	TQ Cert Services Private Limited	Document no: UAS-WI01	
	Certification Scheme for Unmanned Aircraft Systems (UAS)	Rev No:00	Dt: 01-02-2022
	Flight Module Compliance Levels	Page 1 of 1	

The firmware and hardware of the certified UAS should not be modified after certification. Automated methods to check if the UAS is operating with certified software, firmware and hardware are needed.

These checks would be carried out by a submodule of the Flight module. Depending on the way in which these checks are implemented, we have two levels of assurance: Level 0 and Level 1.

One can call the Flight module to be level 0 compliant if the checking process is carried out by software on the host system. For the higher level 1, the checking process is carried out in a more secure trusted execution environment. A more elaborate description is given below:

1. Level 0 Compliance

The Flight Module security implementation has Level 0 compliance if the signing and encryption is implemented within the software zone at host system level. In this case, management of private keys needs to be addressed carefully to ensure it is protected from access by users or external applications. All device providers should at a minimum obtain level 0 compliance and should not have mechanism to easily obtain the private key or inject fraudulent flight logs.

2. Level 1 Compliance

The Flight Module security implementation has Level 1 compliance if the signing and encryption is implemented within the Trusted Execution Environment (TEE) where host system processes or host system users do not have any mechanism to obtain the private key or inject fraudulent flight logs. In this case, management of private keys needs to be fully within the TEE.

3. Communication requirement for multiple module design of FM

If the flight controller and companion computer are in separate modules, the modules constituting Flight Module will have same compliance requirements (Level 0/Level 1) as a single module plus the communication between modules has to be secured using (or equivalent of) 128bit symmetric key encryption (minimum).

4. Generation of Keys for Flight Module

The key pairs used for signing and verification by Flight module are to be generated and stored securely.

i. Key pair is generated at FM level or generated elsewhere and transported to FM.

ii. If key pair is not generated at FM, it should be generated within a zone that has the same security requirements as FM and has to be transported to the FM on a communication channel secured using (or equivalent of) 128 bit symmetric key encryption (minimum).

iii. The FM public key would be signed by the Flight Module Provider using a public key obtained from a valid CA (for Digital Certificates) in India.

iv. If key rotation is required, the newly generated key may be signed using previous key pair.