the system through the monitoring mechanism to prevent attackers from debugging the app;
- Perform anti-hook check on key functions by means of polling;

- Prevent dynamic debugging and dynamic injection attacks by monitoring common debugging methods and features of injection tools;
- Replace and hide 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 logs, shared preferences, databases, and application logs.

Integrity protection

All contents of the app installation packages are cross-checked, and 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 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 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 reverse analysis hard to be performed;
- 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 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.

APPLICATION DATA SECURITY

This section will interpret the data security policy of DJI applications in detail from multiple dimensions such as communication, local data storage and data synchronization, and privacy settings.

DJI GO

DJI GO series applications (including DJI GO, DJI GO 4, and later) 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 data stored locally by DJI GO includes the No-Fly Zone database, flight records and application logs. The locally stored No-Fly Zone database is only used for displaying the No-Fly Zone on the flight interface map, and the actual flight restriction function is implemented in the drone. The No-Fly Zone database in the app is encrypted and stored with signatures to ensure the confidentiality and integrity of the database. There are two types of flight record: simplified flight control log and user flight record data. The simplified flight control log is generated by the drone, including the operating environment information and real-time equipment information (e.g., current altitude, latitude and longitude, power voltage), is protected by the drone and stored in the app, and is not automatically uploaded to DJI servers. User flight record data is recorded by DJI GO during flight, and includes flight time and flight route. This data is protected and stored locally and is not automatically uploaded to DJI servers. Users can view the simplified flight control log and user flight record data on the flight record page and upload them to the cloud. Application logs are encrypted and stored locally, and contain application status information and crash logs, helping to debug and locate any software bugs. Only when the app encounters a problem, the user manually uploads the application log to DJI.

During the first operation of the application, it will prompt to explain and to let user confirm the use of each personal information.

In subsequent use of the application, users can also turn on or off the authorization of the user information they selected at any time in the "Privacy Settings" tab of the application's "Settings" page. The table below lists the configurable user privacy settings.

DJI PILOT

DJI Pilot is an application that interacts directly with enterprise grade 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 drone applications in industry. In addition to inheriting the security features of consumer applications, DJI Pilot delivers features that meet enterprise security demands.

DJI Pilot supports DJI FlightHub, the drone management platform provided by DJI. A detailed introduction to FlightHub can be found in the DJI FlightHub chapter below.

Local Data Mode (LDM)

As enterprise and government agencies value data secrecy, it is necessary to ensure that the data generated during the operation is effectively protected. With LDM, users can cut off all network links from the application and prevent any data from being transferred out.

User Info	Description
DJI device hardware information	Information of DJI device that is paired with the app, including serial numbers of the main control, gimbal, camera and battery.
Mobile device GPS information	GPS information of the mobile device running the app.
DJI device GPS information	GPS information of the DJI device that is paired with the app.
User experience information	This information is used in the product improvement program and will prompt the user to choose whether to participate during its first operation. The information includes the user's preference setting for the app UI interface and drone operation, and helps DJI improve products and services by automatically sending diagnostic and usage data every day. The information record is anonymous.

When Local Data Mode is enabled, all data can only be used locally, and no network request will be initiated to send data to its own server or a third-party server. When users want to use network services, they can temporarily disable LDM to access them (the data accumulated before LDM is disabled will not be transmitted), such as firmware update or unlocking flight restriction.

DJI Pilot PE

DJI Pilot Private Edition (PE) mainly provides the following two working modes for users:

1. Local Data Mode (LDM): It is enabled by default if the user does not configure the address of the private cloud server. LDM cuts off all network links of the application. LDM continues to function while the application is in use and cannot be disabled manually.

2. Private Server Mode: The application will enter Private Server Mode after the user configures the address of private cloud server in the setting menu. This mode needs to be used in conjunction with DJI FlightHub Private Cloud. The data will be transmitted back to the private server set by the user, and will not interact with the DJI server.

DJI Pilot GE

DJI Pilot Government Edition (GE) is specifically customized for government users. Based on DJI Pilot PE, DJI Pilot GE is equipped with enhanced security control capabilities: It supports login without accounts and no flight logs. GE version drones are compatible with DJI Pilot GE only.

DJI ASSISTANT 2

DJI Assistant 2 series software is client software that interacts with DJI drones on Windows and Mac computer platforms. The main basic functions include firmware update, flight 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.

During the use of DJI Assistant 2 software, the following information will be obtained to ensure that all functions are working properly, see table below. During the software's first operation, it will prompt for data access authorization for the software. In subsequent software usage, the user can change the authorization settings at any time in the Settings page at the top right of the software.

User Info	Description
User account information	This information includes account information registered with DJI.
DJI device serial number	This information is the serial number of the DJI device that is connected to this app.
Payload SDK information	This information includes Product ID and License information. Developers apply for Product ID and License Information from DJI Developer Website for using Payload SDK.
Onboard SDK information	This information mainly contains app ID information.
User experience information	This information is used in the product improvement plan and will prompt the user to choose whether to participate after the first installation of the user. The information includes the user's preference record 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 record is anonymous.

DJI Assistant 2 GE

DJI Assistant 2 Government Edition (GE) cannot directly connect with DJI server. Users need to download the upgrade package offline to upgrade their device. It is only compatible with GE devices; mixed usage with consumer or enterprise devices does not work.

DJI SDK SECURITY

DJI produces several SDKs, including Mobile SDK, UX SDK, Onboard SDK, and Payload 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 Mobile SDK (MSDK), developers can build iOS and Android applications that interface wirelessly with drones. MSDK creates a customized mobile app to unlock the potential of 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 the developer develops an app via MSDK for the first time, or when the user runs an app developed by MSDK for the first time, MSDK will connect to a DJI server for activation.	No
Firmware upgrade check	When the user connects a device with an app developed by MSDK, the latest firmware information will be pulled by MSDK from the server, and to prompt the user to upgrade.	No
No-Fly Zone database update	When the user connects a device with an app developed by MSDK, the latest No-Fly Zone database will be pulled by MSDK from the server to help flying in accordance with local laws and regulations.	No
Real-name authentication (Mainland China only)	According to Chinese regulatory requirements, users in mainland China must provide telephone numbers for real-name authentication. This is not required in other regions.	No
Country code	Current user's country code will be obtained. This information will mainly be used to set up the remote controller's frequency band.	No
User experience information	When the user uses an app developed by MSDK, 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 FlightHub	When the developer calls the DJI FlightHub related API in MSDK, communication with the DJI FlightHub server will be established.	Yes
DJI User Center	When the developer calls the DJI User Center related API in MSDK, communication with the DJI User Center server will be established.	Yes
Third-party network RTK service	When the developer calls the API in 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 provided by 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, users must complete SDK registration and activation when using the app for the first time. Activation only needs to be completed when using the app for the first time, and repeated activation is unnecessary. For LDM-equipped apps, after the activation is completed, users can enable the LDM to cut off all network links. Currently LDM mode is not available in mainland China.

DJI UX SDK

DJI UX SDK provides UI elements for all core functions, which enables developers to build mobile applications swiftly with no additional lines of code.

Since the major function of UX SDK is to provide UI elements, internet connection is unnecessary during the use of UX SDK. However, when using the DJI Map Kit, users can embed a third-party map widget, which can trigger an internet connection with the third-party map during use.

UX SDK is an open source project. Users can download relevant source code from DJI Developer Website or DJI SDK official GitHub **(github.com/dji-sdk).**

DJI ONBOARD SDK

DJI Onboard SDK (OSDK) helps to build automated drone applications for supported DJI aerial devices (Matrice 100, Matrice 600, Matrice 210/210-RTK, Matrice 210/210-RTK V2), and the A3 and N3 Flight controllers.

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

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

Part of the DJI OSDK code uses open source; please refer to the following links:

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

Developers need to register a DJI PSDK enterprise account first, 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 PSDK, mainly recording commands and errors related to PSDK functions. The log does not include user 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 PSDK, the app needs to be bound with DJI SKYPORT. During the process, the DJI SKYPORT adapter will verify information such as user account, product name, and product ID with server through MSDK.	No
PSDK unbinding with SKYPORT	PSDK applications can also be unbound from DJI SKYPORT. During the process, the DJI SKYPORT adapter will also verify information such as user account, product name, and product ID with server through MSDK.	No
User experience data	This data mainly records the usage time of each PSDK functions, version information, developer information, GPS Location information after reducing accuracy (reduce accuracy to a 10 km radius), etc. Users can turn off the authorization of user experience data upload in the “Privacy Settings” tab in the app or DJI Assistant 2.	Yes

CLOUD SECURITY

DJI provides users with a variety of cloud services to enrich product features. After obtaining authorization from users, the cloud will store data. 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 value-added services. Other applications perform account operation via embedded web page, 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 prompted if an account is logged in at a location which is not included on the commonly-used location list.
- Traffic Limit: To prevent the 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 key user information in the database and encrypts network traffics with HTTPS.

SERVER SECURITY

This section demonstrates the server security of DJI in three aspects: host security, web application security, and operation security.

HOST SECURITY

DJI internet services are primarily deployed onto the cloud, so the security of services heavily depends on cloud providers. DJI employs Amazon AWS and Alibaba Cloud as cloud service providers, which are known for their security qualification and high reliability. AWS has certification for compliance with ISO 27001/27017/27018, and Alibaba Cloud has certification for compliance with ISO 27001, CSA STAR certification and SOC independent auditing.

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

DJI attaches great importance to host security, and schedule scanners to check host configurations to ensure the security and handle the vulnerabilities on time.

INTERNET APPLICATION SECURITY

In most cases, network requests will pass multiple layers of security protection designed by DJI before reaching back end services, including traffic cleaning for anti-DDoS, a web application firewall (WAF), and runtime application self-protection (RASP). Figure 6

DJI will perform full penetration testing and static code analysis against online applications regularly. Additionally, the coding 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 and efficiently.

OPERATION SECURITY

Server-end operation safety is maintained and operated by a professional operation team at DJI. From the technical perspective, DJI's operation team follows the best practices of resource management and authorization management recommended by AWS and Alibaba Cloud. In the meantime, operations performed on server-end are limited by strict Standard Operation Procedure (SOP). From the management perspective, all operations performed on server comply with local laws and are strictly audited. Following the principle of minimum authorization, host and system permissions are rigorously allocated and controlled and resources of different tenants are isolated properly. The DJI operation and maintenance management team has passed ISO27001 certification in February 2020.

CLOUD SERVICES AND DATA SECURITY

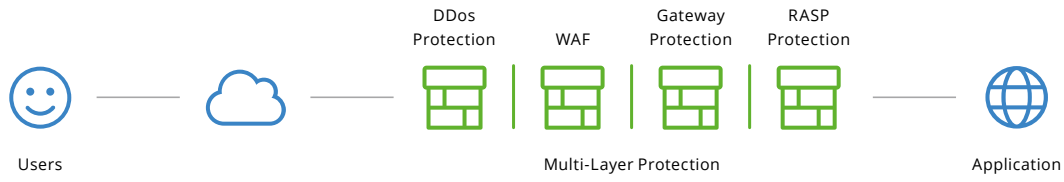
DJI provides a variety of cloud services for consumer users and enterprise-level users, which store user-specific data only with consent.

DJI has formulated "Personal Data Protection Specifications" according to corresponding laws and regulations in order to regulate the data storage of every application. Personal data such as name, email, geographical location, and flight records will be encrypted using AES-256-CBC to ensure all data is confidential.

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

Figure 6: Multi-layer security



DJI-SERVICE

DJI-Service provides most of the back end interfaces for all of DJI GO Apps, including device activation service, services like geographic location information and flight record queries. The data processed by DJI-Service are shown in the table below.

All data is stored on DJI-controlled servers (provided by cloud service companies: AWS and Alibaba) and will not be synchronized with or sent to any other third-party companies.

If a user wants to delete all the data on DJI-Service, one can contact at **support@dji.com** For more details, please refer to the DJI privacy policy: **www.dji.com/policy**

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 GO app. 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. This data will be synchronized by Alibaba Cloud's Data Transfer Service (DTS), to ensure the data of each server in the world is consistent.
- User-uploaded images and videos: This data includes the photos and videos that users upload to DJI Skypixel. Data uploaded by users outside of China is not synchronized to China.

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

User Info	**Corresponding function**
Device SN	Used for equipment activation, unlocking No-Fly Zones, DJI Care, and other services. It is authorized by the user when installing certain DJI apps.
Phone number (Mainland China only)	According to Chinese regulatory requirements, users in Mainland China need to provide telephone numbers for real-name authentication. This is not required in other regions.
Email address (non-Mainland China regions)	An email address is required when using DJI Service in non-Mainland China regions.
Country code	Current user's country code will be obtained and identified by the user's IP address.
Flight record	Users can transfer their flight records among their DJI devices.
User experience information	This information is collected by the app and used for product improvement. Please refer to the Application Security section for more details.

User-uploaded content can be accessed only by specified authorized employees (i.e., operations administrator and content viewer). The purpose of this is to verify that published content complies with our policies (i.e., no pornographic or violent images) and this data is not accessible to unauthorized employees. 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 display 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** For more details, please refer to the DJI privacy policy: **www.dji.com/policy**

DJI FLIGHTHUB

DJI FlightHub is a cloud management platform for enterprise users. It mainly includes real-time monitoring, route planning, data statistics, and personnel / equipment management. The data involved in communication between DJI FlightHub and the app includes the following:

- The drone's on-screen display data: flying control SN, user information, latitude, longitude, speed, altitude, yaw angle, the team to which the drone belongs, motor status, camera availability, and video recording availability, real-time power, battery information, and route information;
- Video and video transmission information, file information, etc.

The above data will be uploaded and stored with the user's consent. HTTPS and WSS-encrypted communication are supported during the communication process. For the video streaming information, an anti-theft chain setting is also supported.

DJI FlightHub supports two deployment methods: public deployment and private deployment. There are three versions: basic, advanced, and a government and enterprise version, providing different levels of functionality. The government and enterprise version supports private deployment, while the other two versions only support public deployment.

DJI FlightHub Public Cloud

For the public cloud version of DJI FlightHub, the corresponding app is DJI Pilot and the default setting is that the pilot will not connect to DJI FlightHub automatically. Instead, the user must authorize the connection. If there is no user authorization, no data will be uploaded to the DJI FlightHub cloud. Users can also use DJI Pilot's Local Data Mode (LDM). When this mode is switched on, no information will be uploaded. If users need to delete uploaded data, they can do so by deleting the corresponding record on the Statistical Analysis page. The public cloud is deployed and managed on independent third-party servers, so data does not interact with each other. For example, the public cloud in China is deployed on servers in China, whereas the public cloud in the US is deployed in the US. By this design, the Chinese and US cloud do not interact with each other, nor do their respective servers.

DJI FlightHub Private Cloud

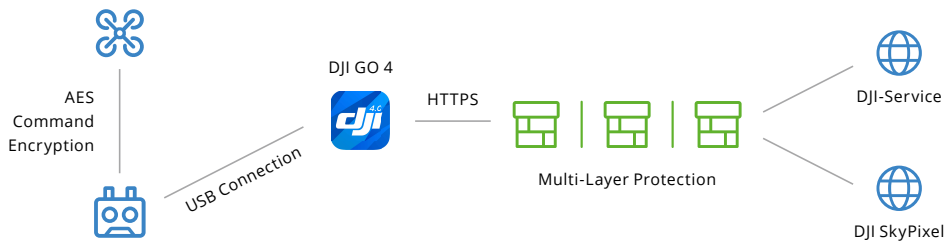
DJI provides an installer for DJI FlightHub and the user deploys the service on their own server. The corresponding app is DJI Pilot PE (Private Edition). The user needs to configure the address of the self-built DJI FlightHub private cloud server in the app. All of the data will be uploaded only to the user's own server address when the user enables the data synchronization option. In addition, the private cloud version of the app does not interoperate with the public cloud version and there is no data interaction between these two versions.

DRONE SECURITY SOLUTIONS

CONSUMER-GRADE SECURITY SOLUTIONS

DJI provides multiple consumer-grade drone platforms, such as Phantom, Mavic Pro, and Mavic 2, software like DJI GO and corresponding cloud services. The DJI consumer-grade drone security solutions implement comprehensive security features for different components in the system. These features include trusted execution environment (TEE), secure updates, secure communication, and log export encryption for devices. Additionally, these is application hardening, privacy protection for applications, and multi-layer application protection for Cloud services. This comprehensive security solution creates a complete defense-in-depth system from the device to the cloud, resulting in the security of the drone system and data. Figure 7

Figure 7: Consumer-Grade Security Solutions



ENTERPRISE-GRADE SECURITY SOLUTIONS

DJI offers different enterprise drone platforms such as the Matrice 200 V2 and Mavic 2 Enterprise, as well as different enterprise-grade application such as DJI Pilot, DJI Pilot PE and corresponding cloud services. In addition to the standard security features of consumer-grade security solutions, DJI enterprise-grade security solutions support security features required by industrial users such as secure communication, video transmission encryption and device password protection for Mavic 2 Enterprise, unlocking No-Fly Zones for certain devices, LDM (optional) for applications, and cloud-based DJI FlightHub services. Figure 8

GOVERNMENT-GRADE SECURITY SOLUTIONS

DJI offers two versions of drone platforms for governments, the Matrice 600 Pro GE and Mavic Pro GE, as well as the DJI Pilot GE app and corresponding cloud services. The main supported system security features for the device include: no flight log, ability to unlock No-Fly Zones, secure communication (with the Wi-Fi function off for Mavic Pro GE), and device isolation (when the government version of the drone and remote controller cannot communicate or connect with the consumer-grade or enterprise-grade versions of the aircraft and remote controller).

For the app, features include LDM mode (enabled by default), offline updates, firmware isolation (when the government version of drones and remote controllers cannot be upgraded to the consumer-grade or enterprise-grade version of the officially released firmware), software isolation (the government version of the drone cannot use the consumer-grade or enterprise-grade version of DJI software). For the cloud, DJI FlightHub privatization deployment is supported. DJI government-grade security solutions eliminate the possibility of connecting to public network through communication blocking, device isolation, and cloud service privatization deployment, meeting the needs of users with high security requirements. Figure 9

Figure 8: Enterprise-Grade Security Solutions

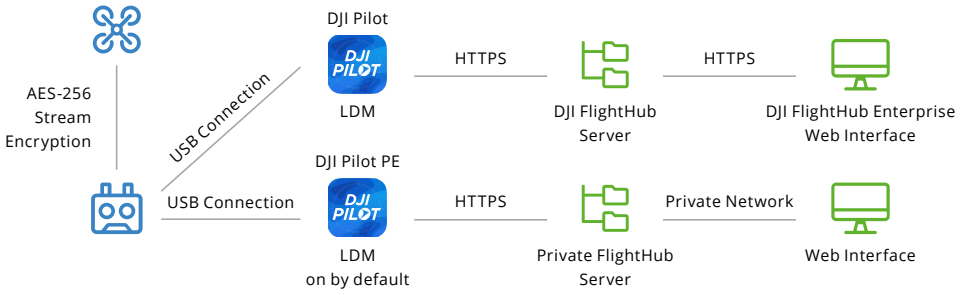
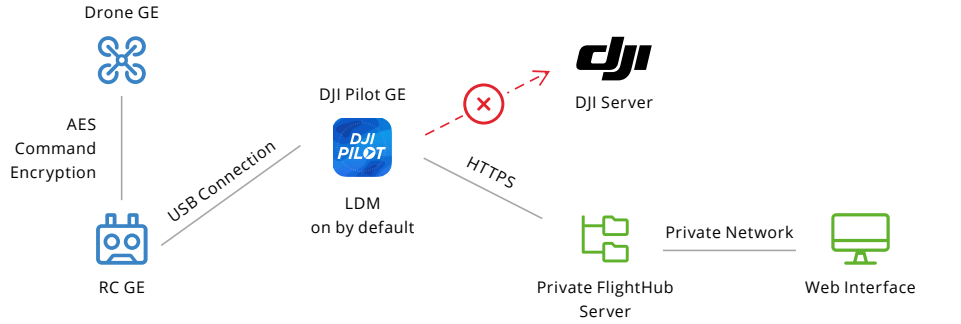


Figure 9: Government-Grade Security Solutions



DRONE SECURITY SOLUTION COMPARISON

	Security Features	Consumer-Grade	Enterprise-Grade	Government-Grade
Standard Solution		Mavic 2 + DJI GO	Mavic 2 Enterprise + DJI Pilot + DJI FlightHub Enterprise Edition	Mavic Pro GE + DJI Pilot GE + DJI FlightHub Government Edition
Device	Trusted Execution Environment	✓	✓	✓
	Secure Boot	✓	✓	✓
	Security Update	✓	✓	✓
	Secure Communication	✓	✓	✓
	Log Export Encryption	✓	✓	No Flight Records
	Device Password Protection		✓	In Development
	Unlock No-Fly Zone		✓	✓
	No Flight Records			✓
	Device Isolation			✓
App	Application Hardening	✓	✓	✓
	Secure Communication Via HTTPS	✓	✓	✓
	Local Data Encryption	✓	✓	✓
	LDM Mode		✓	✓
	Software Isolation			✓
	Offline Upgrade			✓
	Firmware Isolation			✓
Cloud	Multi-Layer Cloud Security Protection	✓	✓	User-defined
	Personal Data Encryption	✓	✓	User-defined
	DJI FlightHub Privatization		✓	✓

GEOFENCE SECURITY PROGRAM

The DJI geofence system includes a flight restriction system and an unlocking system. The flight restriction system intends to restrict drones from flying in certain areas to ensure flight safety. The unlocking system removes the flight restriction partially when the user gets approval from the civil aviation agencies or other air space flight control agencies to operate in the restricted area. These two features are secured by the system security.

FLIGHT RESTRICTION SYSTEM PROTECTION

The flight restriction system includes a No-Fly Zone database and flight control functions. The No-Fly Zone database stores geographic coordinate information, such as No-Fly Zones (e.g. airports), authorized zones, and zones with height limitations. The fight control function decides whether the drone can fly into a specific area and whether to apply certain restriction policies based on the GPS information of the drone and the No-Fly Zone database.

To maintain a consistently reliable geofence system, the No-Fly 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 GPS information from the GPS module on the aircraft and the database stored in the aircraft, does not require networking, and does not upload the user's GPS information. The GPS information sent from the GPS module is signed to prevent man-in-the-middle attacks and GPS 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 No-Fly Zone database in this area.

UNLOCKING SYSTEM PROTECTION

When necessary, a user can apply to unlock a No-Fly 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 GPS coordinates and Device SN to determine whether to unlock the flight restriction.

For more information on flysafe, please refer to the following link for more information:
www.dji.com/flysafe

SECURITY AUDIT

DOI SECURITY AUDIT

The US Department of the Interior (DOI) conducted thorough tests and evaluations on the DJI government-grade version of drones.

Learn more about this report **here**.

DJI FLIGHTHUB SOC2 AUDIT

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

If you wish to read the certification report, contact the DJI after-sales department.

KIVU SECURITY AUDIT

Kivu is a US based third-party independent agency. In 2018, DJI released KIVU's independent report, which reviewed DJI's data practices and concluded that DJI is capable of protecting users' personal data.

Learn more about this report **here**.

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 faults 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 2020, 107 information security experts have submitted 221 reports regarding possible vulnerabilities within our platforms. Each report has been carefully reviewed and evaluated by our team. We have also taken the time to resolve 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$ 80,700 in cash and DJI credits has been awarded to security experts.

Drones have provided tremendous changes and benefits to various industries. However, drone security will be an ongoing challenge. Moving forward, we look forward to strengthening our collaborative efforts with the broader data security research community.

If this is something that interests you, contact us at **bugbounty@dji.com**

If you would like to know more about the Bug Bounty Program, visit **security.dji.com**

DJI PRIVACY POLICY

DJI has explicit policies regarding user 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**

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.

DJI welcomes your input on how to continue enhancing and improving data protection.

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

GLOSSARY

Abbreviations	Full name
AES	Advanced Encryption Standard
API	Application Programming Interface
APP	Application
AWS	Amazon Web Services
CBC	Cipher Block Chaining
DDOS	Distributed denial-of-service attack
DM-Verity	Device Mapper Verity
DOI	U.S. Department of the Interior
DTS	Data Transfer Service
ECC	Elliptic Curve Cryptography
ELF	Executable and Linkable
GE	Government Edition
HTTPS	Hypertext Transfer Protocol Secure
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
LAN	Local Area Network
LDM	Local Data Mode
MSDK	Mobile Software Development Kit
NFZ	No-Fly Zone

Abbreviations	Full name
OSDK	Onboard Software Development Kit
OTP	One Time Program
PE	Private Edition
PSDK	Payload Software Development Kit
RASP	Runtime application self-protection
RC	Remote controller
ROM	Read only memory
RSA	Rivest-Shamir-Adleman
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 Disk
TEE	Trusted Execution Environment
WAF	Web Application Firewall
WPA	Wi-Fi Protected Access
WSS	WebSockets over SSL/TLS

security.dji.com/data