White Paper – The Drone Use-Case

# Seal SQ
# IoT End-to-End Security

## ANAFI Ai
## The 4G Robotic UAV

*The following pages are an extract of PARROT's white paper, highlighting the advanced security features of the ANAFI Ai drone. These features are the result of an extensive collaboration with SEAL SQ and are powered by its Vault-IC series secure element, FIPS 140-2 and Common Criteria CCEAL5+ Certified.*
*A State-of-the-art example of end-to-end device security, implemented by SEAL SQ as the result of over 20 years hardware security, device provisioning, and PKI experience.*

## Cybersecurity by design

### Key features

- Zero data shared without user consent
- FIPS140-2 compliant and CC EAL5+ certified Secure Elements
- Strong authentication for 4G
- Digitally signed pictures
- Transparency and Bug bounty continuous security check

### No data shared by default

Parrot collects no data without the consent of the users. The user can decide whether he shares data to Parrot infrastructure or not. Data hosted by Parrot enables the user to synchronize flight data and flight plans between different devices, eases support and allows Parrot to enhance products.

ANAFI Ai is compliant with the European Union General Data Protection Regulation (GDPR) and goes beyond, for example with a 1-Click deletion of all data so that users keep control very easily. It's a matter of 1-Click in the FreeFlight7 mobile App or in the privacy settings of their Parrot.Cloud account. Thus, users may not only stop sharing data at any time, but they can also ask for data deletion very easily.

When the user consents to share data, data processing is fully transparent and described in the Parrot Privacy Policy.

When ANAFI Ai is connected to the Skycontroller 4 through 4G, Parrot infrastructure is used to pair

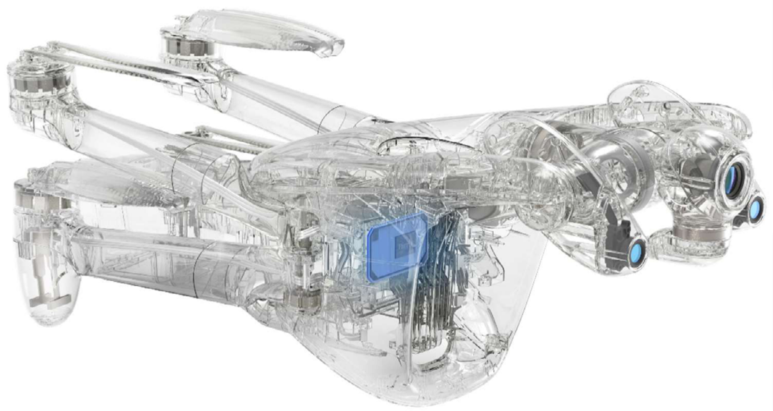
the drone and the remote controller. If the user is not authenticated by the Parrot. Cloud account, he can still use 4G with a unique temporary account. When using Parrot infrastructure for 4G pairing, video is encrypted with a key negotiated between the drone and remote controller, Parrot has no access to unencrypted videos.

## FIPS140-2 compliant and CC EAL5+ certified Secure Element

ANAFI Ai embeds a SEAL SQ Secure Element which is NIST FIPS140-2 Level 3 compliant and Common Criteria EAL5+ certified. A similar Secure Element is also embedded on the Skycontroller 4.

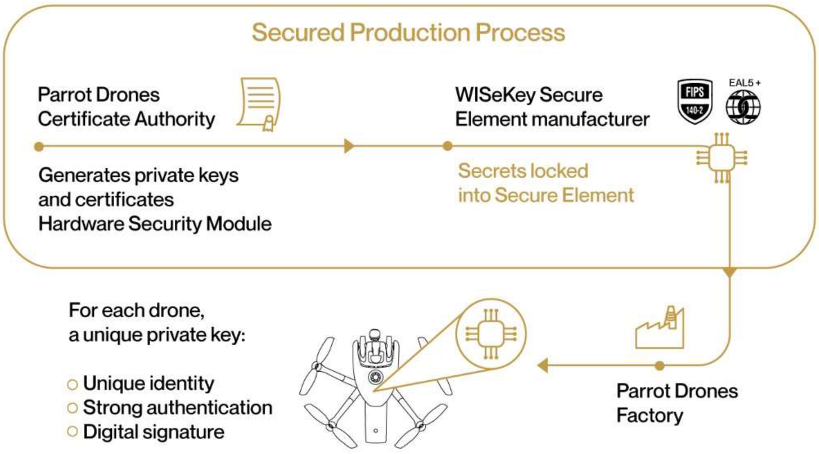
The Secure Element:

- performs cryptographic operations
- stores and protects sensitive information



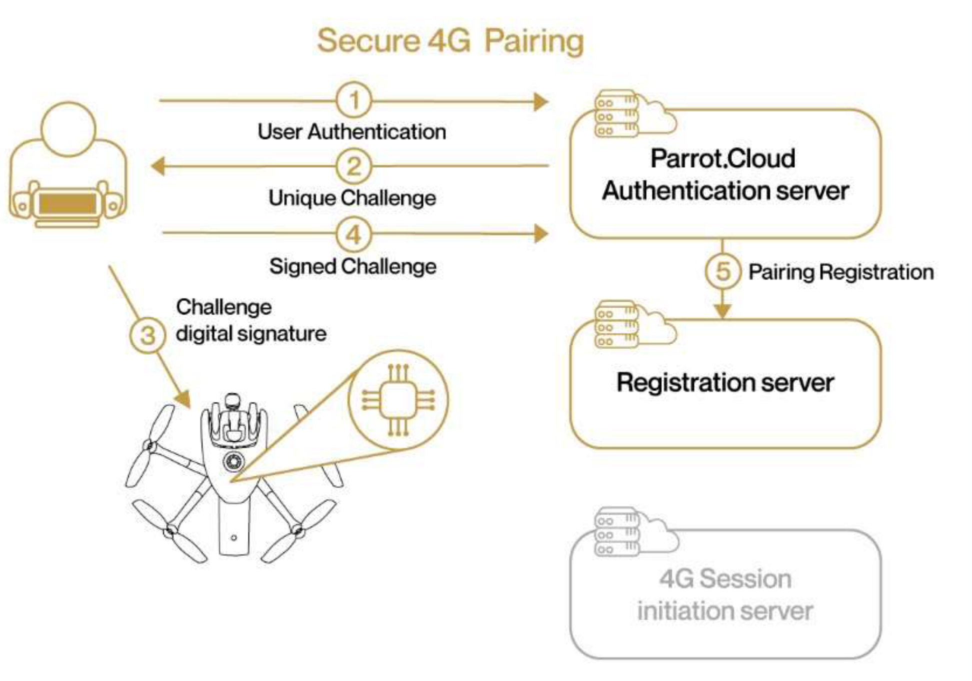
It features an ECDSA private key, with P521 domain parameters, unique to each drone. This private key cannot be extracted from the Secure Element. The certificate associated to this key is signed by a certification authority.

The Secure Element protects the integrity of the embedded software, provides a unique identity to the drone for 4G pairing and strong authentication, and features a unique digital signing of the pictures taken by the drone.

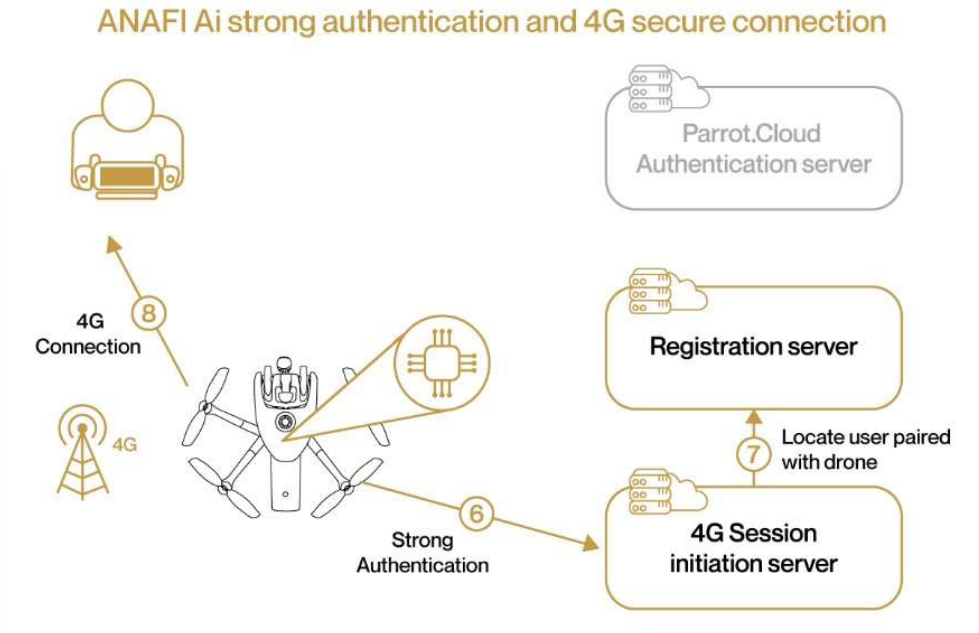


## 4G secure pairing and strong authentication

When a user enables 4G communication, the initial Wi-Fi connection is first used for a secure pairing process. During this process, the user securely proves he is connected to a specific drone. Thanks to ANAFI Ai Secure Element, he can do so without configuring any password inside the drone.



Then, Parrot servers register the association between the user and the drone. When Wi-Fi connection between the user and the drone is lost, ANAFI Ai automatically connects in 4G. ANAFI Ai does a strong authentication on Parrot servers, using its private key stored on the Secure Element. Parrot servers look for the associated users and enables pairing between ANAFI Ai and the Skycontroller 4.


ANAFI Ai strong authentication and 4G secure connection
Parrot.Cloud Authentication server
Registration server
4G Connection
8
4G
Locate user paired with drone
7
6
Strong Authentication
4G Session initiation server

With 4G, ANAFI Ai performs a strong authentication to log in to Parrot servers. This strong authentication implies a client certificate and a unique private ANAFI Ai key, stored in the Secure Element. ANAFI Ai supports TLS, DTLS and SRTP protocols, to protect drone control and video streams to the Skycontroller 4.

## Secure initialization and update

The drone's boot sequence is secured: the system checks that it uses Parrot software, and that this software has not been tampered with. A security check is performed at each initialization. The update service also controls the digital signature of software updates.

## Configuring user keys on the Secure Element

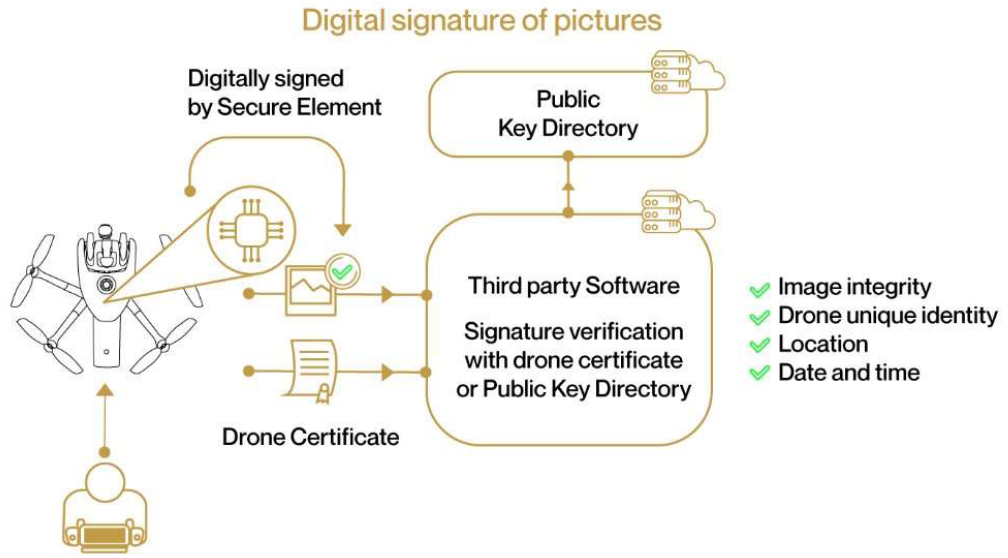
ANAFI Ai users have access to a dedicated operator account of the drone's Secure Element. This account is used to configure keys specific to the user. Users can configure into the Secure Element the

public keys of the flight mission providers they choose to trust. ANAFI Ai will only run flight missions which are numerically signed with these keys. This process prevents an attacker from running malicious flight missions on the drone.

## Digitally signed pictures

ANAFI Ai's Secure Element can digitally sign the pictures taken by the drone. This signature provides a proof that:

- said signed picture has been taken by said drone
- neither the picture itself nor its metadata have been tempered with (voluntarily or not) – metadata, also known as EXIF and XMP, contain information about the date, time, and location of the picture


Digital signature of pictures
Digitally signed by Secure Element
Public Key Directory
Third party Software
Signature verification with drone certificate or Public Key Directory
Drone Certificate
✓ Image integrity
✓ Drone unique identity
✓ Location
✓ Date and time

In other words, the digital signature secures all data relevant to a picture, including the place where and the time when it was taken, and by which ANAFI Ai drone.
Users as well as partners proposing software solutions exploiting drone photographs can verify the digital signature of ANAFI Ai photos, either using the drone's certificate, or through a public key directory, provided by Parrot.

## Transparency and Bug bounty continuous security check

Whenever possible, Parrot uses standard protocol and file formats. There is no obfuscated code, nor hidden features. It allows the user to understand how Parrot products works and check their security. In addition, OpenFlight - the software used to control the drone - is Open Source: then, the users benefit from full control.

Back in April 2021, Parrot has launched a “Bug Bounty” program together with YesWeHack, the first European crowdsourced security platform. Through this partnership, Parrot benefits from YesWeHack’s vast community of cybersecurity researchers to identify potential vulnerabilities in its drones, mobile applications and WebServices.

The Bug Bounty program takes place in two phases:

- The private programs initially gives exclusive access to selected security researchers and includes future Parrot drone models. The expertise and diverse skills of the researchers will confirm the high level of security of the products before they are marketed, for the greater benefit of Parrot users’ security and the protection of their data.
- After this first phase in a private Bug Bounty program, and after being commercialized, the products enters a public program. Their security is then scrutinized by the entire YesWeHack community, representing more than 22,000 cybersecurity researchers.