GOVERNMENT OF INDIA
OFFICE OF THE DIRECTOR GENERAL OF CIVIL AVIATION
OPP. SAFDURJUNG AIRPORT, NEW DELHI

DGCA RPAS Guidance Manual

Approved by the Director General of Civil Aviation

Revision 1 - 2019

Record of Revision

No.	Date	Pages	Remarks
0	9th November, 2018	Page 1 to 57	First Edition
1	3rd June, 2019	Pages 1-4, 30-31, 33, 38-39, 41, 46, 48, 50, 54-64	Revision 1

Table of Contents

Introduction

The objective of this Manual is to acquaint the public and the industry with the procedures being followed for processing all matter pertaining to issue of unique identification number, unmanned aircraft operator permit, and related activities. It will help them understand the flow of various processes involved and understand the intricacies of the system.

It has been our endeavour to place the details of the procedures to be followed by DGCA in a cogent and easily understandable manner. Therefore, the language used is simple and unnecessary details have been avoided. In order to make the reader comfortable, the references to various legislations and documents have been kept at the bare minimum.

(Arun Kumar)
Director General

Acronyms

AAI	Airports Authority of India
ADC	Air Defence Clearance
ADS-B	Automatic Dependent Surveillance - Broadcast
AGL	Above Ground Level
AIP	Aeronautical Information Publication
ATC	Air Traffic Control
ATS	Air Traffic Service
ARC	Aviation Research Centre
ARP	Aerodrome Reference Point (published in AIP)
BCAS	Bureau of Civil Aviation Security
CAR	Civil Aviation Requirements
DGCA	Directorate General of Civil Aviation
DGFT	Directorate General of Foreign Trade
DIPP	Department of Industrial Policy & Promotion
FIR	Flight Information Region
FRTOL	Flight Radio Telephone Operator's License
FTO	Flying Training Organization
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IAF	Indian Air Force
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
IPC	Indian Penal Code
MHA	Ministry of Home Affairs
MoCA	Ministry of Civil Aviation
MoD	Ministry of Defence
NOTAM	Notice to Airmen
NPNT	No Permission-No Takeoff
NTRO	National Technical Research Organization
PPL	Private Pilot License
RF-ID	Radio Frequency Identification
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System(s)
RPS	Remote Pilot Station(s)
SARPs	Standards and Recommended Practices
SIM	Subscriber Identity Module
TSA	Temporary Segregated Areas
TRA	Temporary Reserved Areas
UA	Unmanned Aircraft
UAOP	Unmanned Aircraft Operator Permit
UAS	Unmanned Aircraft System(s)
UIN	Unique Identification Number
VFR	Visual Flight Rules
VLOS	Visual Line-Of-Sight
VMC	Visual Meteorological Conditions
WPC	Wireless Planning and Coordination Wing, DoT

Chapter 1

Acquisition of RPAS

1. Civil RPA is categorized in accordance with Max. All-Up-Weight (including payload) as indicated below:

(i).	Nano	:	Less than or equal to 250 grams.
(ii).	Micro	:	Greater than 250 grams and less than or equal to 2 kg.
(iii).	Small	:	Greater than 2 kg and less than or equal to 25 kg.
(iv).	Medium	:	Greater than 25 kg and less than or equal to 150 kg.
(v).	Large	:	Greater than 150 kg.

2. For Imported RPA:

a) The importer or seller or manufacturer of RPAs should obtain Equipment Type Approval (ETA) from WPC Wing, Department of Telecommunication that drone is working in de-licensed frequency band(s). Such approval shall be valid for a particular make and model.

b) The applicant (other than Nano category) should apply to DGCA for import clearance through Digital Sky Platform.

c) The officer responsible should verify the documents submitted for its correctness and should issue import clearance if found satisfactory. Else, he should reject the application with reason(s).

d) Subsequent to receipt of import clearance from DGCA, the applicant should approach DGFT (all categories) for import license.

e) Only after receipt of import license, the applicant can import the RPAS into India.

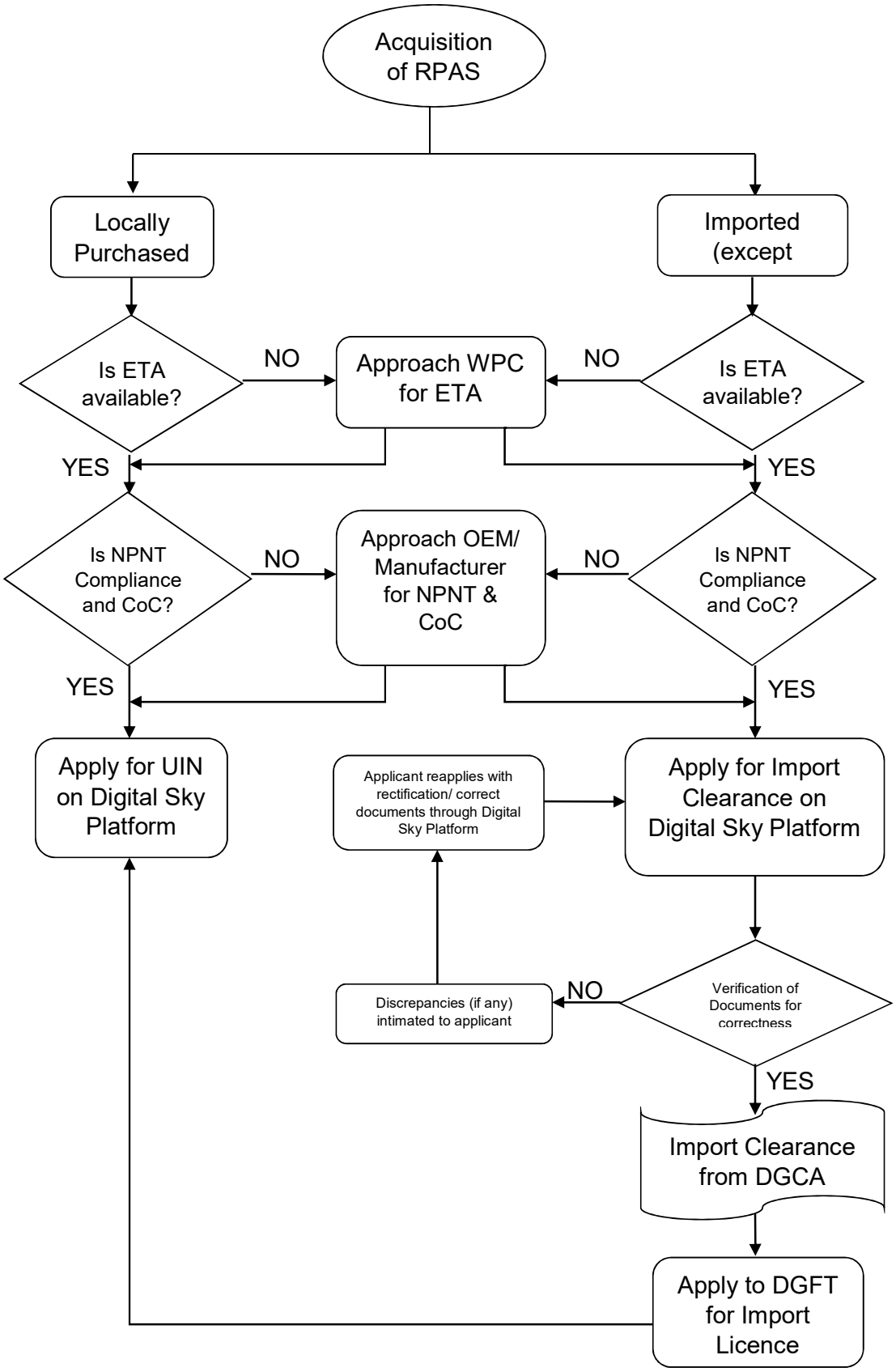
3. For locally purchased RPA:

a) The applicant should ensure that locally purchased RPA has ETA from WPC Wing, DoT for operating in de-licensed frequency band(s). Such approval shall be valid for a particular make and model.

b) The applicant should submit information as per format given in Digital Sky Platform along with application for issue of UIN.

Note: Refer Digital Sky Platform Manual for application filling instructions

Acquisition of RPAS- Flow Chart



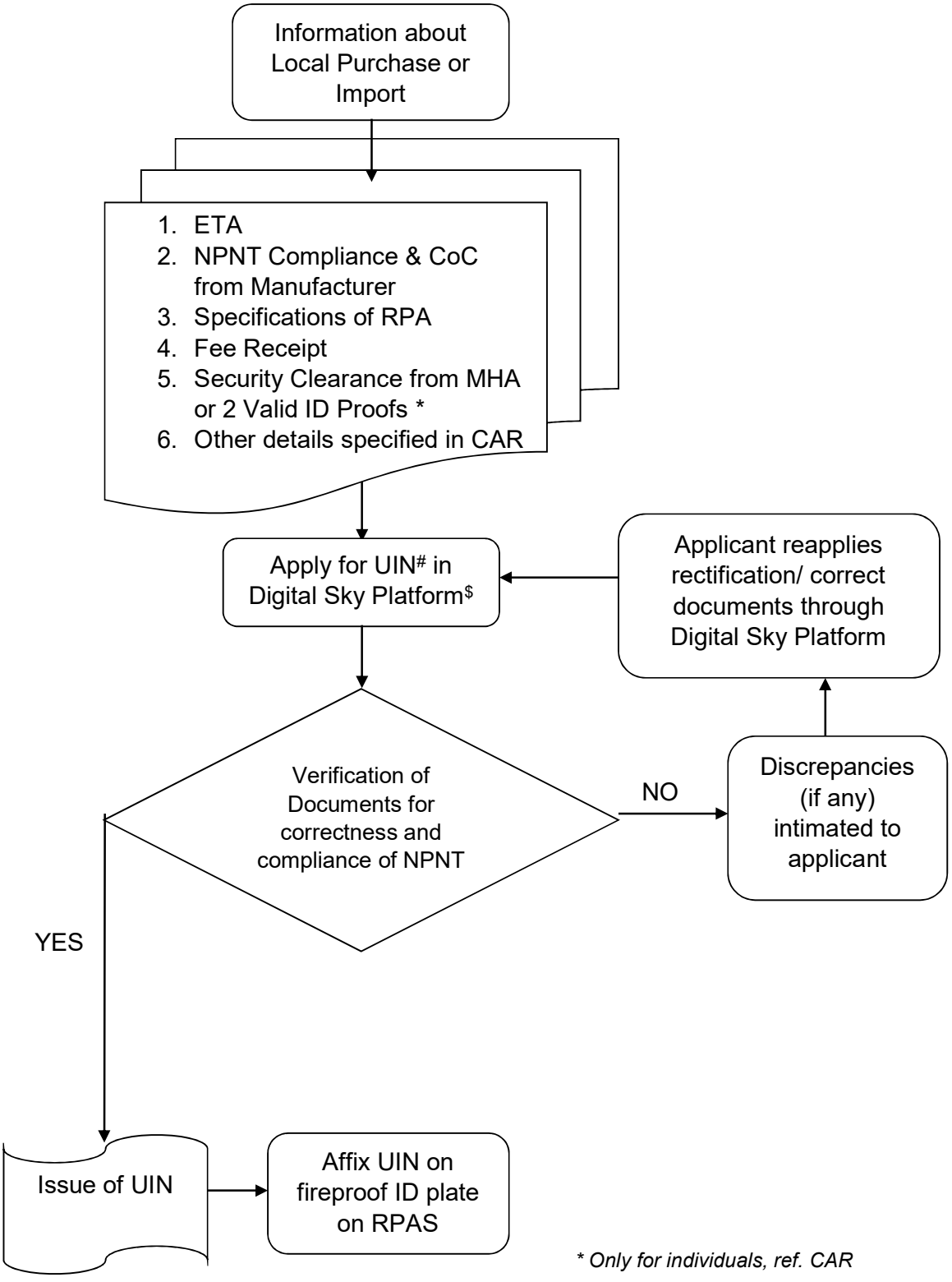
Chapter 2

Unique Identification Number (UIN)

1. Except Nano (flying up to 50ft. in uncontrolled / enclosed premises) and RPA owned by NTRO, ARC and Central Intelligence Agencies are required to obtain UIN.
2. Except foreign entity all others are eligible for applying for UIN.
3. For imported RPAS, ETA from WPC, Import clearance from DGCA and import license from DGFT are required before applying for UIN.
4. For locally purchased RPAS, ETA from WPC and NPNT compliance certificate from OEM is required before applying for UIN.
5. Filled Application for UIN with requisite supporting documents and fee of Rs. 1000/- should be submitted through Digital sky platform.
    - Supporting Documents:-
        a) Equipment Type Approval (ETA) from WPC Wing
        b) OEM Certificate
        c) Security documents from MHA or copies of any 2 IDs (Passport, Driving License, Aadhar)
        d) Specification of UAS & applicable Manuals.
        e) Any other supporting documents deemed necessary
6. The officer responsible should verify the documents submitted for its correctness. If found satisfactory, UIN will be issued by DGCA through Digital sky platform. Else, he should reject the application with reason(s).
7. The applicant should inscribe Fire resistant identification plate with UIN affixed on RPAS.
8. The RPAS (issued with UIN) shall not be sold or disposed-off in any way to any person or firm without permission from DGCA.
9. In case, the RPA is damaged and cannot be restored to original condition, the same shall be notified to DGCA by the owner/ operator for cancellation of UIN.
10. Any changes in the contact details specified in UIN shall be immediately notified to DGCA and all other concerned agencies.

Note: Refer Digital Sky Platform Manual for application filling instructions

UIN Application Flow Chart



** Only for individuals, ref. CAR*

 # except Nano

$ Refer Digital Sky Platform Manual for application filling instructions

Chapter 3

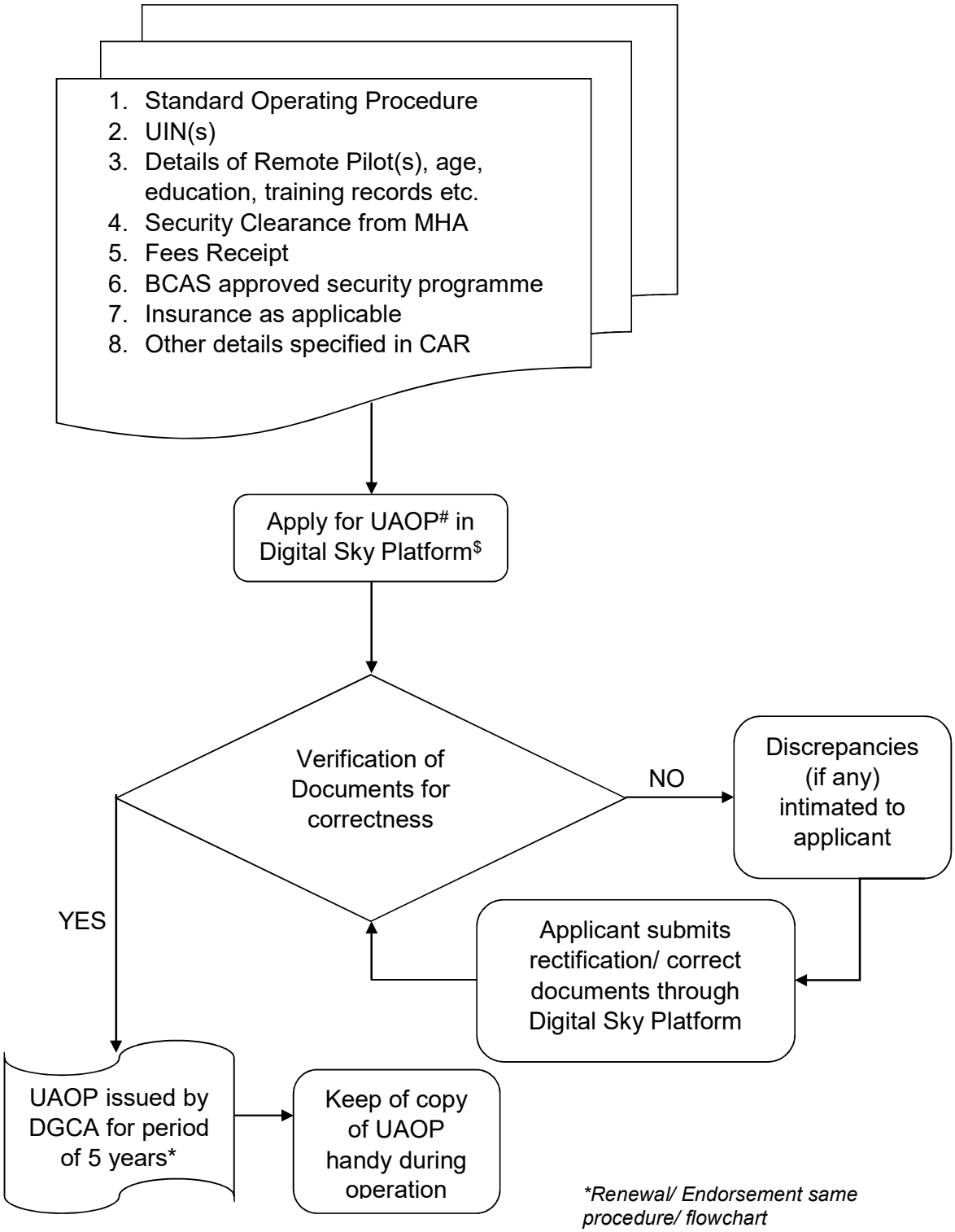
Unmanned Aircraft Operator Permit (UAOP)

1. The following entities will not require UAOP:
    a) Nano RPA operating below 50 feet (15 m) AGL in uncontrolled airspace / enclosed premises.
    b) Micro RPA operating below 200 feet (60 m) AGL in uncontrolled airspace / enclosed premises.
    c) RPA owned and operated by the NTRO, ARC and Central Intelligence agencies.
2. After obtaining UIN , the eligible applicant should apply for UAOP through Digital Sky platform along with following supporting documents and requisite fees * (at least 7 working days prior to actual commencement of operations) :
    (i). Standard Operating Procedure
    (ii). Permission of the land/property owner (only for area used for take-off and landing of RPA);
    (iii). Details of remote pilot(s) along with security clearance from MHA or self-attested copies of at least two out of three valid identity proofs viz. Passport, Driving License/ Pilot License or Aadhar Card and copies of training records.;
    (iv). Insurance details (as applicable);
    (v). Security programme as approved by BCAS.

    *** Fees for UAOP of Rs 25,000/- to be deposited in Bharatkosh link *https://bharatkosh.gov.in/* and applicant should upload the generated receipt along with application.**
3. After satisfactory vetting of submitted documents and fees, UAOP shall be issued by DGCA through digital sky platform. A copy of the UAOP will be provided to MHA, BCAS, IAF, ATS Provider (AAI / MoD), and district administration (Superintendent of Police) for information.
4. For a company or corporation registered elsewhere than in India, UAOP will be issued to the Indian company that has taken RPAS on lease.
5. The UAOP are not transferrable and its validity will be for a period of five years from the date of issue.
6. For renewal of the UAOP same procedure will be followed and the applicant has to submit fresh security clearance from MHA. The fee for renewal of UAOP is Rs.10,000/-.

Note: Refer Digital Sky Platform Manual for application filling instructions

UAOP Application/ Renewal* Flow Chart



**Renewal/ Endorsement same procedure/ flowchart*

 # Check for exemption criteria

$ Refer Digital Sky Platform Manual for application filling instructions

Chapter 4

RPAS Operation

1. Refer AIP supplement on RPAS published by AAI.

Chapter 5

Remote Pilot & Training

1. A remote pilot is a person charged by the operator with duties essential to the operation of a remotely piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.

2. Remote pilot should have attained 18 years of age.

3. Remote pilot should have passed at least 10^{th} exam in English.

4. A remote pilot should either obtain security clearance from MHA or submit self-attested copies of at least two out of three valid identity proofs viz. Passport, Driving License or Aadhar Card.

5. In case of foreign remote pilots employed by Indian entity as per para 6.1 (b), (c), and (d) of CAR Section 3, Series X, Part I, DGCA shall forward documents for Security clearance to security agencies in accordance with the procedure being followed for Foreign Aircrew Temporary Authorization (FATA) pilots.

6. Remote Pilot training is not applicable for Nano and Micro category RPA pilots intending to operate in uncontrolled airspace. However, the owner and user should be fully aware of responsibilities for all aspects of flight safety during such operations.

7. The remote pilot should have undergone ground/ practical training at any DGCA approved Flying Training Organization (FTO).

8. The theory subjects should have follow topics:

   a) Basic Radio Telephony (RT) techniques including knowledge of radio frequencies.
   b) Flight Planning and ATC procedures.
   c) Regulations specific to area of operations.
   d) Basic knowledge of principles of flight and aerodynamics for fixed wing, rotary wing, and hybrid aircraft.
   e) Airspace Structure and Airspace Restrictions with knowledge of No Drone Zones
   f) Basic Aviation Meteorology.

9. The practical training should comprise of RPA in flight having live component, and/ or simulated flight training to demonstrate control of RPA throughout its operating conditions, including safe recovery during emergencies and system malfunction.

10. Details of DGCA approved Flying Training Organisations (FTO) available in DGCA website. List of FTOs conducting remote pilot training will be available on Digital sky Platform.

11. The training records should be maintained by FTOs that is imparting the training.

12. Copy of training records and Remote Pilot logbook should be maintained and available with the remote pilot.

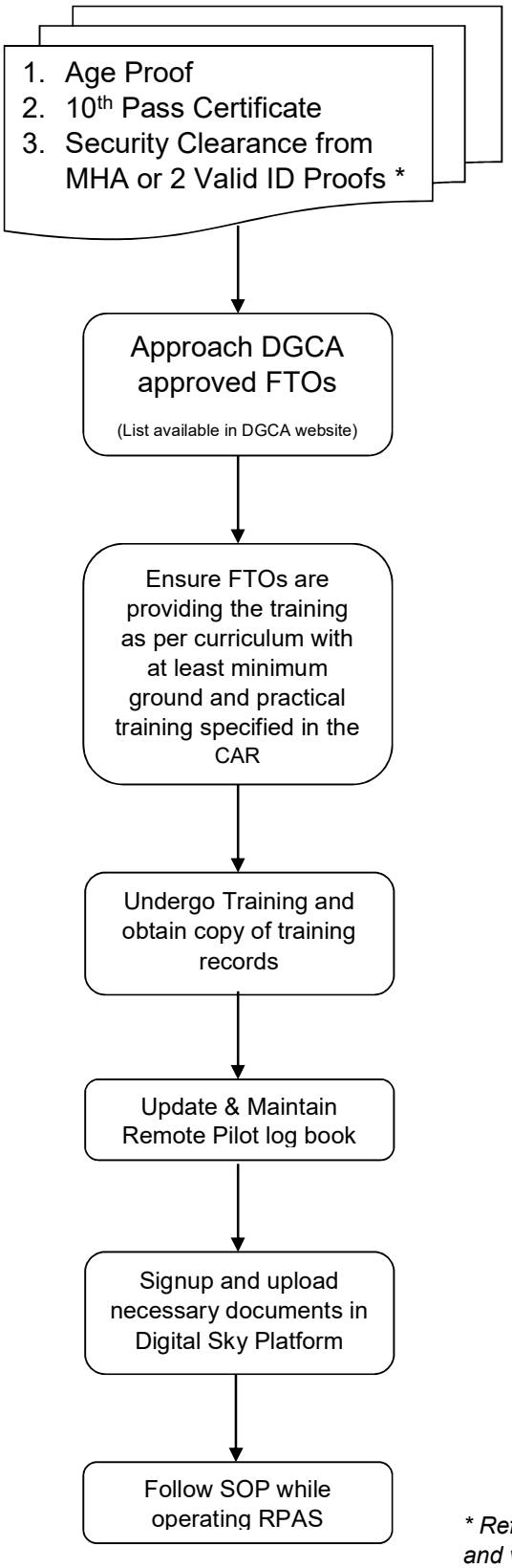
13. The remote pilot should ensure he has necessary permission(s)/ clearance(s). He should carry out pre-flight inspection. He should not fly the RPA unless he/ she is reasonably satisfied that all the control systems of RPA including the radio and Command & Control link are in working condition before the flight.

14. Remote pilot should be equipped with communication facilities to establish two way communication with the concerned ATS unit. He should establish and maintain contact with ATC prior to entering the controlled airspace.

15. Remote pilots should prefix RPA call-sign with the word UNMANNED whenever is required to have voice communications with ATC. He should also that no Radio Frequency Interference (RFI) is caused to air traffic operations and air navigation equipment.

16. The remote pilot should ensure that privacy norms of any entity are not compromised in any manner.

Remote Pilot Training Flow Chart



** Refer CAR for exemption criteria and valid IDs*

Chapter 6

Manufacturing of RPAS

1. Although Manufacturers/ OEM of RPAS are not regulated through the CAR Section 3, Series X, Part I, being a responsible entity, a manufacturer is expected to follow the procedure specified hereunder.

2. Apart from the indigenous manufacturer; the entity importing parts and assembling RPA in India (assembler) will also be considered as manufacturer.

3. A manufacturer should develop and ensure that their RPAS meets the minimum standards specified in the CAR.

4. The manufacturer should carryout necessary tests as many as required. The manufacturers may use the test sites specified in the CAR for carrying out such tests.

5. OEM/ Manufacturers may alternatively utilize unused airstrips or Government educational institutions campus, provided adequate safety precautions are in place. However, they need to ensure that no manned or unmanned aircraft is flying during such operations in the intended test area.

6. The manufacturers/ OEM of Nano RPA shall engrave/ display prominently the manufacturer's serial number on the Nano RPA. Also, they may appropriately geo-fence their nano RPA for 50ft AGL ceiling.

7. The manufacturer/ assembler of micro and above should comply with the NPNT specification provided in this document at Chapter 7.

8. If the RPA developed is a nano or micro category, the minimum standards set by manufacturer/ OEM will be considered. However, for micro category, the manufacturer should certify compliance of the NPNT, equipment and other standards specified in the CAR as per the sample given in this manual.

9. If the model developed is small or above category, the OEM/ manufacturer should use the checklist given in this chapter and get it certified by certifying agency by showing compliance to applicable standards. In addition, the manufacturer should submit certificate of compliance as per the sample given in this manual.

10. Post certification (by self or certifying agency), all models to be listed on the Digital Sky Platform with all requisite details. This will ensure the user/ operator/ Remote Pilot can pick their correct model from the list.

11. The manufacturer/ OEM may obtain ETA from WPC, DoT to facilitate the end user, as the ETA is given for particular type/ model, or lot in case of import.

12. Manufacturer should develop following manuals:
    a. RPA Flight Manual/ Manufacturer's Operating Manual specifying operating conditions/ limitations.
    b. Maintenance manual/ guidelines/ procedure
    c. Maintenance inspection schedule/ overhaul interval
    d. Self-explanatory information booklet for end users

13. The manufacturer shall provide the self-explanatory information booklet to end users in the RPAS package/box.

14. Maintenance and repair of RPAS should be carried out in accordance with the manufacturer's approved procedures in authorised service centres of the manufacturer/ OEM or remote pilot/ operator. In latter case, the OEM/ Manufacturer should ensure that remote pilot/ operator does not have unauthorised access to mandatory equipment/ firmware (including NPNT).

15. Nano RPA Manufacturers/OEMs must ensure traceability of purchaser for every drone. Their agents/distributors must collect and safely store IDs at point of sale. Manufacturers should ensure record of serial numbers at distributor/agent is maintained and kept up to date.

16. Checklist for manufacture of Small and above categories of RPAS

(Both Indian & Foreign)

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
1.	**General**			
1.1	Category of RPAS	Define as per Para 3 of CAR Section 3, Series X, Part I	Statement & design review	
1.2	Weight	a) Empty weight b) Maximum all-up-weight	To be verified by actual weighing	
1.3	Type of RPA	a) Fixed wing/rotary wing b) Launch and recovery type	Statement	
1.4	Dimensions	Wing span/max diagonal distance (rotor) (as applicable)	To be verified by actual measurement	
1.5	Life of RPA	a) Airframe b) Engine c) Battery d) Propeller/ rotor e) Number of maximum permissible landings	By design review	
2.	**Performance**			
2.1	Speeds	a) Minimum operating speed – the minimum specified operating speed of RPA at standard sea level conditions shall be at least 10% above the actual stall speed b) Determine maximum operating speed at standard sea level conditions c) Determine that maximum kinetic energy on impact does not exceed 95 KJ at any combination of mass and speed	To be demonstrated by actual test and supported by analysis To be demonstrated by actual test and supported by analysis To be demonstrated by actual test or analysis	
2.2	Range	Determine maximum range in still air	To be demonstrated by actual test or analysis	
2.3	Endurance	a) Determine fuel and oil consumption (if applicable)	To be demonstrated by actual test or analysis	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
		b) Determine rate of discharge of battery (if applicable)	To be demonstrated by actual test or analysis with charge capacity more than 85% at all times	
2.4	Operational altitude	Determine maximum attainable altitude at standard sea level conditions	To be demonstrated by actual test or analysis	
2.5	Operational envelope	Determine boundaries of operational envelope within which safe flight, in normal and emergency conditions, can be demonstrated under combinations of weight, centre of gravity, altitude, temperature and airspeed	To be demonstrated by actual test or analysis	
2.6	Ceiling height	Determine ceiling height over a range of weight, centre of gravity, altitude, temperature and airspeed	To be demonstrated by actual test or analysis	
2.7	Propeller speed and pitch for safe operation	a) Determine propeller speed and pitch limits that ensure safe operation under normal operating conditions b) Determine integrity of propeller and its mounting at maximum rpm	To be demonstrated by actual test or analysis To be demonstrated by actual test or analysis	
2.8	Stability and control	a) Determine that RPA is able to maintain a stable flight without pilot input b) Determine that pilot is able to control RPA with ease.	To be demonstrated by actual test To be demonstrated by actual test	
3.	**Powerplant**			
3.1	Powerplant (engine/ battery operated)	<u>Engine Operated</u> a) Determine that fan blade can withstand ultimate load of 1.5 times the centrifugal force resulting from operation b) Determine that engine installation is such that it prevents excessive vibration from any part	To be demonstrated by actual test or analysis To be demonstrated by actual test	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
		c) Ensure that exhaust is firmly mounted to the structure and free from any obstructions	To be demonstrated by actual test	
		d) Determine that there is no fuel leak in the system under pressure during operational tests on ground	To be demonstrated by actual test	
		<u>Battery Operated</u>		
		a) Determine that safe cell temperatures and pressures are maintained during charging/discharging cycle	To be demonstrated by actual test or analysis	
		b) Determine that no explosive or toxic gases are emitted in normal operation	To be demonstrated by analysis and actual test	
		c) Determine that no corrosive fluid is discharged which may damage the surrounding structures/ equipment	To be demonstrated by analysis and actual test	
		d) Ensure that motor controller has overcurrent/ overheating protection	By design review	
4.	**Structure**			
4.1	Strength requirements	a) Demonstrate that airframe structure shall be able to withstand flight limit loads without failure, malfunction or permanent deformation	Static test to limit load (based on max all-up-weight) Visual check on engine mounting and structure after the test for deformation, if any	
		b) Applicant has to provide analysis of the structure showing that a factor of	To be demonstrated by analysis	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
		safety of 1.5 has been used c) Determine that each removable bolt, screw, nut, pin or other fastener whose loss could jeopardize the safe operation of the RPAS, shall incorporate a locking device d) Determine that RPA is free from excessive vibrations under any operational speed and power condition e) Determine that propeller blade clearance is sufficient from structure and/or components, and from ground.	All critical bolts of main load carrying structures to be tightened using a locknut All bolts to be locked using thread locking compound To ensure that every bolt has at least two threads sticking out of the nut (not applicable for self-locking nut) To be demonstrated by actual test Sufficient propeller blade clearance of all blades from structures and/or components under expected maximum load to be verified during design review, and by actual demonstration.	
4.2	Shock absorbing mechanism of RPA, if applicable	a) It must be shown that the limit load factors selected for design will not be exceeded. b) The landing gear may not fail, but may yield, in a test showing its reserved energy absorption capacity	To be demonstrated by test or by analysis To be demonstrated by free drop test	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
5.	**Material and Construction**			
5.1	Type of material for construction	The suitability and durability of materials used for parts, the failure of which could adversely affect safety, must: a) be established on the basis of experience or tests; b) meet approved specifications, which will ensure that strength and other properties assumed in the design data are correct; c) take into account the effects of environmental conditions, such as temperature and humidity, expected in service	 By design review or analysis By design review or analysis By design review or analysis	
5.2	Fabrication Method	a) Methods of fabrication used must produce consistently sound structures b) If a fabrication process, such as gluing, spot welding, heat-treating, etc. requires close control, the process must be performed according to an approved process specification c) Fabrication method must be substantiated by a test program	By design review or analysis By design review By design review and test	
5.3	Means of protection against deterioration or loss of strength in operation due to any cause i.e. weathering, corrosion and abrasion.	a) Effect of in-service wear on the loading of critical components should be determined b) Effect of temperature and moisture should be determined in computing the material design values	By design review or analysis followed by flight or ground test By design review or analysis as material strength properties of materials, such as composites	

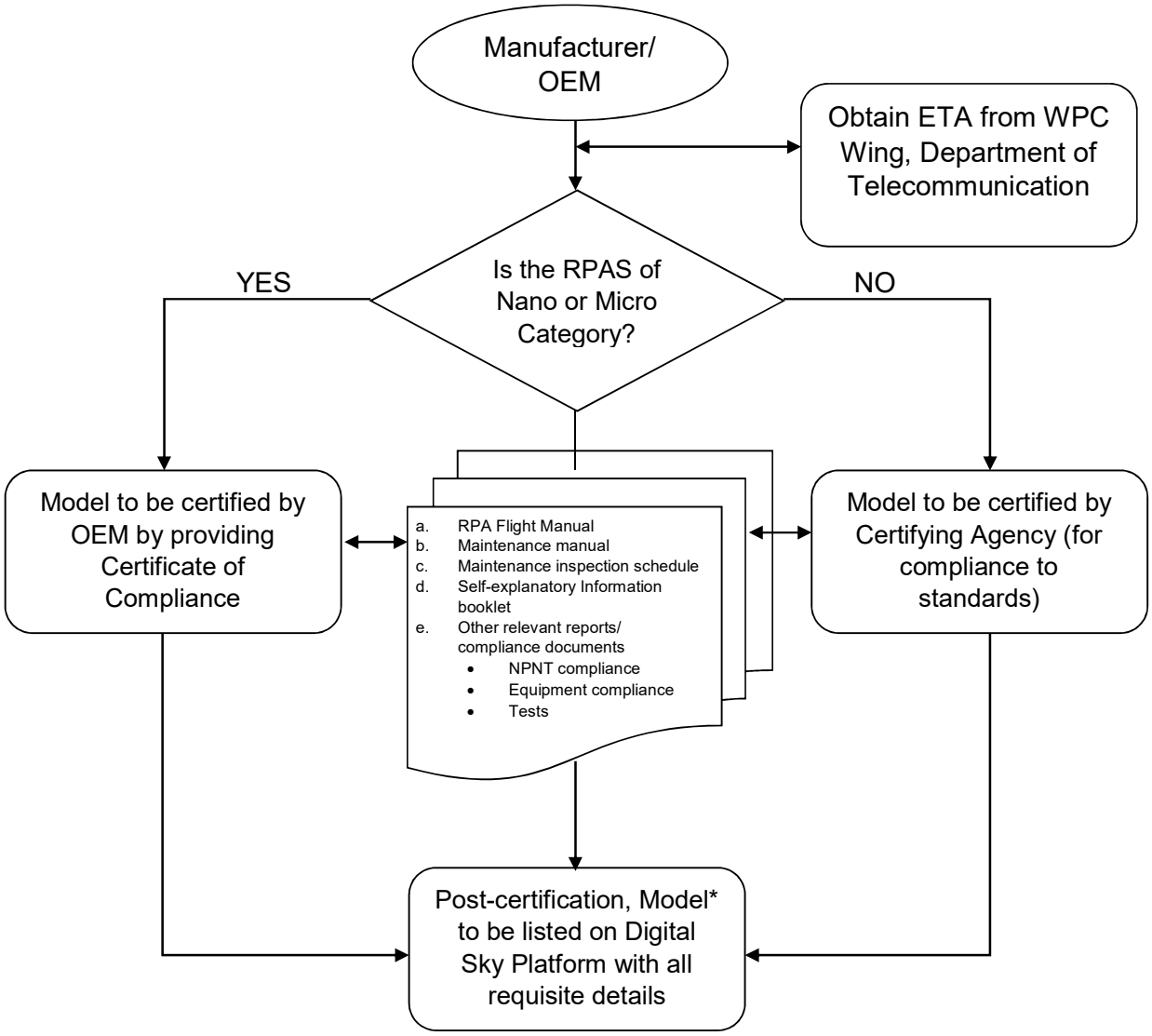
No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
			and adhesives are significantly affected by temperature and moisture	
5.4	Fire resistant identification plate on RPA for inscribing UIN.	a) Determination of ID plate material which should be fire resistant b) Determine location of ID plate along with its secure fixing on RPA	By design review and analysis By design review	
6.	**Data Link**			
6.1	Type of data-link used for communication (C2- data link) (frequency band etc.)	a) Determine full functioning of data link communication b) Demonstration of system to alert the remote pilot with aural and visual signal, for any loss of command and control data link c) Determine that communication range is sufficient to have a permanent connection with the RPA d) Determine that when data link is lost or in other contingencies, the RPA follows a predefined path to ensure safe end of flight within the required area restrictions e) Determine the capability of system to inform remote pilot by means of a warning signal in the event of data link loss f) A command and control data link loss strategy must be established, approved and presented in the RPA Flight Manual	To be verified during a distance communication test from all possible azimuth angles To be demonstrated by actual test To be demonstrated by actual test To be demonstrated by actual test with data link off To be demonstrated by actual test By design review and documentation	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
7.	**Digital Sky Platform - No Permission No Take-off (NPNT)**			
7.1	Firmware tamper avoidance	a) Determine protection of onboard computer firmware from tampering (software) b) Determine safety and security of firmware update c) Define authentication procedure to change flight parameters	Manufacturer to produce certificate of compliance indicating compliance to all conditions	
7.2	Hardware Tamper Avoidance	a) Determine protection of onboard computer hardware from tampering b) Determine mechanism to replace crucial hardware like radio modules, GPS and flight controller	To be demonstrated by actual test To be demonstrated by actual test	
7.3	NPNT	Compliance to NPNT technical specification	To be demonstrated by actual test	
8.	**Instruments/Equipment**			
8.1	a) Global Navigation Satellite System (GNSS) receivers b) Geo-fencing capability c) Autonomous Flight Termination System or Return Home (RH) option d) Flashing anti-collision strobe lights e) SSR transponder (Mode 'C' or 'S') or ADS-B OUT equipment. f) RFID and GSM SIM Card g) Detect and Avoid capability	Determine following for all instruments and equipment: • Adequate source of electrical energy, where electrical energy is necessary for operation of RPAS • Wiring is installed in such a manner that operation of any equipment will not adversely affect the simultaneous operation of any other equipment • Wiring lay out is according to the wiring diagram • All wiring is suitable for the current and voltage going through • No kinks in the wiring exist	By design review and test	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
	h) Flight controller with flight data logging capability i) Barometric equipment with capability for remote sub-scale setting j) Actuators k) Servo controllers	• Wiring routing is not along the sharp edges • Soldering connections between cables are not there • All equipment are connected with adequately secured connections to prevent loosening during vibrations • Minimum operating current • Maximum operating current		
9.	**Qualification testing**			
91.	Environmental tests	Determine that instruments and equipment withstand the following: a) Effects of voltage spikes from power source; b) Susceptibility to HIRF or lightning strike; c) Temperature and humidity variations; d) Shock resistant, etc.	To be demonstrated by test	
9.2	EMI/EMC test	Determine that each electrical instrument and equipment is protected against EMI coming from the operational environment to ensure normal operation	To be demonstrated by test	
9.3	Software	a) Determine impact of loss of function and malfunction of RPA b) Determine that sufficient independence exists between software components with respect to both function and design	To be independently verified and validated (IV&V)	
9.4	Hardware	a) Determination of hardware design life cycle through established quality control procedure,	To be independently verified and	

No.	Design Parameter	Compliance Criteria	Means of Compliance	Remarks
		component reliability, service experience indicating successful operation of component, etc. b) Component performance and reliability to be monitored on continuous basis.	validated (IV&V)	
10.	**Documentation**			
a)	RPA flight manual	RPA flight manual should contain the following information: 1. Limitations / operating conditions/ operating envelope 2. Normal Procedures, pre-flight checklist, etc. 3. Emergency procedures 4. Performance (at various combination of weight, altitude, temperature and wind conditions) 5. Any other relevant information required for safe operation of RPA	Manufacturer to provide RPA Flight Manual with supporting evidence	
b)	Other design documents	1. Analysis reports 2. Test reports 3. Detailed drawings 4. Consolidated hardware and software independently verified and validated reports 5. Material procurement record 6. Manufacturing process records	All documents to be frozen	

Manufacturing of RPAS – Flow Chart



** Not mandatory for Nano*

Sample Certificate of Compliance

(In OEM/ Manufacturer's letter head)

Certificate of Compliance

I certify that the RPAS listed below **complies with the material, minimum standard specified in the CAR Section 3, Series X, Part I including 'No permission- No Takeoff' specifications**.

I also certify that I am an official representative for _____, the manufacturer of the RPA listed below. Furthermore, I certify that where Test methods, Demonstration, Analysis requirements are part of the specifications, that the manufacturer has performed the necessary quality control to substantiate this certification.

RPAS Description:

Manufacturer:_____

RPA Model: _____

RPA Type: _____

RPA Category: _____

Serial Number: _____

(Please attach list of serial numbers in alphabetical/ numeric order or scheme of numbering as an annexure to this certificate)

Quantity to be supplied: _____

Remarks: _____

(Signature of the authorised official)
Title
Manufacturer Name
Date

Note:

1. This certificate of compliance should be provided by all categories of RPAS except Nano.

2. The manufacturer should also include drawings, test reports, statements and submit DGCA with this certificate. The manufacturer may provide a master index/ compliance matrix to their system documentation.

3. Any change (upgrade) in the model will require fresh certificate of compliance from the manufacturer.

Chapter 7

NPNT Specifications

Digital Sky

Technology Standard - Registered Flight Module

For questions and feedback on the technology standard, please reach out on forum.digitalsky.dgca.gov.in

Table of Contents

Definition of Terms

CA	Certifying Authorities
DGCA	Directorate General of Civil Aviation
DHE	Ephemeral Diffie-Hellman
DSC	Digital Signature Certificate
DSP	Digital Sky Service Provider
ECDHE	Elliptic Curve Diffie-Hellman
GLPS	Global Level Positioning System (GPS, GLONASS, Galileo, IRNSS, etc)
HSM	Hardware Security Module
IST	Indian Standard Time
NPNT	No Permission No Takeoff
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RFM	Registered Flight Module
RPAS	Unmanned Aircraft System(s)
RPAS	Remotely Piloted Aircraft System(s)
UFII	Unified Flight Information Interface
UIN	Unique Identification Number
UUID	Universally Unique Identifier

Version History

Version	Date	Comments
1.0	22/10/2018	Publication of Registered Flight Module v1.0 Technology Standard
1.1	03/06/2019	1. Revision in Exhibit C Diagram 2. Addition of 2.3 - Communication Requirement for multiple chip or module design 3. Addition of 3.1 Key Generation 4. Extension in Keypair Generation to allow for Smart Card/PKI Token in addition to HSM 5. Revision in Permission Artefact from XML to JSON 6. Removed support for pilot pin 7. Removed test cases related to pilot pin 8. Added NPNT test tool 9. Added support for ECC 10. Removed Pilot pin RFM API

1. Introduction

Imagine a future where Remotely Piloted Aircraft Systems (RPAS) augment human capabilities. They could help farmers prioritize where to apply fertilizer, or help energy companies monitor their infrastructure, or even enable emergency response teams to quickly map the extent of damage after natural disasters. In the near future, RPAS could deliver packages, streamline agriculture management, reinvent human mobility, and even save lives. Therefore, Digital Sky puts in place a seamless and secure technology and regulatory framework to integrate this new technology into the Indian airspace.

Digital Sky enables a proactive approach to enforcement of safety and security guidelines by ensuring that a RPAS does not take-off without a signed digital permission, obtained via the Digital Sky Service Providers, and necessary flight logs and occurrence reports are reported back to the relevant authorities via the DSPs.

We envision a future, when millions of RPAS are flying across the country, without significantly increasing the regulatory burden. Thus, Digital Sky can be extended in the future to carry out autonomous flights, automated RPAS traffic control, air taxis, besides other use-cases.

1.1 Mission

The mission of Digital Sky is to create a completely digital, paperless, and presenceless process, thus fast-forwarding to a future of on-demand seamless permissions for RPAS, operators, and pilots.

1.2 Vision

The vision is to create a digital infrastructure that will support safe, efficient, and secure access to Indian airspace for millions of RPAS.

1.3 Target Audience and Prerequisites

This is a technical document and is targeted primarily at RPAS manufacturers or providers who want to build registered flight modules as per this specification. Civil Aviation Requirements for Operation of RPAS are out of scope of this technical document - they have been made available at http://dgca.nic.in/cars/D3X-X1.pdf

NOTE: In this document, the term “Flight Module Provider” is used to refer to a RPAS manufacturer or any agency who has partnership with the manufacturer to manage certification and related software/security aspects of registered flight modules:

- One provider may have many RPAS models
- One provider may have many versions of the Registered Flight Module (RFM)
- One Registered Flight Module (RFM) service may handle many models

The Flight Module Provider should be a legal entity registered in India and is responsible for certification, key management (as per this specification), and any security or other responsibilities set forth by DGCA.

For more details on the Registered Flight Module, you may refer to Section 2.

1.4 Guiding Design Principles

1.4.1 Safety by Design

Every RPAS should be designed, manufactured, remanufactured, or rebuilt with safe design and manufacturing considerations. Improper design and manufacture can result in hazards to personnel if minimum industry standards are not conformed to on mechanical components, controls, methods of operation, and other required information necessary to insure safe and proper operating procedures.

1.4.2 Security by Design

The software and systems must be designed from the ground up to be secure. There must be end-to-end security of data using PKI, DSC, tamper detection, and other security measures like continuous monitoring, hunting, and response.

1.4.3 Privacy by Design

The following privacy principles must be embedded into the design:

- Proactive not reactive; Preventative not remedial
- Privacy as the default setting
- Visibility and transparency – keep it open
- Respect for privacy of all the stakeholders – keep it ecosystem-centric

1.4.4 Open Platform and Open Standards Based

The framework should use open technology and legal standards available in the country. It should be agnostic to applications, programming languages, and platforms.

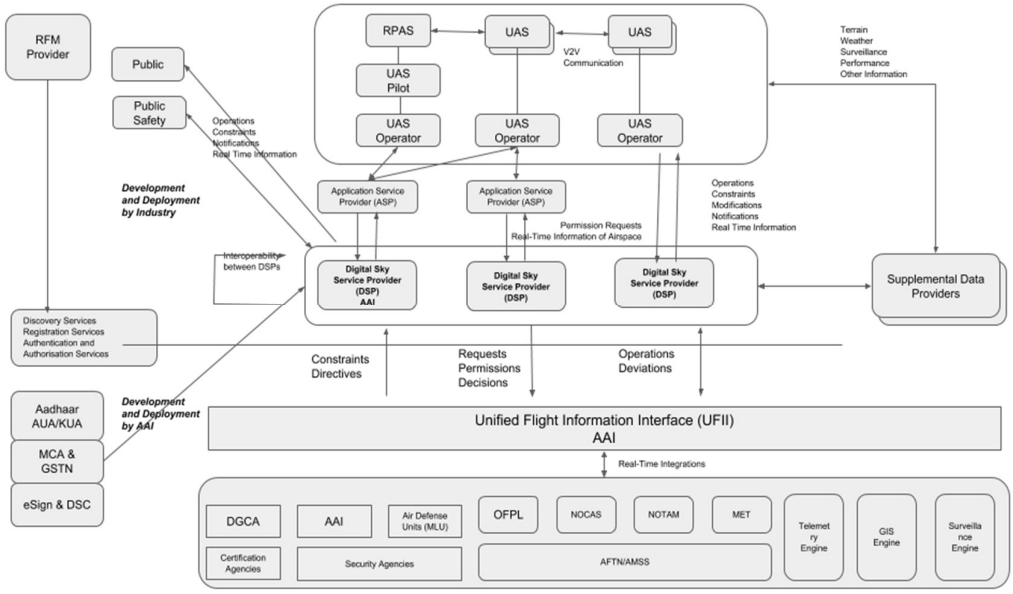
1.4.5 Universal Identity

The technical framework should leverage universal, authenticable, non-repudiable, and digital identities to allow interoperability across all users (pilot, flight module provider, operator, drone, etc) in the system. For example, Aadhaar for Individuals, GSTN for Businesses, etc.

1.4.6 Ecosystem Driven Approach

An ecosystem approach is necessitated such that the interfaces between the partners (like Digital Sky Service Providers and Application Service Providers) and systems (like Unified Flight Information Interface) are well defined and standardized. Hence, there must exist a technology backbone that would hold together this partner ecosystem.

Exhibit A: High-Level Overview of Digital Sky Ecosystem



1.4.7 Information Technology Act Compliant

The framework must use digital signatures to guarantee non repudiation (includes identity and integrity) of the access permissions given by/for users in permission flows as well as actions taken by the users. This makes the framework fully legal under the IT Act[1].

1.4.8 Minimalist and Evolutionary Design

The design of the framework should be simple and minimalistic. It should not present adoption barriers for the ecosystem. The design of the systems should be evolutionarily - their capabilities should be built incrementally while allowing for rapid adoption.

1.4.9 Ease of Doing Business

[1] http://www.meity.gov.in/content/information-technology-act

The framework should be designed by placing the operator in the centre, thus only adopting approaches that are convenient and easy for doing business.

1.4.10 Digital Enforceability

The framework should allow operators to set permissions and rights for airspace permission access at a fine-tuned level (for example, the ability to choose a polygon area of airspace at a particular altitude and for a particular date and time) and the same must be enforced digitally through No Permission No Takeoff and generation of verifiable flight telemetry.

2. Registered Flight Modules

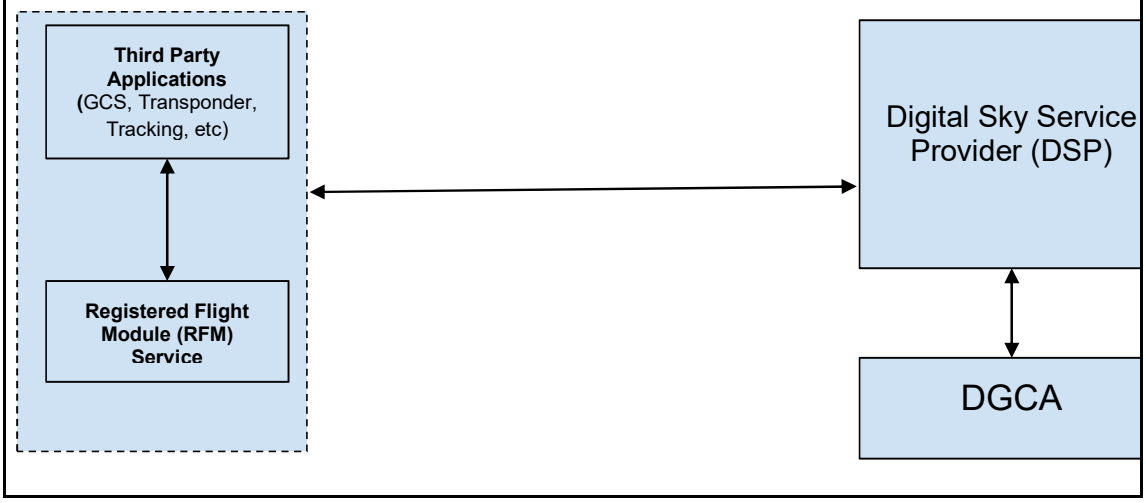
2.1 Registered Flight Module (RFM)

Registered Flight Modules specification described in this document provides the following key features:

1. Non Repudiable Identification of RPAS – every Flight Module has a unique identifier allowing end to end traceability, accountability, traffic management, and forms the foundation for issuance of UIN.
2. No Permission No Takeoff (NPNT) - every RPAS must obtain a valid permissions artefact and verify the same before it can arm itself.
3. Eliminating use of synthetic flight logs - there should be no mechanism for any external system to provide simulated flight logs and get it signed.

It is important to note that it is in Flight Module Provider's interest to ensure the above items are implemented securely since any compromise on these will result in fraudulent activities signed using the Flight Module Provider key. As per IT Act it is essential for the key owners (Flight Module Provider) to protect the signature key and take responsibility for any compromise.

Exhibit B: High-Level Overview of RFM Ecosystem



DGCA does not mandate any specific hardware design and Flight Module Providers are expected to innovate appropriate form factors for market use. That being said,

minimum mandates related to the security of keystore and key management are being prescribed in this specification.

2.2 Levels of RFM Compliance

2.2.1 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.

2.2.2 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.

2.3 Communication requirement for multiple chip or module design

Registered flight module can be implemented using multiple chips or modules (for example, flight controller and companion computer may be put together as a logical RFM), in which case the chips or modules constituting Registered Flight Module will have same compliance requirements as a single module plus the communication between modules has to be secured using or equivalent of 128bit symmetric key (minimum).

3. Registration

3.1 Generation of Keys

1. Key pair is generated at RFM level or generated elsewhere and transported to RFM.
2. If keypair is not generated at RFM, it should be generated within a zone that has the same security requirements as RFM and has to be transported to the RFM on a communication channel secured using or equivalent of 128bit symmetric key (minimum).
3. If key rotation is required, the generated key may be signed using previous key pair and sent for updation to DigitalSky.

3.2 Registration of Flight Module

Prior to registration of a flight module, the Flight Module Provider must:

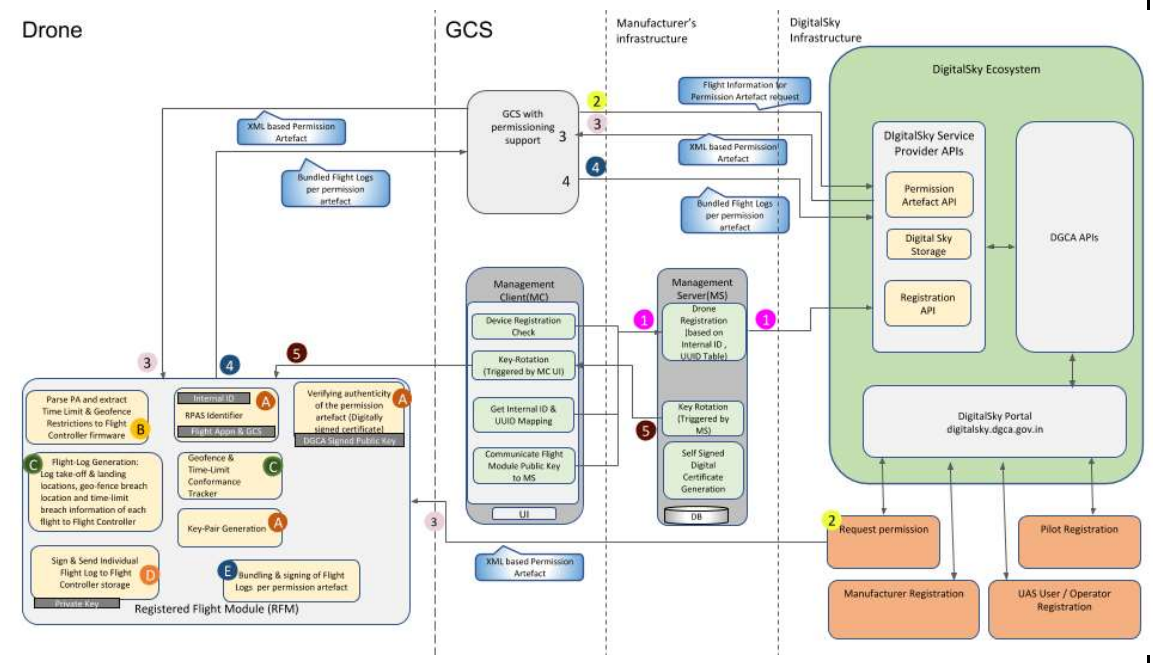
1. Register with Digital Sky and provide the list of certified models.
2. Procure a digital certificate from a valid CA[2] in India and get it signed by DGCA. The public key in the certificate would be the Flight Module Provider key and it would be used to sign the Drone ID and flight module public key. Flight Module

[2] http://www.cca.gov.in/cca/?q=licensed_ca.html

Providers can have one or more keys and can rotate, revoke their keys via Digital Sky.

For registration of each flight module, the Flight Module Provider must provide for a Flight Module Management Client and Flight Module Management Server. (Key Management for the Management Server may be maintained by an external Technology Service Provider through a valid custodian agreement.)

Exhibit C: High Level Sequence Diagram of RPAS, Ground Control Station, Management Client and Server, and Digital Sky



3.2.1 Functionality of Flight Module Management Client

1. Management client may or may not be packaged with RFM Service as an installable.
2. Management client should implement an "init" method internally to check if flight module is registered, connect to management server, initialize and rotate keys, and check for software upgrades.
3. When running, management client should detect for physical flight module connected and readiness of it. The Management Client reads the RPAS Drone ID during each power-up init() call. Then Management Client checks whether the Drone ID is mapped to any UUID (generated and sent by the server for the first time).
4. If UUID is not available, that means the system is not registered. If flight module is not registered, it should auto initiate registration.
    a) In that case to start the registration process, Management Client will send the Drone ID to Management Server
    b) Management Server generates new UUID, sends this back to the Management Client, initiates other work-flows with Digital Sky for the RPAS registration
    c) The Drone ID can be composed of serial numbers, internal identifiers, signatures, etc. Flight Module Providers must ensure that this Drone ID does not change during the life of that physical flight module.

d) In addition, to avoid invalid/non-genuine flight modules being registered, a concept of "one-time activation code" could be used to authenticate if the flight module is genuine.

    i. Flight Module Providers can send the one-time activation codes to people/entities who procure the flight module.
    ii. This provides a mechanism to do out of band authentication.
    iii. Once it is activated, optionally user registration can be done and user authentication may be used for all management services in addition to client software authentication.

e) Registration should include Drone ID (serial number or any other internal ID that is used to recognize physical flight module), host fingerprint, timestamp, flight module keys, and other flight module details for authentication, etc.
f) Flight Module Provider may keep additional attributes/info for their own management and audit purposes.
g) Flight Module Provider should check pre-existence of serial number or other physical unique attributes to ensure same flight module gets same flight module code UUID. In the case of new registration, server generates a new flight module code (UUID) and should send back to client.
h) Flight Module Provider's Management Server should call Digital Sky Register API to ensure flight module is registered with Digital Sky.
i) After successful registration with Digital Sky, Flight Module Provider's Management Server should sign the flight module public key and return to client.

5. If flight module is registered, it should initiate key rotation when necessary.
    a) Management service should trigger key rotation under 2 scenarios:

        i. based on the trigger from management server during "init" (ideally done at least once a day);
        ii. based on the manual trigger from management client UI (this is needed only in special conditions where manual key reset needs to be triggered). This trigger should call same "init" to re-initialize.

    b) When key needs to be rotated, flight module should generate new key pair, send public key to server for signing and updating management server registry.
    c) Private key must be generated and stored securely within keystore.
    d) See keystore security section (3.1.5) for details on keystore protection.

6. Management client should check for software upgrades and initiate upgrades.

3.2.2 Functionality of Flight Module Management Server

1. All management server communication must be via HTTPS (with DHE/ECDHE for perfect forward secrecy).
2. Management server should authenticate management clients and allow registration, key rotation, triggering upgrades, and other necessary management services. See previous section for details.

3. Management server should use a Hardware Security Module (HSM)/Smart Card/PKI Token for key management. The HSM/Smart Card/PKI Token must be compliant with FIPS140-2 Level 3 or FIPS140-2 Level 4.
4. Flight Module database, secret token for authenticating management client, flight module fingerprint, user credentials, etc. should be protected through controlled access, encryption, and other security best practices.
5. Appropriate security mechanisms should be in place to protect HSM/Smart Card/PKI Token and flight module database access.
6. Log files should not contain any sensitive data (like private keys, secret tokens, passwords, PII, etc).
7. Management Server should implement configurable key rotation policies and should be configurable as per DGCA policies.
8. All flight modules should generate an asymmetric key pair within the flight module. This would be the flight module key pair. Every physical instance of the flight module should have its own flight module key pair.
9. Flight Module public key should be signed by one of the Flight Module Provider's keys. The provider must sign the flight module public key on the Flight Module Provider's server within the HSM/Smart Card/PKI Token.
10. Flight Module Provider MUST ensure each physical flight module has a unique code (drone id). Maximum length of the code is 50 characters when represented as string. To ensure flight module codes are globally unique it is necessary that Flight Module Provider uses a 128-bit UUID (represented in HEX notation).
11. Note: Flight Module public-private key generation and signing of flight module public key with Flight Module Provider key can be performed at any point of time during flight module's lifecycle.

3.2.3 Digital Sky APIs for Registration and Deregistration

The Flight Module Provider's "Management Server" should request the Digital Sky Registration API whenever a new flight module needs to be registered. The Flight Module Management frontend to management server interfaces are specific to the Flight Module Provider.

These APIs will be provided by Digital Sky and only certified Flight Module Providers will be able to request the same. This will be made possible using IP Whitelisting and validation of the digital signature and API.

Register API

Request URL: https://{baseUrl}/api/droneDevice/register/<Flight Module Provider id>

Input

```
{
      "drone" : {
            "version" : "",
            "txn": "",
            "deviceId": "",
            "deviceModelId": "",
            "operatorBusinessIdentifier" : "",
            "idHash" : "",
      },
      "signature" : "",
      "digitalCertificate" : ""
}
```

Input Property Keys	Description
drone.ver (mandatory)	version of the API
drone.txn (mandatory)	transaction identifier (of max length 50) entered by manufacturer, which is also returned as part of response as is and is useful for linking transactions full round trip across systems.
drone.deviceId (mandatory)	Unique Drone's Drone Id
drone.deviceModelID (mandatory)	Device Model Id
drone.operatorBusinessIdentifier (mandatory)	Operator Unique identifier to be linked to the drone device
drone.idHash(optional)	Hash of the Drone Id of the Drone
Signature (mandatory)	Base64 Encoded Digital Signature of the drone data
Digital Certificate (mandatory)	Base64 Encoded X509 Certificate of the manufacturer

Output

```
{
   "txn":"",
   "responseTimeStamp":"",
   "code":"",
   "error":""
}
```

Output Property Keys	Description
txn	transaction identifier as entered in the request
responseTimeStamp	
code	Response codes: REGISTERED REGISTRATION_FAILED OPERATOR_BUSINESS_IDENTIFIER_INVALID OPERATOR_BUSINESS_IDENTIFIER_MISSING INVALID_SIGNATURE INVALID_DIGITAL_CERTIFICATE DRONE_ALREADY_REGISTERED INVALID_MANUFACTURER MANUFACTURER_BUSINESS_IDENTIFIER_INVALID BAD_REQUEST_PAYLOAD
error	Error details if registration has failed

DeRegister API

Request URL: https://{baseUrl}/api/droneDevice/deregister/<Flight Module Provider id>

Input

```
{
      "drone" : {
                  "version" : "",
                  "txn": "",
                  "deviceId": "",
                  "deviceModelId": "",
                  "idHash" : "",
      },
      "signature" : "",
      "digitalCertificate" : ""
}
```

Input Property Keys	Description
drone.ver (mandatory)	version of the API
drone.txn (mandatory)	transaction identifier (of max length 50) entered by manufacturer, which is also returned as part of response as is and is useful for linking transactions full round trip across systems.
drone.deviceId (mandatory)	Unique Drone's Drone Id.
drone.deviceModelID (mandatory)	Device Model Id
drone.idHash(optional)	Hash of the Drone Id of the Drone
Signature (mandatory)	Base64 Encoded Signature of Drone Json Data
Digital Certificate (mandatory)	Base64 Encoded X509 Certificate of the manufacturer

Output

```
{
   "txn":"",
   "responseTimeStamp":"",
   "code":"",
   "error":""
}
```

Output Property Keys	Description
txn	transaction identifier as entered in the request
responseTimeStamp	
code	Response codes: DEREGISTERED DEREGISTRATION_FAILED DRONE_NOT_FOUND DRONE_NOT_REGISTERED INVALID_SIGNATURE INVALID_DIGITAL_CERTIFICATE INVALID_MANUFACTURER MANUFACTURER_BUSINESS_IDENTIFIER_INVALID BAD_REQUEST_PAYLOAD
error	Error details if deregistration has failed

Payload verification process during Registration or Deregistration:

1. Digital signature is verified against the drone data in the request, using the digital certificate.
2. Verify if the digital certificate belongs to the manufacturer by matching the organization name of the manufacturer saved against the manufacturer business identifer in the digitalsky system with that of the 'o'(case insensitive) property in the subject of the digital certificate.
3. Validate the digital certificate passed as a part of payload using the certificate chain uploaded during the manufacturer profile creation. Validation fails if either the certificate chain itself is invalid or if the digital certificate is invalid.

3.2.4 Certificates and Keys Policies

1. Below are the currently supported algorithms for digital signing:
    a. SHA256withRSA (2048 bit key)
    b. ECDSA with safecurves (https://safecurves.cr.yp.to)
2. All Flight Module Provider certificates should be procured from a certification authority (CA) as per Indian IT Act.
   (http://www.cca.gov.in/cca/?q=licensed_ca.html)
3. All Flight Module Provider certificates should be class II or class III and X509 v3 compliant.
4. Organization attribute in the certificate's subject SHOULD match the Flight Module Provider's name registered with DGCA

3.2.5 Keystore Security

1. Keystore should be limited with read and write rights only for the user as whom the RFM service runs and no other user accounts should have access to it.
2. Keystore password has to be complex and auto generated. The following list of approaches are possible:
    a. A combination of random data, user credentials and flight module identification data -derived key using identities
    b. The logic how key is derived using these values has to be obfuscated to avoid any possible security threats.
    c. The key derivation logic should be in a compiled native machine dependent code and cannot be an Open API.
    d. The password should be changed for every key rotation.
    e. Use White Box Cryptography to derive the password.
    f. The password should be more than 16 characters in length and should contain small letters, capital letters, special characters, and numbers.
    g. A server side logic to help with opening the keystore.
3. The RFM service should fail its integrity check upon the keystore permissions not correct or has unwanted access and should inform the server about such failures. This failure would be tracked as an incident by the Flight Module Provider.
4. All type of access and access attempts to the keystore should have audit logs.
5. The private key should not be extractable (wrapped or direct)
6. It is recommended that key pair is generated inside the flight module service. Note that flight module authentication must be performed before allowing any connection to management server
7. The keystore has to be cleared and zeroed in case the RFM service is deleted.

For detailed recommendations and best practices on key management, you

may refer to the following global standards by NIST

- Part 1: General: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final
- Part 2: Best Practices for Key Management Organization: https://csrc.nist.gov/publications/detail/sp/800-57-part-2/final
- Part 3: Application-Specific Key Management Guidance: https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

3.3 Issuance of UIN

Once the flight module has been successfully registered with Digital Sky based on the process outlined in 3.1, following steps need to be completed to receive a UIN:

- Approve Operator Linkage Request (linking drone with operator)
- Fill UIN Form on Digital Sky and Submit
- If approved, then UIN is issued and flight module is added to registry.

Through Digital Sky, an end to end linkage of the Flight Module Provider, RFM/RPAS, Owner, Operator, and Pilot is formed providing traceability and ensuring accountability.

4. Registered Flight Module (RFM) APIs

The RFM should be implemented at the Flight Controller Level. The RPAS RFM Provider should not allow un-notified access to the UA flight controls - the RFM service should be notified of every call (pertaining to conditions specified in this RFM specification) to the UA flight controller. There should not be any bypassed or unchecked access to the RPAS flight controls.

The permission artefacts and the flight logs must not be stored by the RFM. It must be stateless and must provide a tamper-proof mechanism to offload any storage and state handling to the host system.

4.1 RFM Core Functionality

4.1.1 RPAS Identification (Drone ID)

1. Items to be Uniquely Identified to avoid alterations:
    a. UID of Hardware modules used like MicroProcessor/Controller, Radio Modules.
    b. Version Hash of firmware and bootloader on-board.
    c. Unique License/Identifier of Flight Module Provider
2. Layers for Identification:
    a. Flight Application: Connected Hardware modules identification, Flight Module Provider License Verification
    b. Co-Computer/GCS: Flight Module Provider License Verification.

4.1.2 Verifying authenticity of the Permission Artefact

Permission Artefact is an electronic representation of a permission to fly granted through the Digital Sky Service Providers. Here's the XML structure of the artefact:


```
{
   "droneId":2,
   "id":"0",
   "pilotBusinessIdentifier":"4b3bbbc2e307474188d182ae955224fc",
   "payloadWeightInKg":"0",
   "payloadDetails":"0",
   "flightPurpose":"0",
   "maxAltitude":114,
   "startDateTime":"19-03-2019 07:00:00",
   "endDateTime":"19-03-2019 13:00:00",
   "flyArea":[
      {
         "longitude":93.4989563203491,
         "latitude":24.98958739448595
      },
      {
         "longitude":93.49979678709262,
         "latitude":24.98433022695947
      },
      {
         "longitude":93.50756424845548,
         "latitude":24.984514759481144
      },
      {
         "longitude":93.50628467413502,
         "latitude":24.98935432573667
      },
      {
         "longitude":93.4989563203491,
         "latitude":24.98958739448595
      }
   ],
   "status":"APPROVED"
}
```


The permission artefacts will come with a digital signature (a form of Public key cryptography), encrypted using Digital Sky private encryption key. The RFM service must use the corresponding public keys (released by Digital Sky) to verify that the permission artefact is released by authorised DSP and has not been tampered with during transport. If the public key has to be changed (When Digital sky requests the Flight Module Providers to change), the Flight Module Provider has to release a firmware update to update the key. Flight Module Provider should build security measures to ensure that any 3rd party is not able to alter the public keys used to verify the permission artefact in the library.

4.1.3 Provide information of Time and Location bound restrictions to Flight Controller

The verified permission artefact will provide geofence information in horizontal and vertical plane to the Flight Controller. The permission artefact also consists of the time period for which the permission is valid.

4.1.4. Collect Flight Logs

The Flight Module Provider is required to implement functionality to provide following data to the RFM service. This data will be saved against each permission artefact.

I. Date-time information from GLPS data in IST
II. Date-time information from system in case GLPS fixture is unavailable.
III. System clock timestamp
IV. For each power cycle, the list of takeoff, land coordinates.
V. Upon breach of the geofence, the start/stop timestamp, a list of GLPS coordinates during the time the drone was outside the geofence, captured at 1 Hz minimum.
VI. Upon breach of the time limits, the additional time, and list of start/end timestamp for which the RPAS was in air should be provided to the library.
VII. The flight logs captured during the period of the permission artefact should be stored on the flight controller along with hash of the logs to ensure tamper-proof records. A record must be maintained on-board to connect next and previous flight logs to avoid omission and the same should be inaccessible to the user. Once the permission artefact is expired or when user wants to submit logs, the complete bundle of such logs should be signed using RFM private key and submitted to the DSP.

4.1.5 Sending Flight Logs to Digital Sky Service Provider

The Flight Module Provider is responsible for providing the communication interface between RFM and DSPs or external applications, which can ultimately interact with DSPs. Since, third party applications can provide the functionality for sharing permission artefact and flight log data between DSPs and RFM, it is suggested to provide a standardized communication interface to the external applications to interact with RFM's permission artefact and Flight Log APIs. Finally, the Flight Module Provider is responsible for providing to user, at least one way of sharing this data, either over a direct link between RFM and DSP or through an external application (e.g. Ground Control Station).

4.2 RFM API Reference

1. Get_rfmInfo
   Parameter 1: IST date-time (fetched from GLPS data or any other source)
   Output 1: RFM public key
   Output 2: Digital Sky Public Key being used in RFM
   Output 3: Firmware Version
   Output 4: RFM version
   Output 5: RPAS category
   Output 6: Operator ID obtained during registration
   [Provide RPAS info]
   a. The API will return the required information for any external application.

b. The RFM Provider has to sign the information using RFM private key.

2. Apply Permission Artefact:
   Parameter 1: Permission_artefact
   Parameter 2: IST date-time (fetched from GLPS data or any other source)
   [provide permission artefact to the RFM]
   a. This API should be called by Flight Controller or host system every time the RPAS is powered on.
   b. RFM will verify the signed permission artefact using the Digital Sky Public Key.
   c. RFM, being stateless, will not store the permission artefacts in the memory, so Flight Module Provider is responsible for providing relevant permission artefact to the RFM on every power cycle. The permission state is maintained by the RFM for the current power session only.
   d. RFM will use timestamp provided by Flight Module Provider, the artefact publish timestamp (marked by DSP when the artefact is created), and the ttl (time to live) value to validate that the artefact is eligible at that time and that the system time-date is not falsified.
3. Get_Geofence_restriction:
   Parameter 1: IST date-time
   [provides geofence information to the Flight Controller or Host system after a valid permission artefact has been applied]
   a. RFM will verify the date-time stamp to reassert the time validity of the permission artefact
   b. This API is provided by RFM for the Flight Controller or Host system. The Flight Controller is expected to use this data for enforcing safety restrictions or warning the pilot.
   c. It is responsibility of Flight Module Provider to ensure that the RPAS follows the geofence restrictions. In case of geofence or time limit violations, the Flight Module Provider should provide the event details to the RFM.
4. Get_time_restriction:
   Parameter 1: IST date-time
   [Provides allowed time limit after a valid permission artefact has been applied]
   a. RFM will verify the date-time stamp to reassert the time validity of the permission artefact.
   b. It is responsibility of Flight Module Provider to ensure that the RPAS is landed before the permitted time period expires. In case of time limit violations, the Flight Module Provider should provide the event details to the RFM
5. Log_takeoff_location:
   Parameter1: IST date-time
   Parameter2: GLPS coordinates
   [To provide takeoff event information to library for internal logging.]
   a. The Flight Module Provider is responsible to implement the functionality to ensure that this API is called immediately after takeoff event.

b. The Flight Module Provider should not provide any means to bypass the notification to RFM on a takeoff event.
c. The RFM will store and package all such events in one flight log against a permission artefact.

6. Log_Land_location:
   Parameter1: IST date-time
   Parameter2: GLPS coordinates
   [To provide land event information to RFM for internal logging.]
   a. The Flight Module Provider is responsible to implement the functionality to ensure that this API is called immediately after land event.
   b. The Flight Module Provider should not provide any means to bypass the notification to RFM on a land event.
   c. The RFM will store and package all such events in one flight log against a permission artefact.
7. Log_geofence_breach:
   Parameter1: IST date-time
   Parameter2: Breach_start_timestamp
   Parameter3: Breach_stop_timestamp
   Parameter2: GLPS coordinates
   [To provide geofence breach event information to RFM for internal logging.]
   a. The Flight Module Provider is responsible to implement the functionality to ensure that this API is called immediately after a geofence breach incidence.
   b. The Flight Module Provider is responsible for implementing functionality to call this API at 1 Hz, from the time when Geofence is breached to when the drone lands.
   c. The RFM will store and package all such events in one flight log against a permission artefact.
8. Log_timelimit_breach:
   Parameter1: IST date-time
   Parameter2: time_overrun_start_timestamp
   Parameter3: time_overrun_land_timestamp
   [To provide time limit breach event information to RFM for internal logging.]
   a. The Flight Module Provider is responsible to implement the functionality to ensure that this API is called immediately for a time limit overrun event.
   b. During the first call, when the drone is still in flight, the time_overrun_timestamp parameter will not have any value. The event would be logged as start of time overrun.
   c. When the drone lands this API should be called again to indicate end of flight. In this case the API caller needs to provide time_overrun_start_timestamp again. This event will be registered as end of time-overrun event.
   d. The RFM will store and package all such events in flight log against a permission artefact.

9. Get_individual_flight_logs:
   Parameter1: IST date-time
   [To get the individual flight logs from the RFM for storage]
   a. The RFM must prepare a flight log after each land, geofence breach, or flight time overrun.
   b. These flight logs will be digitally signed by the RFM to make sure that flight logs are not tampered with during the transport. It is Flight Module Provider's responsibility to implement the functionality required to keep the private key secure. These reports may be verified against that public key that was shared during registration of the RPAS.
   c. It is responsibility of the Flight Module Provider to implement the functionality to collect these reports immediately after every takeoff, land, Geofence and time-limit breach event from RFM. In case of crash where such events were not registered, the RFM on next power cycle, should close the log with failed landing incidence.
   d. The Flight Module Provider is responsible to implement the functionality to store all the flight logs until they are uploaded to the DSP. This storage should provide the 'write access' only to the applications authorized by Flight Module Provider. The read access to the storage should be available in case of accidents. The Flight Module Provider is required to provide the authorities with the specialized equipment required to read the flight logs from a crashed/damaged RPAS's onboard storage.
   e. Flight Module Provider is responsible to provide communication interface to upload the flight log directly to the DSP or through external applications, such as Ground Control Station.
   f. The Flight Module Provider is responsible to ensure the storage space for logs. If storage space is not available for logging then the flight should not be allowed.
10. Bundle_flight_logs:
    Parameter1: IST time-stamp
    Parameter2: List_of_individual_incidence_reports_from_storage
    Parameter3: Permission Artefact
    Output1: Bundled_incident_report_with_digital signature.
    [To bundle the signed flight logs from storage into a single bundle (a bundle per permission artefact).]
    a. After the time-period of a permission artefact is over, the user has to submit the flight logs to Digital Sky APIs within 3 days. The Flight Module Provider is required to implement the functionality to provide all the flight logs associated with a particular permission artefact and pass them on to this API to get in return a signed bundle.
    b. Flight Module Provider is responsible to provide communication interface to upload this bundle directly to the DSP or through external applications, such as Ground Control Station.

4.3 JSON Schema for flight log

```
{
   "$id":"http://dgca.gov.in/schema/incident_report_field.json",
   "type":"object",
   "properties":{
      "PermissionArtefact":{
         "$id":"/properties/PermissionArtefact",
         "type":"string",
         "format":"base64"
      },
      "FlightLog":{
         "$id":"/properties/FlightLog",
         "type":"array",
         "items":{
            "$id":"/properties/FlightLog/items",
            "type":"object",
            "properties":{
               "TimeStamp":{

"$id":"/properties/FlightLog/items/properties/TimeStamp",
                  "type":"integer",
                  "title":"Timestamp in MilliSeconds",
                  "default":0
               },
               "Latitude":{

"$id":"/properties/FlightLog/items/properties/Latitude",
                  "type":"number",
                  "format":"float",
                  "title":"Latitude in Degrees East",
                  "default":0
               },
               "Longitude":{

"$id":"/properties/FlightLog/items/properties/Longitude",
                  "type":"number",
                  "format":"float",
                  "title":"Longitude in Degrees North",
                  "default":0
               },
               "Altitude":{

"$id":"/properties/FlightLog/items/properties/Altitude",
                  "type":"integer",
                  "title":"Ellipsoidal Height in Meters",
                  "default":0,
                  "minimum":-99999,
                  "maximum":99999
```

```
                },
                "CRC":{

"$id":"/properties/FlightLog/items/properties/CRC",
                    "type":"integer",
                    "title":"Circular Redundancy Check (optional)",
                    "default":0,
                    "minimum":0,
                    "maximum":4294967296
                }
            },
            "required":[
                "TimeStamp",
                "Longitude",
                "Latitude",
                "Altitude"
            ]
        }
    }
}
```

(Possible Reference for 32 bit CRC https://en.wikipedia.org/wiki/Cyclic_redundancy_check#CRC-32_algorithm)

5. Test Structure for Certification

The certification of registered flight modules would involve test cases covering secure provisioning of keys, implementation of Flight Module Management Server and Client, functional tests, security tests, and other compliance related tests.

It is required by Flight Module Providers to minimise the attack surface at the system level using methods such as but not limited to protective meshing, encrypted communication, etc. In addition, it is highly recommended that tamper responsiveness be implemented for the system.

Here are a list of example test cases:

Sr. No.	Type of Test
1	Fake and authentic signed permission artefact test
2	Individual flight log storage test (including digital signature verification)
3	Geofence breach flight log test
4	Time limit breach flight log test

5	Bundled flight log test (including digital signature verification)
6	RTH test in case of violation of permissions in the context of geofence bounding box breach and max time-limit breach
7	Accidental storage data retrieval test with the specialized equipment
8	Overall no permission-no takeoff policy test
9	Secure Boot and Secure Upgrade
10	Secure Provision of Keys
11	System Level Tamper Responsiveness
12	Any other test as defined by the Certification Agencies

There will be certification agencies that will be empanelled to certify the RPAS, Registered Flight Module, etc. These agencies shall publish the detailed list of test requirements beforehand that would be necessary for certification.

If you would like to test out your RFM Implementation, you may try out the open source test tool: http://139.59.71.151/

In case you find any bugs or have any improvements, you may make the same here: https://github.com/iSPIRT/NPNT-Provisional-testing-tool

6. References

- Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS): http://dgca.nic.in/cars/D3X-X1.pdf

7. Appendix

7.1 General Safety Guidelines

1. **Firmware Tamper Avoidance:** *There is possibility to change firmware by the user so as to change the behaviour of the drone which might not follow laid guidelines under which the drone was originally cleared.*
    a. ReadOut Protection on MicroProcessor/MicroController for onboard firmware to avoid Copying of onboard keys and other sensitive information.
    b. Ensure keys are erased from memory during firmware update operation.
    c. Have authentication procedure to change Flight Parameters or have some parameters hidden or immutable unless Flight Module Provider supplies it post verification.

2. **Hardware Tamper Avoidance:** *There can be a possibility of changes to the onboard hardware like replacing Flight Controller or GLPS module, which might again lead to deviation from guidelines.*
    a. Secure Unique Identification of crucial hardwares like Radio Modules, GLPS and Flight Controller might be able to avoid this.
3. **Spoof Avoidance:** *Ensure that the Flight Controller can't be run as hardware in the software loop by connecting over provided external interfaces, a feature available by default in many flight control softwares.*
4. **Link Hijack Avoidance**
5. **Drone System Failure Actions:** In cases of hardware or software failure, the drone system must have excessive audio visual notifications to raise alarm. Failures to Test for:
    a. GLPS Failure.
    b. Sensor Failure.
    c. Inability to hold altitude due to one or more onboard hardware failures.
    d. Battery Failure, if there is a power cut-off for any reason, the notification system be given isolated power for raising alarm.

    In addition to raising the audio visual alarms the drone system must initiate manual-mode recovery actions as decided by the manufacturer. In severe fault cases, the drone system must automatically trigger recovery actions as decided by the manufacturer.

7.2 Registry of Certified Registered Flight Modules

The list of certified RFMs will be made available via a registry for third party applications to consume. These applications are expected to check with this registry during RFM service installation (if applications are managing these) and usage. There shall also be a registry for pre-certified RFM services.

7.3 Registry of Digital Sky Service Providers

DGCA shall make available a machine readable list of all certified DSPs

7.4 Items Under-Discussion for Next Release of Specifications

- Hardware
    - Implementation of Trusted Execution Environment
- Software
    - Implementation of Pre Flight Checks
    - Possible Scenarios in case of Time Overrun and/or Geofence Breach - R2H/Safe Recovery in Controlled Airspace/etc
- Responsibility shift of management server to RFM and DSP and interoperability between DSP and hardware

Chapter 8

Procedure for acceptance of RPAS model for Digital Sky

This is prerequisite requirements before acquisition of RPAS by user/ operator. Manufacturers should comply with the requirements laid down in Para 15 of the CAR Section 3, Series X, Part I for operation of RPAS in India.

The procedure for acceptance of RPAS model complying with digital sky platform is divided into 4 stages.

Stage-1:- Manufacturing of RPAS

All OEM/ Manufacturers/ Assembler of RPAS (except Nano) in the country as well as in foreign country (intending for operation in India) should develop the RPAS in accordance with the requirements laid down in CAR Section 3, Series X, Part I and Chapter 6 & Chapter 7 of RPAS guidance manual.

Stage-2:- Submission of documents

OEM/ Manufacturers/ Assembler should submit an application to DGCA or certifying agency accredited by QCI along with documents listed below:

- Certificate of Compliance
- Compliance Matrix (compliance checklist)/ Master Index (list of documents) as applicable
- Detailed drawings (Structural wireframe, 3D view, wiring diagram, pictures, etc.)
- Analysis Reports
- Test Report (Ground/ Flight)
- Manufacturing Process
- Material procurement record
- Consolidated hardware and software independently verified and validated
- RPA flight manual/ manufacturer's operating manual
- Maintenance manual/ guidance/ procedure
- Maintenance inspection schedule/ overhaul interval
- Self-explanatory information booklet for end users
- Educative materials regulations of the country including do's & don'ts
- Other relevant technical literature/ reports – NPNT compliance, equipment compliance etc.

Stage 3:- Scrutiny of documents and familiarisation meeting

- The application will be scrutinised by the concerned officers in DGCA or the certifying agency. The officer responsible should verify the documents submitted and intimate for any shortfalls.
- Shortfall documents submitted by the manufacturers should be verified by the officer responsible and process for further necessary action.

- Familiarisation meeting (if required) may be organised in DGCA HQ or in the facility of the manufacturer's for understanding the design, manufacturing process and compliance to regulations.
- Test report generated on NPNT test tool (available on Digital Sky Platform) to be submitted to DGCA.

Stage 4:- Acceptance of Model and uploading on Digital Sky

- The testing of NPNT compliance may be verified by Certifying Agency.
- Further, actual flying and demonstration may be conducted at agreed/ designated test site to check compliance to regulations. After satisfactory demonstration, certifying agency will provide a compliance certificate.
- With compliance certificate, manufacturer will approach DGCA. The concerned DGCA officer will recommend the acceptance of RPAS model to competent authority for their approval and acceptance letter will be issued to manufacturer.
- Subsequently, the RPAS model no. along with specification will be populated on Digital Sky portal for easy trails for user/ importer/ operator/ remote pilot to pick their correct model from the list.

Note:-

1. For interim measure till such time certifying agencies are on boarded, all acceptance process will be undertaken by DGCA and it will be provisional and time bound. The manufacturer has to go through the certification scheme as and when it is made available.
2. For actual flying and demonstration by Foreign OEM (if required), a onetime import clearance may be provided by DGCA.
3. Any relaxation if required for acceptance of the RPAS may be processed as per CAR Section 1, Series B, Part III with the approval of competent authority depending upon the merit in the application made.

Checklist for acceptance of RPAS model

(To be filled by DGCA official)

Sl No.	Checklist Item	Remarks
1.	Name and Address of Manufacturer	
2.	Model No.	
3.	Type of RPAS (Fixed-wing / Rotary wing)	
4.	All-up-weight and category	
5.	Power plant - Engine/battery operated	
6.	Payload	
7.	Type of data-link used for communication (frequency band etc.).	
8.	Compliance to Digital Sky Platform Specifications for "No Permission – No Takeoff (NPNT)" technical literature/ reports (if applicable)	
9.	Documents submitted	
	• Certificate of Compliance	
	• Compliance Matrix/ Master Index	
	• Detailed drawings	
	• Equipment Type Approval (ETA)	
	• Analysis Reports & Test Report (Ground/ Flight)	
	• Manufacturing Process	
	• Consolidated hardware and software independently verified and validated	
	• RPA flight manual/ manufacturer's operating manual	
	• Maintenance manual/ guidance/ procedure including inspection schedule/ overhaul interval	
	• Self-explanatory information booklet for end users	
	• Educative materials regulations of the country including do's & don'ts	
	• Other relevant– NPNT compliance, equipment compliance, Organisations registration certificate, undertakings, etc.	

10.	Instruments/ Equipment(if applicable)	
	• Global Navigation Satellite System (GNSS) receivers for horizontal and vertical position fixing.	
	• Geo-fencing capability.	
	• Autonomous Flight Termination System or Return Home (RH) option.	
	• Flashing anti-collision strobe lights.	
	• RFID and GSM SIM Card.	
	• Flight controller with flight data logging capability.	
	• SSR transponder (Mode 'C' or 'S') or ADS-B OUT equipment.	
	• Barometric equipment with capability for remote sub-scale setting.	
	• Detect and Avoid capability.	
11.	Any Exemption required/ granted	
12.	Signature of the officer scrutinising the case	
13.	Name and designation of the officer scrutinising the case	
14.	Signature of the officer reviewing the case	
15.	Name and designation of the officer reviewing the case	
16.	When found satisfactory, prepare a detailed note recommending for the acceptance & a draft acceptance letter for approval of competent authority	

Chapter 9

Authorisation procedures for operations of RPAS on case-by-case basis

1. The authorisation procedures for operations of RPAS on case-by-case basis are categorised based on specific purpose e.g. BVLOS, Night Flying, flying above 400ft/ in controlled airspace, Agricultural Spraying, Aerial Photography in no-drone zone, beyond VMC/ manufacturer's specifications/ R & D, or combination of any of the above.
2. The applicants after obtaining UIN and UAOP for normal operations may then apply for specific purpose operation for examination and subsequent endorsement for specific operations in the UAOP.
3. For RPAS operators intending to operate beyond the conditions specified in Para 12.2 and 12.3 of the CAR Section 3, Series X, Part I using the proviso of Para 14.1 of the above mentioned CAR should use the following procedures.

    i. For the RPAS Operator intending for BVLOS operation (day)

    - BVLOS operations shall be to conduct experimental BVLOS operations of Remotely Piloted Aircraft Systems (RPAS) in controlled conditions within identified and segregated low altitude Indian territorial airspace for a period of at least 2 months, to collect evidence, prepare safety case and submit Proof of Concept (POC) to DGCA.
    - The proposed experimental BVLOS RPAS operation should be conducted by team of expert agencies and services providers, known as Consortium.
    - Consortium partner and their role are specified below:

CONSORTIUM PARTNER	ROLE
Project Coordinator	Represents the consortium of experts. He/ She will be the single point of contact representing each consortium and will be responsible for achieving the milestones laid out in the proposal.
UAS Operator	Operate UAS and comply with all the safety standards and risk mitigation strategy for UAS operations
UTM Service Provider	Provide UTM services including situational awareness to UAS operators and coordination with ATC
Supplementary Service Providers (SSP)	Provide 3D maps, weather data, surveillance and telemetry data of manned and unmanned aircraft, population data etc.
Agencies for Data Acquisition & Analysis	Collect, collate and analyse data
SMS Expert	Preparation of safety case and proof of concept

- The Project Coordinator, on behalf of the Consortium, should submit a proposal for conducting experimental BVLOS RPAS operations, to DGCA, for assessment and approval. The proposal should also contain proof of qualification and experience of members and partner companies of the Consortium. The proposal should also contain an undertaking executed by the partners forming the Consortium on their roles and responsibilities in the proposed experimental BVLOS operation.
- Experimental BVLOS operations should be conducted in low traffic density, uncontrolled (Class G) airspaces (Green Zone) below 400 ft AGL, preferably in sparsely populated areas to reduce the risk of collateral damage.
- BVLOS Sorties should be conducted during day only and subject to meteorological conditions specified in the Para 12.3 of the CAR.
- Operations may be as VFR or IFR flights, but VMC should prevail at take-off and landing areas.
- Weather limitations stipulated by UAS manufacturer should be complied with.
- UAS launch and recovery areas should be identified along with alternate sites.
- Remote Pilot should hold a valid manned aircraft pilot license (at least PPL) and should be authorised to operate experimental BVLOS flights by DGCA.
- Safe VLOS track record of the UAS operator and the remote pilot is a pre-requisite for conducting experimental BVLOS operations.
- Flight Plan should be filed for each sortie of experimental BVLOS flight. Energy reserve of 15% of flight time should be provisioned for.
- Clearance should be obtained from concerned ATC unit before commencement of experimental flights. Completion of each sortie should also be informed to ATC.
- Each Consortium should establish mobile or stationary Control Rooms covering both launching and landing areas of RPAS. The control rooms should be accessible to authorised personnel for monitoring and regulating BVLOS experimental operations if required.
- Each BVLOS experiment should be monitored by a team of authorised personnel, on behalf of BEAM Committee, which should include an AAI ATC officer and IAF Air Defence Officer. The presence of AAI/IAF officers should be mandatory for a period of 5 days at the start of the experiment, which, can then be reduced to random inspections.
- Principle of non-exclusivity will be followed while approving BVLOS experiments. This means that no consortium will have

exclusive right to conduct BVLOS experiments in a particular airspace bubble assigned to them. If there are more than one consortia applying for conducting experiments in the same general airspace, experiments should be conducted on time-sharing basis.

- Only micro (meeting equipment requirement + UAOP) and small RPA having autonomous and DAA capability will be allowed for such operations.
- Consortium should develop Standard Operating Procedures (SOP) for coordinating with ATC in normal and abnormal situations such as C2 lost link. The consortium should carryout hazard identification and risk management (e.g. JARUS SORA methodology).
- Experimental BVLOS operations should be attempted only after all risks are brought within acceptable level of safety.
- Consortium should submit detailed testing procedures, coordination procedures with ATC and HIRM report to DGCA for permission for commencement of experimental BVLOS operations.
- The proposals submitted to DGCA will be evaluated by an Expert Committee known as BVLOS Experiment Assessment and Monitoring (BEAM) Committee. The BEAM Committee, on examination of the proposal, may reject or recommend to DGCA for approval of the proposal, along with recommended amendments, if any.
- DGCA may issue written approval with operating conditions and limitations to each Consortium for conducting experimental BVLOS operations. Exemptions if required for allowing such operations will invoke procedures specified in the Chapter 10 of this manual.
- The approval will be for a stipulated time period or until regulations specific for BLVOS operations comes into effect.

ii. For the RPAS Operator intending for BVLOS operation (night)

- BVLOS Sorties should be conducted during day only and subject to meteorological conditions specified in the Para 12.3 of the CAR. On successful completion of day BLVOS experiments for at least 1 month, night operations may be considered by DGCA (safety case) based on the analysis carried from the collected data.
- Only IFR operations shall be permitted during night.

iii. For the RPAS Operator intending for BVLOS operation (above 400ft and/ or in controlled airspace)

- Not permitted/ Reserved

iv. For the RPAS Operation beyond meteorological conditions specified in the Para 12.3 of the CAR/ RPAS operations by manufactures or R&D Organisations:

- Only Manufacturers/ R&D Organisations involved in the development of RPAs may be allowed for such operations. Such operations will be restricted to the test sites or green zone in coordination with concerned ATC and local administration.
- In case any other entity (UAOP holder) desires for such operations should justify the reason with having safety risk assessment carried out in consultation with the RPA manufacturer of the model with which the experiment/ operation is required to be carried out.
- The proposals submitted by such applicants to DGCA will be evaluated by BEAM Committee. The BEAM Committee, on examination of the proposal, may reject or recommend to DGCA for approval of the proposal, along with recommended amendments, if any.
- DGCA may approve such operations with operating conditions and limitations. Exemptions if required for allowing such operations will invoke procedures specified in the Chapter 9 of this manual.
- The approval will be for a stipulated time period.

v. For the RPAS Operator intending for discharging or drop substances

- Not permitted/ Reserved

vi. For the RPAS Operator intending for combination of RPAS operations specified above.

- Not permitted/ Reserved