NPNT SOLUTION

-PATANJALI MAITHANI

Scope of this presentation

This presentation specifies a robust solution for a RFM to attain NPNT compliance .

Main objectives of NPNT

For attaining NPNT compliance , a flight module provider is supposed to develop following infrastructure.

1) Inside RFM
2) A Flight Module Management Client
3) A Flight Module Management Server

Goals of Inside RFM Infrastructure

1)**Key pair generation**: We aim to achieve Level 1 compliance (i.e In TEE), in which key pair generation takes place inside the hardware RFM module itself.(TEE-Trusted Execution Environment, more specification yet to come on this in later release of the RPAS guidance manual)

SOLUTION: A program for randomly generating two 1024-bit long prime numbers and performing multi-precision modular arithmetic is flashed upon the RFM module and called upon whenever a key rotation is required.

2) **Parsing permission artefact and validation**: Permission artefact(PA) is an XML document which contains the information of permitted geospace and time period for the flight to be taken by the RPAS. This document is digitally signed by the DGCA to ensure that the information attached to it is non-tampered and has its original source from the DGCA.

SOLUTION: The transfer of PA from management client(MC) to RPAS is done using MAVSDK FTP class(File Transfer Protocol). To make sure that the PA has come from the particular MC, Public Key Cryptography is used, where minimum key length is 128 bit(as specified in the RPAS guidance manual). Once the file is sent to the RPAS, information from various nodes can be fetched and processed as per the standards given in the RPAS guidance manual. XML canonicalization, SHA256 and RSA decryption are the programs that are written inside the RFM module firmware to make the validation of the XML document possible. The DGCA Public key is securely installed on to the RFM, once validated on the management server(MS).

3) **Monitoring Geofence for breach**: If during flight, RPAS overrun the limit of allowed time period or passes the permitted geospace, Return to home(RTH) action should get implemented. Along with the RTH, the timestamp and geo coordinates are supposed to be logged at a minimum rate of 1Hz in the log file.

SOLUTION: A program is written to read the constantly updated position output from the EKF and check if it lies inside the polygon specified by the latitude and longitude coordinates in the permission artefact. If the position output from the EKF turns out to be outside the permitted geospace then the RTH action is enabled and side by side log filing is also initiated.

4)**Signing logs using private key:** 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.

SOLUTION: A program is written inside the RFM module to generate the json format log file according to the schema defined in the RPAS guide manual. For signing the flight logs, RSA encryption(private key of flight module is used)and SHA 256 algorithms are used.

Summary for Inside RFM Infrastructure

Following key features are to be embedded in RFM module.

1)Key Pair Generation

2)Parsing permission artefact and validation

3)Monitoring Geofence(time and position)

4)Generation and signing of Flight logs.