D2.2-TN1: CERTIFLIGHT service CONOPS

DELIVERABLE DETAILS			
Deliverable Nr	**Lead Beneficiary**	**Dissemination Level**	**Status**
D2.2	d-flight	PU	CONTROLLED
Edition	**Revision**	**Issue**	**Document Code**
01	00	01.00	D2.2_01.00
File Name	D2.2-TN1 Certiflight Service Conops_01.00		
Ref. Template	D0.0-Certiflight Document Template_01.00.dotx		

DOCUMENT HISTORY					
Issue	**Date**	**Status**	**Author**	**Partner**	**Change Description**
00.01	14/04/2023	DRAFT	M. Formato	d-flight	First draft and consolidation of document structure
00.02	04/07/2023	DRAFT	M. Formato F. Russo	d-flight TopView	Updated sections 3 and 4
00.03	15/07/2023	DRAFT	A. Russo M.Nisi S. Maurizi	TSP	Edit of sequence diagrams in paragraph 4.2
00.04	19/07/2023	DRAFT	A. Mennella F. Russo M. Formato	TopView d-flight	General Review of the document Integration of Authenticated tracking sequence diagram
01.00	24/07/2023	CONTROLLED	A. Mennella V.M. Ascione	TopView	Formal review of the coordinator

APPLICABLE DOCUMENTS		
Ref.	File Name	Description
AD 1	Grant Agreement-101082484-CERTIFLIGHT	Project Grant Agreement

REFERENCE DOCUMENTS		
Ref.	File Name	Description
RD 1	Commission Implementing Regulation (EU) 2021/664	This Regulation lays down rules and procedures for the safe operations of UAS in the U-space airspace, for the safe integration of UAS into the aviation system and for the provision of U-space services
RD 2	Commission Implementing Regulation (EU) 2021/665	The document amends Implementing Regulation (EU) 2017/373 as regards the requirements for air service providers of traffic management/air navigation services and other functions of the air traffic management network in the designated U-space airspace in the controlled airspace.
RD 3	Commission Implementing Regulation (EU) 2021/666	Amend regulation (EU) n. 923/2012 regarding the requirements for manned aviation operating within the U-space airspace.
RD 4	Commission Delegated Regulation (Eu) 2019/945	This Regulation lays down the requirements for the design and manufacture of UAS. It also defines the type of UAS whose design, production and maintenance shall be subject to certification. It also establishes rules on making UAS intended for use in the 'open' category and remote identification add-ons available on the market and on their free movement in the Union.
RD 5	Commission Delegated Regulation (Eu) 2019/946	Allocation of funding from the general budget of the Union to cover the costs for the development of the European Travel Information and Authorisation System.
RD 6	Commission Implementing Regulation (EU) 2019/947	Rules and procedures for the operation of unmanned aircraft.
RD 7	AMC and GM to Implementing Regulation (EU) 2021/664 — Issue 1	Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space.

REFERENCE DOCUMENTS		
Ref.	File Name	Description
RD 8	AMC & GM to Regulation (EU) 2019/947 — Issue 1, Amendment 2	Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft.
RD 9	ASTM F3411-22 - Standard Specification for Remote ID and Tracking	This specification covers the performance requirements for remote identification (Remote ID) of unmanned aircraft systems (UAS)
RD10	ISO 23629-12:2022	This ISO standard UAS traffic management (UTM) — Part 12 contains Requirements for UTM service providers. This document includes compliance monitoring, safety, security, privacy, and other organisational requirements for providers in the context of UAS traffic management services.

This document is part of a project that has received funding from the EUSPA under grant agreement No 101082484 under European Union's Horizon Europe programme.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Union Agency for the Space Programme ('granting authority'). Neither the European Union nor the granting authority can be held responsible for them.

SUMMARY

LIST OF FIGURES

LIST OF TABLES

Abstract

This technical note document describes the concept of operations (abbreviated CONOPS) of CERTIFLIGHT platform. The CONOPS is a document that summaries the high-level operational concept and approach for a particular system or service. The CONOPS provides a broad understanding of how an actor is intended to operate the system, highlighting its functionalities, procedures, outcomes, and interactions with other entities. In our case the CONOPS of CERTIFLIGHT platform describes the characteristics of the system from the point of view of the final user, describing who are the actors and the stakeholders of the services offered, which privileges they have on the platform and which kind of operations they can execute.

The document is also used to communicate the quantitative and qualitative characteristics of the CERTIFLIGHT system to all stakeholders, providing a common basis of understanding of CERTIFLIGHT services in the relevant operating environment.

The document is divided in three sections:

- Chapter 2 describes the operating environment where the relevant CERTIFLIGHT services are supposed to be used.
- Chapter 3 highlights the Core services of CERTIFLIGHT platform and the main actors that will benefit of such services.
- Chapter 4 describes the CERTIFLIGHT concept of operations in terms of high-level elements, stakeholder views and operational workflow for the most important cases of utilization pf the platform. The high-level sequences of operations are reported for a comprehensive understanding of the interactions among main CERTIFLIGHT entities.

Finally, the content of this technical note will be included in the D2.6 deliverable for a better understanding of the System Requirements and for the design justification of CERTIFLIGHT platform architecture.

1 Scope of the document

The objective of this document is to develop the high-level CONOPS of the service based on the user's need and the Use Cases analysed in detail in D2.1. This document will identify the actors the nodes, links, and expected outcomes of CERTIFLIGHT services, considering their interfaces with the existing U-space/UTM Platform. This document represents the D2.2 contractual deliverable related to the activities undertaken in Task 2.2 showed in the study logic hereafter reported.

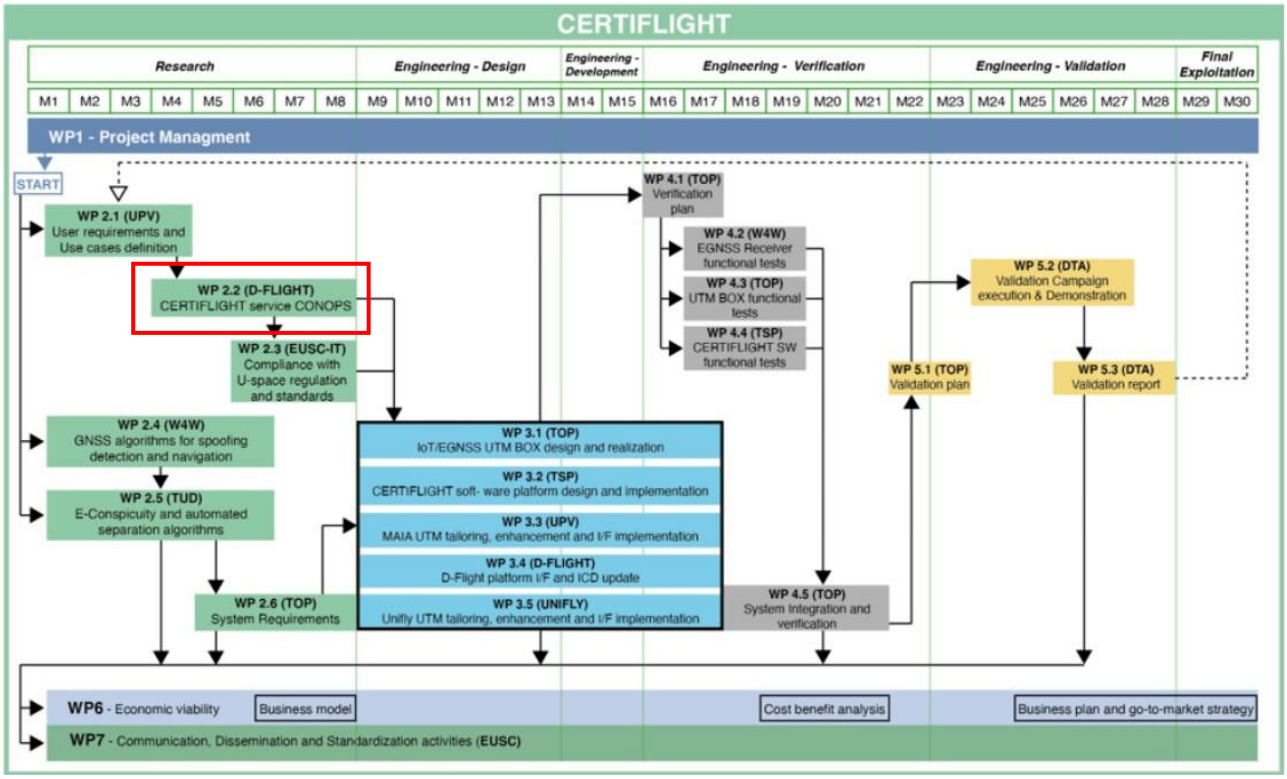


Figure 1-1 Work Breakdown Structure

1.1 Acronyms

Acronyms	Description
AAM	Advanced Air Mobility
ADS-B	Automatic Dependent Surveillance - Broadcast
AMC-GM	Acceptable Means of Compliance – Guidance Material
ARS	Accident and incident Reporting Service
ATC	Air Traffic Control
AuTRS	Authenticated Tracking Service
BVLOS	Beyond Visual Line of Sight
CIS	Common Information Service
DLS	Digital Logbook Service
EVTOL / eVTOL	Electric Vertical Take Off and Landing
FATO	Final Approach and Take-Off
FLARM	Flight Alarm
GME	Ground Movement Equipment

Acronyms	Description
IAM	Innovative Air Mobility
IAS	Innovative Aerial Services
IFR	Instrument Flight Rules
LRS	Legal Recording Service
OSNMA	Open Service Navigation Message Authentication
RID	Remote Identification
SmaCoM	Smart Contract Management
STOL	Short Take-Off and Landing
TLOF	Touchdown and Lift-Off
TRS	Tracking service
UAM	Urban Air Mobility
UAS	Unmanned Aircraft System
USSP	U-space Service Provider
UTM	Unmanned Aircraft System Traffic Management
VFR	Visual Flight Rules
VLL	Very Low Level
WP	Work Package

Table 1-1 Acronyms list

2 Operating environment

This chapter is intended to provide the context(s) in which the relevant CERTIFLIGHT services are used. A first general description of U-space and Innovative Air Mobility is provided. The nature of the airspace (U-space and non-U-space) and the related ground infrastructure are then described.
According to the Drone Strategy 2.0, on the civil side of the drone's eco-system, the drone services include the following interlinked segments:

- Innovative Aerial Services (IAS), including two segments:
  - Aerial Operations: surveillance, inspection, mapping, imaging, etc.
  - Innovative Air Mobility (IAM), covering international, regional and Urban Air Mobility (UAM)
- U-Space - the European ecosystem of services and specific procedures designed to support safe, efficient, and secure access to airspace for drones' operations.
  With the U-Space framework applicable from 26th of January 2023[1] there have been defined new services for drone operators, extending their operation spectrum and airspace where to conduct operations and provide a better definition of the roles and responsibilities of the entities involved in the definition of U-space. Also, with these, any drone operator planning flights in U-Space is required to subscribe to one of the U-space service providers (USSPs).

The European Union Aviation Safety Agency (EASA) Concept of Operations (CONOPS) defines the IAS as "the set of operations and/or services enabled by the new airborne technologies - the operations and/or services include both the transportation of passengers and/or cargo and aerial operations (e.g., surveillance, inspections, mapping, telecommunication networking)"

The concept of Innovative Air Mobility (IAM) aims to accommodate operations with novel aircraft designs (that do not automatically fall under one of the known categories, but which have vertical take-off and landing (eVTOL) capabilities for take-off and landing, specific distributed propulsion features, that can be also operated in an unmanned configurations), that are conceived to offer a new air mobility of people and cargo, in particular, in congested (urban) areas based on an integrated air and ground-based infrastructure. IAM describes a diverse array of aircraft types (such as manned and unmanned), whose designs are enabled by ongoing innovations particularly in the areas of hybrid and electrification of propulsion systems, energy storage, lightweight materials, digitalisation, and automation. These innovations have made possible an array of novel designs spanning multi-rotor, tilt wing, tilt-rotor, powered wing, offering short take-off and landing (STOL) through to VTOL capabilities.[2]

[1] *An extensive analysis of the regulations is provided in Deliverable D2.3.*
[2] *European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', Brussels, 22.11.2022*

Figure 2-1 - Categories of Innovative Aerial Services proposed in the EU Drone Strategy 2.0

2.1 U-space

U-space is a set of services that are based on a high level of digitization and automation of specific functions and procedures designed to support safe, efficient, and secure access to airspace for a large number of drones. For this reason, U-space is an enabling framework designed to facilitate any type of routine mission, in all classes of airspace and all types of environments, even the most congested, by addressing an appropriate interface with the manned aviation and air traffic control. In support of this initiative, the SESAR Joint Undertaking drafted the U-space project in 2017, a vision of how to make U-space operationally possible. The project proposes the implementation of 4 sets of services to support the EU aviation strategy and regulatory framework on drones:

- U1: U-space foundation services covering electronic registration, electronic identification and geofencing;
- U2: U-space initial services for managing drone operations, including flight planning, flight approval, tracking, and interfacing with conventional air traffic control;
- U3: Advanced U-space services that support more complex operations in densely populated areas, such as conflict detection assistance and automatic detection and avoidance features;
- U4: U-space full services, which offers very high levels of automation, connectivity, and digitization for both the drone and the U-space system.

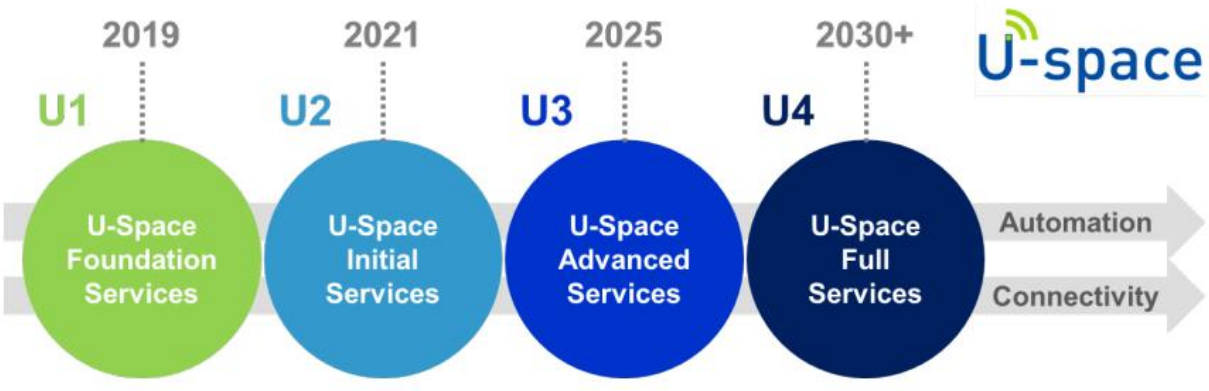


Figure 2-2 U-space implementation roadmap

Each phase of the incremental U-space rollout will offer a new set of services, including an updated version of the services that already existed in the previous phase. For completeness, the following table lists all the services, divided into each implementation phase.

Phase		Service
U1 Foundation Services	U1.1	Registration
	U1.2	Network Identification
	U1.3	Geo-awareness
	U1.4	Registration Assistance
U2 Initial Services	U2.1	Geo-Fence Provision (incl. dynamic geo-fencing)
	U2.2	Emergency Management
	U2.3	UAS Flight Authorisation
	U2.4	Weather Information
	U2.5	Tracking and Position Reporting
	U2.6	Operation Plan Preparation/Optimisation
	U2.7	Conformance Monitoring
	U2.8	Traffic Information
	U2.9	Drone Aeronautical Information Management
	U2.10	Procedural Interface with ATC
	U2.11	Surveillance Data Exchange
	U2.12	Operation Plan Processing
	U2.13	Risk Analysis Assistance
	U2.14	Accident/Incident Reporting
	U2.15	Navigation Infrastructure Monitoring
	U2.16	Communication Infrastructure Monitoring
	U2.17	Digital Logbook
	U2.18	Legal Recording
	U2.19	Geospatial Information Service
	U2.20	Population Density Map
	U2.21	Electromagnetic Interference Information
	U2.22	Navigation Coverage Information
	U2.23	Communication Coverage Information
	U2.24	Citizen Reporting Service
U3 Advanced Services	U3.1	Tactical Conflict Resolution
	U3.2	Collaborative Interface with ATC
	U.3.3	Dynamic Capacity Management

Table 2-1 U-space Service list

In June 2021 U-space regulatory framework (EU 2021/664, EU 2021/665, EU 2021/666) baselined the definition and obligation of U-space ecosystem stakeholders such as ANSPs, U-space Service Providers, Common Information Services providers (where relevant), UAS operators and Manned aviation, consolidating the definition of mandatory services and optional ones (see the ones highlighted in bold in the list above).

In this context the services offered by CERTIFLIGHT platform can be seen both as a suitable implementation of services already considered in the actual regulations (i.e., Tracking) or envisioned in the U-space implementation roadmap (i.e., Legal Recording service, Digital Logbook), or as

innovative services to be proposed to the U-space community and the standardization groups (i.e. Authenticated Tracking, Smart Contract activation)

2.2 Urban Air Mobility

Urban Air Mobility (UAM) is a new air transportation system for passengers and cargo in and around densely populated and built environments, made possible by vertical take-off and landing electric aircraft (eVTOL) equipped with new technologies such as enhanced battery technologies and electric propulsion. These aircraft will have a pilot on board or be remotely piloted. With the number of people living in urban areas increasing by around 3 percent each decade, transport in urban areas is expected to become even more challenging than it is today and UAM can represent a factor of innovation and relief of road transport in our cities.

There are numerous projects underway and planned at European level, which aim to develop the technologies and regulations necessary to allow European countries to play a leading role in the future by developing skills capable of developing not only the Urban Air Mobility but also all those sectors that could benefit from technological innovations related to mobility. Of particular importance is the initiative on Urban Air Mobility promoted by the European Commission within the Smart Cities Marketplace project. There are several initiatives active throughout Europe that are part of the Smart Cities Marketplace project, with an important role for Municipalities and Regions which are increasingly called upon to design future applications in collaboration with regulatory bodies, operators, and industrial players.

The study conducted by EASA on the theme of acceptance by the public was important, which investigated in detail the perception that European citizens have towards these new forms of mobility, the main concerns related to the main applications and identified the main cities where Urban Air Mobility can be successfully developed (Paris, Barcelona, Hamburg, Budapest, Milan, and the Oresund region).

The services offered by CERTIFLIGHT are mainly targeted to all U-space users, though we consider that most of their adoption will be captured in the Certified and in the Specific category, where almost the totality of UAM or AAM operations will take place.

2.3 Airspace

This paragraph describes different aspects of the airspace of interest of CERTIFLIGHT operating environment. The "Urban Airspace" is currently not so used by aviation for reasons of risk and disturbance, especially noise. The general expectation is that Urban Air Mobility will use airspace that is currently mostly unused. ICAO Annex 11 Section 2.6 defines seven airspace classes, A to G, in terms of VFR and IFR flight rules, and the services offered. Only subsets of flight rules {VFR, Special VFR, IFR} are permitted in classes A to G. ICAO Annex 2 defines Prohibited and Restricted areas as being something other than classes A to G. Restricted areas can enable air use which is neither IFR nor VFR. U-space airspace, considered as the enabler for managing complex and dense of UAM and UAS operations, can be deployed in not-controlled and controlled airspace. In this latter case, procedural

or collaborative interface with relevant Air traffic service Unit is necessary to manage (dynamically) the coexistence of both services, U-space, and Air Navigation ones.

2.3.1 U-space airspace

EU regulation 2019/947 Article 15 allows for the creation of Geographic Zones for the management of UAS traffic. EU regulations 2021/664 and 2021/665 allow for a Geographic Zone to be designated a U-space airspace. U-space airspaces are effectively Restricted Areas in the terms of ICAO airspace. EU regulation, therefore, defines a means of operating in U-space airspace which does not include a Tactical conflict resolution service and state that the geographic bounds of U-space airspaces are assembled and published by the CIS (Common Information Service).

The official information published by the CIS, regarding Geographical Zones for the management of UAS traffic, will be those used for comparison against CERTIFLIGHT services. For instance, the CERTIFLIGHT post flight services as the Flight report generation, will be compared with the CIS information to investigate possible airspace infringement situations.

2.4 Ground Infrastructure

The operational scenario must also consider the ground infrastructure.

2.4.1 CNS infrastructure

The CNS infrastructure for U-space services relies on robust and secure communication systems to facilitate real-time data exchange between UAS, ground control stations, and other relevant stakeholders. It encompasses various communication technologies, including cellular networks, satellite communications, and dedicated UAS communication channels. These communication links enable commands and telemetry data exchange, traffic information dissemination, and situational awareness sharing among UAS operators, air traffic management (ATM) systems, and other U-space service providers.

Regarding navigation, accurate and reliable information is vital for safe and efficient UAS operations. The CNS infrastructure incorporates navigation systems that allow UAS to determine their position, altitude, and orientation. This includes the use of satellite-based systems as GNSS as primary navigation infrastructure for UAS. By leveraging these navigation technologies, U-space services ensure that UAS can navigate precisely and adhere to designated flight paths and airspace restrictions. Considering the limited portion of airspace for UAS operations, enhanced navigation services for accurate positioning are strongly demanded.

Effective surveillance capabilities are essential for U-space services to maintain situational awareness and detect potential conflicts or hazards. The CNS infrastructure incorporates surveillance systems that enable UAS tracking and monitoring. These systems may include radar, ADS-B (Automatic Dependent Surveillance-Broadcast) or ADS-B Light (ADL), FLARM, 5G and other sensor technologies. By integrating surveillance data from various sources, U-space services can provide real-time traffic information, detect and avoid collisions, and support strategic deconfliction of airspace.

The CNS infrastructure for U-space services also encompasses robust data management capabilities. It involves the collection, processing, and dissemination of various data types, such as flight plans, weather information, traffic data, and operational restrictions. Data management systems ensure that relevant information is accessible to all stakeholders in a timely and secure manner. This enables UAS operators, U-space service providers, and ATM systems to make informed decisions, coordinate operations, and ensure overall safety and efficiency of UAS operations.

The CNS infrastructure plays a central role in enabling safe and efficient U-space services for drone operations. By providing reliable communication, precise navigation, effective surveillance, and robust data management, this infrastructure ensures the seamless integration of UAS into the airspace. As U-space services continue to evolve, advancements in CNS technologies will further enhance the safety, scalability, and automation of drone operations, enabling a wide range of commercial and societal applications, where CERTIFLIGHT is positioned.

2.4.2 Vertiport

The term vertiport is used here to indicate urban-air mobility airports. Two forms are presented, first the vertiport for passenger operations and then the vertiport for cargo operations with small UAS.
Vertiports are landing and take-off sites for passenger carrying VTOLs and will be equipped with a number of facilities, including charging facilities for electrically operated vertical take-off and landing (eVTOL) vehicles as well as passenger boarding, de-boarding, and waiting areas. Several companies are presently developing vertiport concepts and infrastructure and these are largely inspired by heliports, including the touchdown and lift-off (TLOF) area, the final approach and take-off (FATO) area, the safety area around the FATO and stands as applicable. Additionally, while the aircraft is moved between TLOF and stand without depending on its power and wheels, ground movement equipment (GME) needs to be accommodated in the vertiports. GME serves as towing equipment in the form of a wheeled vehicle to move the aircraft horizontally on the vertiport surface, which can be either manually operated or remotely controlled or supervised by a member of the technical ground crew. Vertiports may be located in any area, but realistically predominantly in urban areas and close to airports, permitting air taxi operations within cities and between cities and airports.

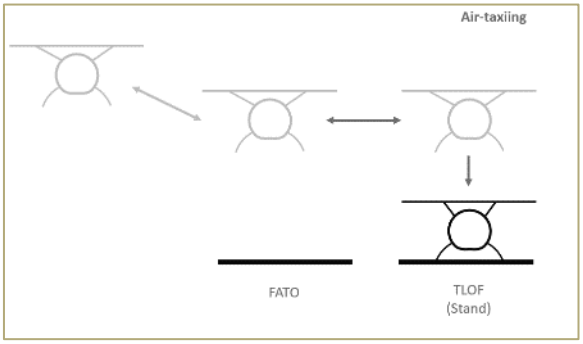


Figure 2-3 Air taxiing in Vertiport

Much of the passenger vertiport description applies to vertiports for cargo flights, but there are some simplifications beyond the absence of passengers. Two modes of cargo flight can be identified linked to the type of operation which impact vertiport location. For the first one the flight takes off and lands with the cargo on board. The cargo vertiport is at a source/sink of cargo, such as a warehouse,

logistics centre, “fulfilment centre” or “dark store.” The location of the vertiport is determined by the location of the source/sink of cargo.
In the second one, the cargo is collected and then delivered during the flight. Aircraft leave and return to the vertiport without cargo. The vertiport is only concerned with flight operations. The vertiport position can be optimised for flight efficiency, safety, and social acceptance.

For the scope of CERTIFLIGHT, vertiport operations including freight delivery can benefit of different services as Smart contract activation to automate a large number of operations and commercial transactions based on specific conditions (i.e., time or position based) achieved during the flight.

3 CERTIFLIGHT Core Services

The purpose of CERTIFLIGHT project is to offer a new U-space service for the legal certification of tracks generated by drones and aircraft flights.
To obtain a flight information with legal significance CERTIFLIGHT combines the already mentioned OSNMA, E-Conspicuity and Blockchain technologies to offer the following core services:

- Tracking (TRS)
- Authenticated Tracking (AuTRS)
- Remote identification (RID)
- Legal Recording (LRS)
- Digital Logbook (DLS)
- Accident and Incident Reporting (ARS)
- Smart contract management (SmaCoM)

Some of the services listed are intended to be as an implementation of standards and EU regulations, while others are brand new and will be addressed to standardization process during the project.
The figure below, highlighted in blue, shows CERTIFLIGHT services which are directly derived from the ISO 23629-12:2022.
It's important to note that RID service is not part of standard. However, the standard reports the Network (electronic) Identification which is a way to implement the Remote ID.

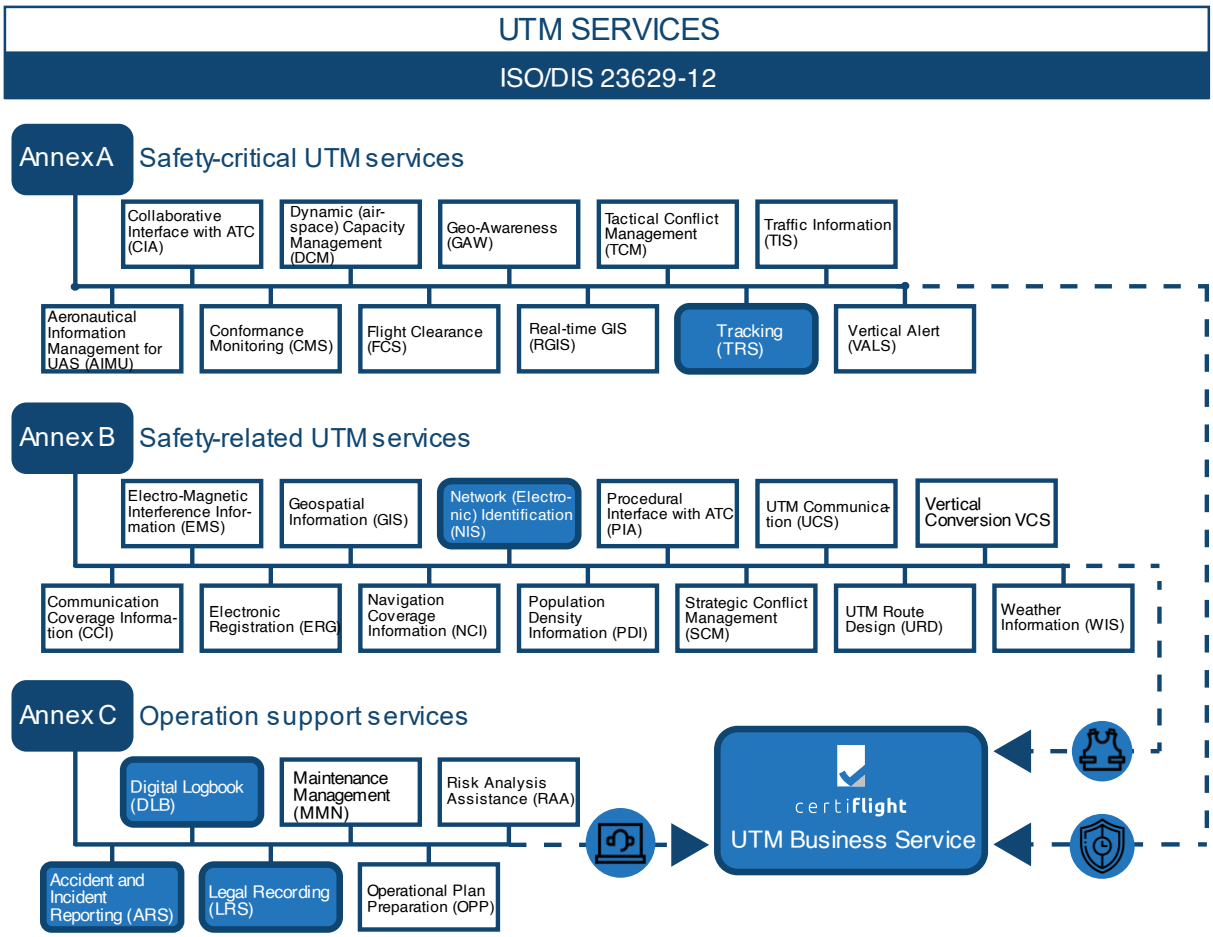


Figure 3-1 UTM services implemented by CERTIFLIGHT - ISO 23629-12:2022

The set of core services offered by CERTIFLIGHT can be distinguished in two types:

- In-flight services
  These services are intended to be mainly in real-time, having an impact on the carrying out of the operations.
- Post-flight services
  These services are intended to be provided at the conclusion of the flight, by storing and processing the data collect.

3.1 In-flight services

The in-flight services provided by CERTIFLIGHT are the followings:

1. Tracking (TRS)
2. Authenticated Tracking (AuTRS)
3. Remote identification (RID)

These services are main related to safety and are based on real-time data processing.

3.1.1 Tracking (TRS)

The Tracking service plays a crucial role for U-space, as it allows U-space service providers to display, monitor and predict the movements of unmanned aerial systems (UAS) in the airspace. It helps ensure safety and prevent potential conflicts between UAS and other aircraft. There are various ways tracking can be implemented in U-space, either as a service provided by the U-space Service Provider, where the position and therefore the movement of the UAS is received (by the producer or by the consumer), either as a shared service between interconnected providers (e.g., exchange surveillance data) or via remote pilot station. It is essential that services such as monitoring, tactical conflict prediction and traffic information have access to tracks rather than observations to ensure accurate and effective airspace management.

3.1.2 Authenticated tracking (AuTRS)

The Authenticated tracking service is intended as an extension of the tracking service included in ISO 23629- 12 Annex A Safety-critical UTM services. This service is not present in the U-space catalogue, and it has been proposed in the standard as amendment of the actual TRS service, providing enhanced functionalities.
This service aims to increase the robustness and the resiliency against GNSS spoofing and meaconing through the authentication of GNSS position exploiting new GNSS authentication features.

The authenticated tracking is a real time service, that USSPs can exploit to inject authenticated tracking data in their systems. Data generated by GNSS enabled receivers are fundamental for the certification of flight tracks especially when data shall be exchanged between USSPs according to the interoperability requirements actually suggested by standardization groups (i.e., DSS in ASTM 3411-22a) but likely to be included in the next upcoming regulations.

The implementation proposed by CERTIFLIGHT project relies on the GNSS service OSNMA offered by Galileo in combination with blockchain technology.

This is a basic service offered by the CERTIFLIGHT UTM Box

3.1.3 Remote identification (RID)

The American Society for Testing and Materials (ASTM) defines the Remote ID as a service which "allows governmental and civil identification of UAS for safety, security, and compliance purposes. The objective is to increase UAS remote pilot accountability by removing anonymity while preserving operational privacy for remote pilots, businesses, and their customers. Remote ID is an enabler of enhanced operations such as beyond visual line of sight (BVLOS) operations as well as operations over people.

The ASTM 3411-22a identifies two types of Remote ID:

- Broadcast Remote ID is based on the transmission of radio signals directly from a UAS to receivers in the UAS's vicinity.
- Network Remote ID is based on communication by means of the internet from a network Remote ID service provider (Net-RID SP) that interfaces directly or indirectly with the UAS, or with other sources in the case of intent-based network participants.

This is a basic service offered by the CERTIFLIGHT UTM Box

3.2 Post-flight services

The post-flight services are provided in the form of dedicated reports resulting from the processing and analysis of data gathered during the flight.
The data processed leads to the generation of two kinds of flight reports:

- Basic Report, which is only based on in-flight services data that are transmitted by the CERTIFLIGHT UTM Box (only) in real time to CERTIFLIGHT platform. This data includes authenticated positioning, time, UAS attitude, navigation parameters and ancillary telemetry data. The basic report offered by CERTIFLIGHT platform is available right after the flight and it is generated using only the data transmitted by the UTM Box. This service is envisioned to have an immediate report of the flight activities undertaken considering only the information transmitted by the UTM Box. Basic Metrics calculated in post flight can be included in the basic report, but not the result of APP and GSD algorithms which needs GNSS observables data and IMU data at higher rate to properly work.

- Full Report, which provides additional information generated from the data logged on the UTM Box. In fact, some data including attitude data, GNSS Observables and UAS payload data, cannot be transmitted in real time, due to the narrow band digital channel used for data transmission, therefore such data will be stored onboard the UTM Box. To generate the full report, the user must download the UTM Box data to CERTIFLIGHT portal with an authenticated mechanism, provided by the embedded SW application, to guarantee the chain of trust. The full data after being stored to the CERTIFLIGHT Portal data base with security mechanisms, are used by the different algorithms and metric generators to create additional information to include in the report. APP and GSD algorithms can be lunched here considering IMU data available at 10 Hz refresh rate and GNSS Observables. GNSS Metrics are fully applicable for this report. Finally, if the UAS Operator decides to upload also UAS payload data to the CERTIFLIGHT portal, it will be reflected in the full report as well.

The basic and the full report represent the core CERTIFLIGHT services. Depending on the configuration and the parameters about how such reports will be requested, they will specialize in the following post-flight services:

1. Legal Recording (LRS)
2. Digital Logbook (DLS)
3. Accident and Incident Reporting (ARS)
4. Smart contract management (SmaCoM)

3.2.1 Legal Recording (LRS)

The Legal Recording Service is intended to assist in the investigation of claims and incidents. The service must guarantee the recording of all information transmitted in the U space and allows a complete view of the state of the system, always. Additionally, the records can be used as a source and augment information datasets for research and education of new technologies. In fact, the processing of the registration dataset using dedicated algorithms, including those based on Artificial Intelligence, makes it possible to identify risky situations and to adapt the parameters for assessing the risk of future operations. However, considering the commercial nature of drone operations, the recordings may not be accessible to everyone but only to authorized profiles/stakeholders.

The Legal Recording service can be implemented with both basic and full report services, however full report service is recommended to include also in the report the outcome of APP and GSD algorithms on top of OSNMA features.

3.2.2 Digital Logbook (DLB)

The Digital Logbook service extracts information from Legal Recording to produce relevant reports for users of the service. First, it will give users access to their own information only. In fact, drone operators and pilots will be able to see information summaries for the flights in which they have been involved: start and end times, locations, aircraft id, distance, track, etc. Drone pilots will then be able to see the entire mission profile and statistics on their flight experience and generally, UAS Operator, will also be able to see the histories/statistics of all the flights of their aircraft in the fleet.
The Digital Logbook service must be implemented in a secure way for the sensitive information it processes and should be able to allow various query functions. For this reason, authorized users, such as accident investigators or the police, can have general access to all data as well as directly concerned (Pilots and UAS Operators).
For the implementation of this service, the basic report offered by CERTIFLIGHT portal is suitable.

3.2.3 Accident and Incident reporting (ARS)

This service allows drone operators and other interested parties to report accidents and incidents. The service is intended to also represent a single storage point for reports, throughout their life cycle and for this reason, given the nature of the information it contains, it must be secure and allow access only to people authorized to process data.

Accident and Incident reporting is closely linked to the Legal recording service and therefore indirectly, of all parts of U-space. There may be some connection between the emergency management service and the accident and incident reporting service; in fact, some emergency events could trigger the automatic creation of an accident/inconvenience report.
Within a U-space Airspace, the service should also be open to other stakeholders, such as anyone who is present during the occurrence of an incident/accident, to report what they have observed regarding UAS-related events. Therefore, the user interface should be designed in a way that also encourages "external" actors to report enough information to identify the affected flights.

For the implementation of this service, the full report offered by CERTIFLIGHT portal is recommended.

3.2.4 Smart Contract management (SmaCoM)

CERTIFLIGHT intends to be the tool to manage the smart contracts.
The smart contracts are simple agreements “if/when/where…then…” statements that are written into code on a blockchain structure.
From the operational point of view, it is possible to identify four main steps of these particular agreements:

1. **Conclusion of the contract,** the parts agree on how transactions and their data are represented on the blockchain, defining specific “if/when/where...then…” rules that govern those transactions and the framework for resolving disputes.
2. **Blockchain validation,** the contract becomes “smart” when entered into the Blockchain. The information stored in the blockchain are inalterable.
3. **UAS as oracle,** the Blockchain cannot access data outside the network. Intervenes the oracle, a third-party agent, that transmits particular data to the smart contract. The oracle in our case is the drone equipped with the OSNMA UTM Box.
4. **Execution,** the actions are executed when the IF/THEN clause have been met and verified. For example: flight delay for critical delivery applications, automatically triggers refund.

Such information is well written and confined in the report that acts as a verification tool to prove the conditions that the parties have agreed during the negotiation phase.
Both basic and Full report are suitable for Smart contract management, depending on the typology of contract that an UAS Operator and a client have agreed.

3.2.5 Summary

The table below summarizes the core services and their background.

Name	Acronym	Service type	Standard and Regulation background
Tracking	TRS	Real-time	• Listed in ISO 23629-12:2022 • Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a

Name	Acronym	Service type	Standard and Regulation background
			regulatory framework for the U-space • ASTM F3411-22A 'Standard Specification for Remote ID and Tracking'
Authenticated Tracking	AuTRS	Real-time	New service proposed in ISO 23629-12 (waiting for feedback)
Remote identification	RID	Real-time	• Listed in ISO 23629-12:2022 as "NIS" • Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space
Legal Recording	LRS	Post-flight	• Listed in ISO 23629-12:2022 • Article 15 of EU2021/664
Digital Logbook	DLS	Post-flight	• ISO 23629-12:2022
Accident and Incident Reporting	ARS	Post-flight	• Listed in ISO 23629-12:2022 • Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space
Smart contract management	SmaCoM	Post-flight	New service to be proposed to suitable standardization group (WP7 activity)

Table 3-1 CERTIFLIGHT core services summary

4 CERTIFLIGHT Service CONOPS

This section describes the CERTIFLIGHT concept of service in terms of high-level elements, stakeholder views and operational workflow.
Starting from the identified User Needs and Use Cases proposed, the consortium identified the main stakeholders of the CERTIFLIGHT services.
The figure below represents a high-level architecture, where it is possible to observe the relationships between the main components of the CERTIFLIGHT service.

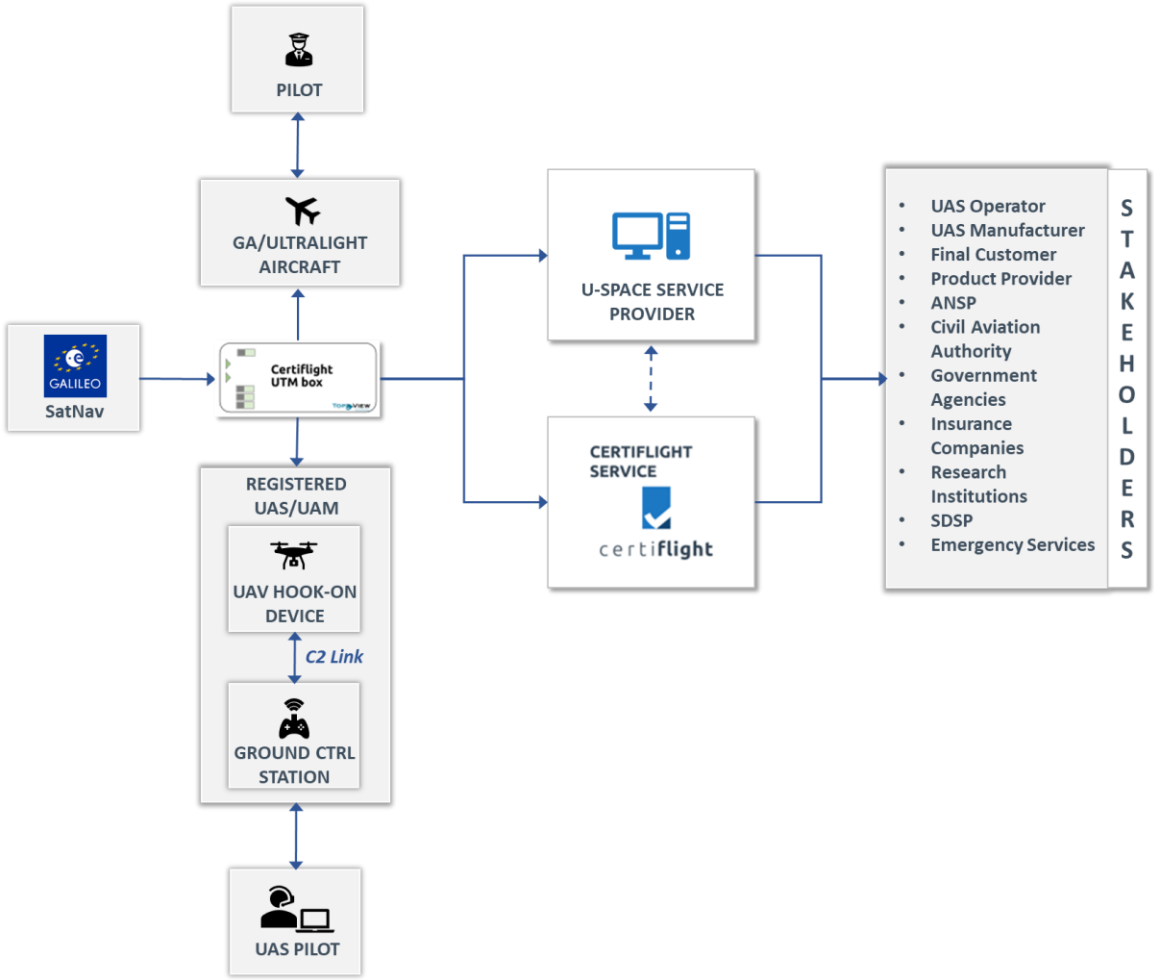


Figure 4-1 General Architecture

The following paragraphs describe the stakeholders and their role as well examples of operational workflow of the service.

4.1 Stakeholders and roles

The architecture of a complex system such as CERTIFLIGHT brings together different elements and requires operating procedures involving numerous actors. For this reason, CERTIFLIGHT can be defined also as a set of microservices and organizations that share a common set of goals and work together to provide specific added value services to customers primarily concerned with security, performance, and legal concerns.

A Stakeholder is an individual, team or organization with interests or concerns related to the CERTIFLIGHT services. The mapping from stakeholder to Use Case can be many depending on the scenario to which it refers. The following figure maps the stakeholders identified in the overall architecture thanks also to the description of the use cases.

Figure 4-2 CERTIFLIGHT stakeholders

The stakeholder can influence directly nor indirectly the service provision. So, to identify the role of each, they can be read as users of CERTIFLIGHT and then divided according to the type of features they can access, the so-called software privileges.

The software privileges refer to the access levels and permissions that are assigned to users of the software.

The privileges of software users can vary depending on the type of software and the level of access or authority assigned to them.

Some common types of privileges that users may have in software are the following:

1. Administrator or superuser: Administrators or superusers are users with the highest level of privileges. They can access all features of the software, including managing the accounts of other users, accessing advanced configuration settings, and performing maintenance or administrative operations. As a result, this level will be reserved to the consortium members.
2. Regular user: They can use the main features of the software but may not have access to advanced settings or account management functions. Regular or standard users have a limited level of access compared to administrators.

3. **Guest or limited user**: Guest or limited users are users with even lower privileges. They typically have access only to basic functionality and may be restricted from performing certain actions or accessing certain sensitive data.
4. **User with specific privileges**: In some cases, specific privileges can be assigned to certain users based on their needs or responsibilities. For example, an authority may request specific data. This user may also access the specific data by dedicated API.
5. **Read-only user**: Some software allows assigning read-only privileges to certain users. These users can view the data or content but cannot make changes or perform actions that can impact the system.

The table below briefly describes the role and the possible access level of each stakeholder.

Stakeholders		
Name	Role	Access level
UAS Operator (Main User)	is the legal entity, performing one or more UAS operations and is accountable for them. Plans and supervises the operation.	Regular User
GA/Ultralight Pilot (Main User)	Pilot in command of the aircraft interested in the presence of nearby drone traffic for his safety. He expects a user-friendly solution capable to assess warning capabilities in case of presence of local drone traffic. Pilots have also interest for proof of no-infringement of airspaces.	Regular User
UAS Pilot	Supervises the flight through his Ground Control Station and is ready for intervention in case of emergencies. The pilot depends directly on the UAS operator, which may assign to the pilot only the features specific for his role	Limited access
Nearby flight operator	Flies in the same airspace of the UAS operator and GA/Ultralight pilot (Main Users). Interested to know the position of other aircraft in the surroundings that may impact his flight activities.	Read-only
UAS Manufacturer	Mainly interested in vehicles and equipment. The UAS manufacturer or a representative may have a role in CERTIFLIGHT Services. It could be indirectly involved, in case of autonomous manoeuvre undertaken by the drone itself without the intervention of the pilot.	Read-only
U-Space Service Provider (USSP)	This stakeholder provides one or more of the U-space services as listed in the U-space paragraph 2.1.	User with specific privileges
Supplemental Data Service Provider (SDSP)	Provides access to supplemental data to support U-space services. E.g., Weather Data Service Provider, Ground risk observation service provider.	Read-only
Civil Aviation Authority	Generic term to encompass national or local civil aviation authority, or some entity delegated by them. It could be Interested in an approved tool for the generation of certification of “No infringement” as a proof or	User with specific privileges

Stakeholders		
Name	Role	Access level
	compliance with conformance monitoring service. It could be also interested in the service outcomes to be aware of the "health status" of the runway during the inspection and as proof in case of accident for investigative purposes.	
Emergency Services	Organisations involved in preparation and execution of emergency services/operations such as fire brigade, emergency, first aid, Search and Rescue (SAR). They could be interested in monitoring the data feed from UAS to increase situational awareness	Read-only
Research Institutions	They study the effectiveness of drone technology in different applications (e.g., in organic agriculture) and develop new techniques and applications.	Users with specific privileges
Final Customer	The Final customer is directly or indirectly involved. He could: • Require goods delivered at precise conditions. • Farmers as primary beneficiaries of drones as they can use it to satisfy the traceability requirements for organic crops. • Power Grid Owner or Powerline Maintenance Company expecting a solution that facilitates efficient integration of drone Operator into the portfolio of power grid monitoring technologies. • Quarry Owner expecting a solution that enables accurate calculation of mined material for asset management and compliance purposes. • Others with specific needs in line with CERTIFLIGHT solution.	Read-only
Product Provider	Use the services of a UAS Operator. (e.g., ships goods, delivery)	Read-only
Air Navigation Service Provider (ANSP)	Air Navigation Service Provider (ANSP) is an organisation that provides the service of managing the aircraft in flight or on the manoeuvring area which is the legitimate holder of that responsibility.	Users with specific privileges
Air Traffic Control (ATC)	Air traffic control service is a service provided for the purpose of preventing collisions (between aircraft, and on the maneuvering area between aircraft and obstructions) and expediting and maintaining an orderly flow of air traffic.	Users with specific privileges
Airport Service Provider (ASP)	Any natural or legal person responsible for providing services at the airport.	Read-only
Government Agencies	Authorities involved in preparation and supervision of the operations of law enforcement such as police (e.g.,	Users with specific privileges

Stakeholders		
Name	Role	Access level
	Traffic Police), security, military, homeland security that are responsible for law enforcement methods.	
Insurance Company	A company that creates insurance products to take on risks in return for the payment of premium may benefit of CERTIFLIGHT report for speed up transactions made by an insurance broker.	Read-only
Port Authority	Organization that controls and manage the activities in a port and could be involved in flight authorization process as geo-zone manager.	Read-only

Table 4-1 Stakeholders roles and feature access level

4.2 Operational workflow

This paragraph presents examples of operation workflow using the UML sequence diagrams.
The unified modeling language (UML) is a general-purpose modeling language that is intended to provide a standard way to visualize the design of a system[3].

These models show the logic behind the actors (people who affect the system) and the system in performing the task. Reading a sequence diagram begins at the top with the actors or the systems. Under each actor or system there are long dotted lines called lifelines, which are attached to them. Actions are performed with lines that extend between these lifelines. When an action line is connected to a lifeline it shows the interaction between the actor or system. Messages will often appear at the top or bottom of a system sequence diagram to illustrate the action in detail. For example, the actor could request to log in, this would be represented by login (username, password). After each action is performed, the response or next action is located under the previous one. By reading down the lines, it is possible to understand how certain actions are performed in the provided model, and in what order. In the sequences the tasks may be repetitive, simple, or complex tasks.

The UML sequence diagram specifies and shows the following:

- External actors
- Messages (methods) invoked by these actors.
- Return values (if any) associated with previous messages.
- Indication of any loops or iteration area

The diagrams in the following paragraphs present different types of action, identified by specific arrows. The types of arrows are listed in table below.

For making the diagrams more readable no exchanging parameters were added in the charts, i.e., login (user, password) -> login.

[3] https://www.uml.org/

Arrow Type	Meaning
synchronous message	The sender waits for the recipient to process the message and returns before continuing with another message. The tip of the arrow used to indicate this type of message is solid.
Return message	The message recipient has finished processing the message and is returning the control to the message caller.
Asynchronous message	The caller does not wait for the recipient to process the message and returns before sending other messages to other objects within the system. The type of the arrow used to show this type of message is a line arrow
Self Message 	A self-message can represent a recursive call of an operation, or one method calling another method belonging to the same object.

Table 4-2 Types of messages in UML sequence diagram

4.2.1 Device factory initialization

The diagram describes the sequence of actions to complete at the very end of the process of manufacturing before the device is distributed to the end-user.
The objective is to proof the genuinity of the device manufactured and to establish the chain of trust of information produced by the Device to the end user.

The diagram assumes the presence of a factory portal, which is a utility to initialize new devices.
The steps of the sequence are the followings:

1. The CERTIFLIGHT selling operator accesses the factory portal to initialize the device.
2. The device generates a key-pair using its secure hardware module and shares the public key with the factory portal.
3. The factory portal forwards the public key to the Device Gateway, which is aware of the identities of all the produced devices. Now the device gateway is prepared for device activation described in the next paragraph.
4. The success response from the gateway makes the device ready for selling.
5. Optionally, to double check the successful outcome of the initialization process, a cryptographic challenge is produced by the Device and verified by the Device Gateway. Such phase is a light simulation of the end-user initialization.

This procedure happens before the sale of the device and it is internal to the CERTIFLIGHT consortium, without any external intervention.

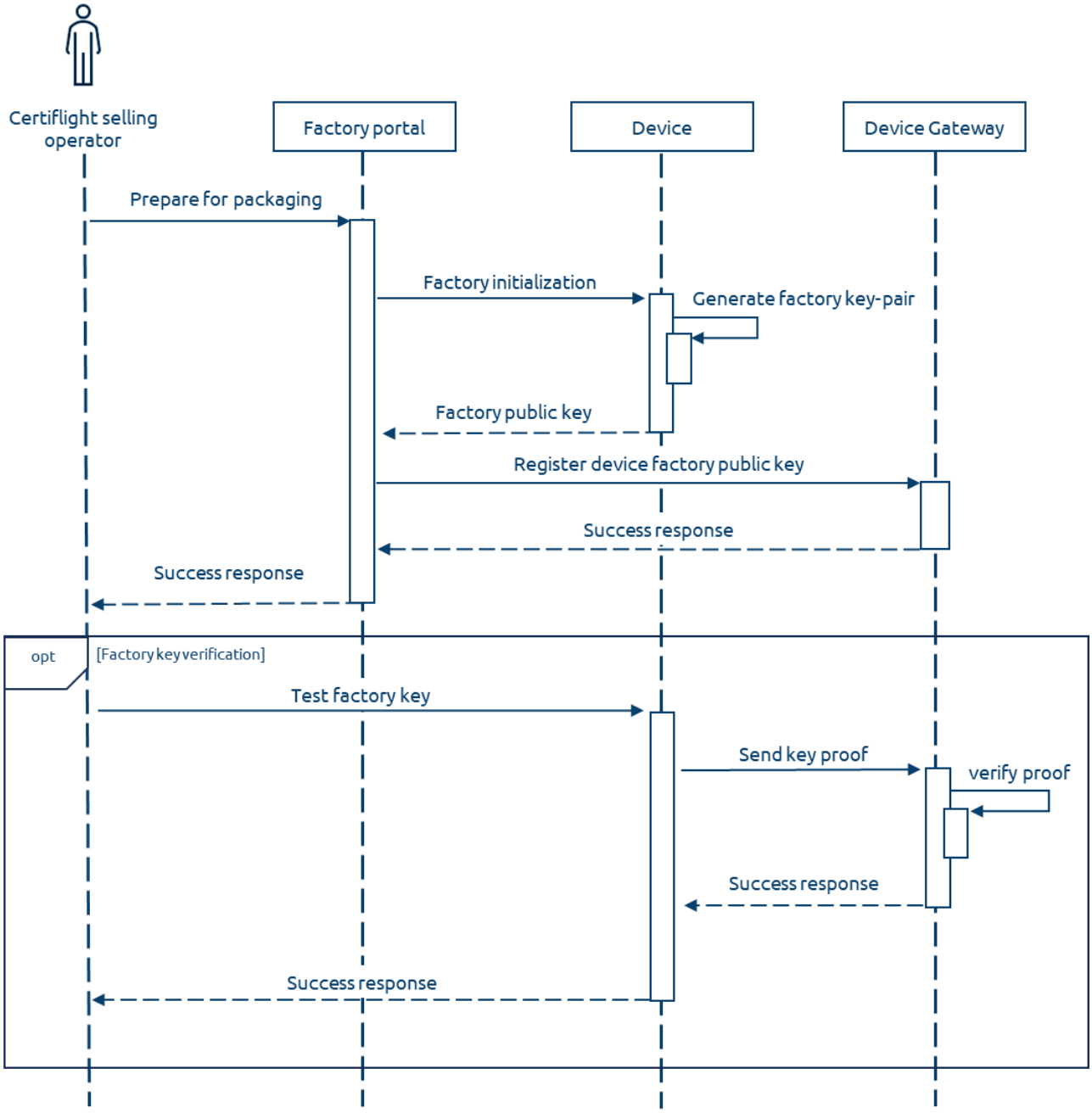


Figure 4-3 Device factory initialization - factory key assignment

4.2.2 Device first activation by the user

This diagram describes the sequence of actions expected to happen in a successful activation by an end-user of a new device.

The steps of the sequence are the followings:

1. The end-user triggers the activation process of the Device.
2. The Device generates an activation message consisting in three sub-steps:
    a. Compute a cryptographic proof of knowledge of the identity generated in the manufacturing post-process.
    b. Generates a new key-pair to use from that moment on.

c. Computes a proof of knowledge of the new identity.
d. The message payload contains the two proofs of knowledge and the new identity public key.

3. The Device Gateway checks the two proofs of knowledge and replaces the old identity with the new identity. Before proceeding with this step, the device gateway must have the key obtained from the factory portal in its register, as described in the previous paragraph. The new key identifies the device as active and genuine.
4. The user provides to the CERTIFLIGHT portal a proof of physical ownership of the Device in the form of a scratchcard/QR/serial code, included with the Device package.
5. The CERTIFLIGHT portal subscribes to the Device data on the Device Gateway using the secret code provided by the user as a proof of ownership.

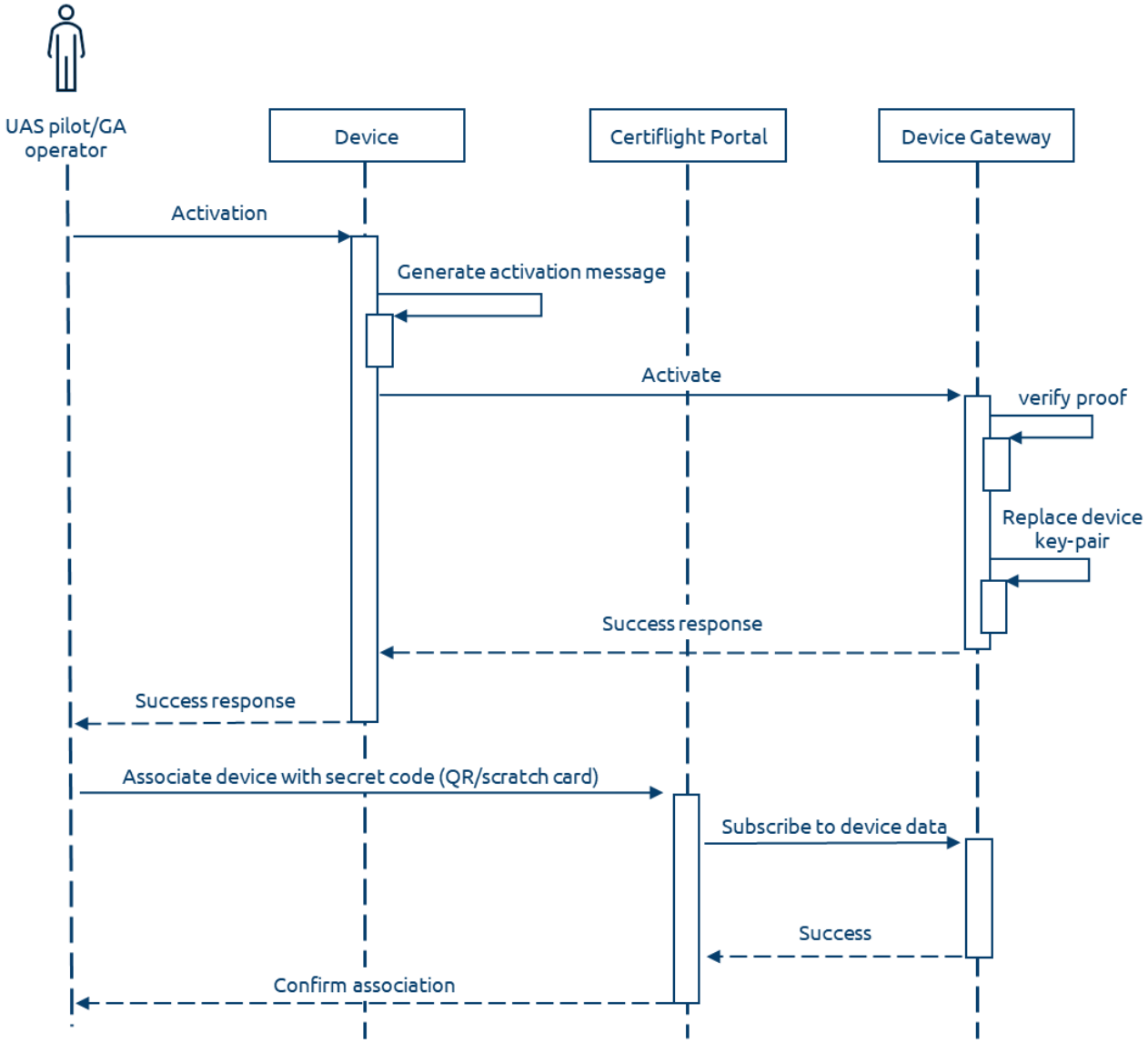


Figure 4-4 Device first activation by the user

4.2.3 In-flight workflow – generation of basic flight report

The diagram describes the sequence of operations which happen during a flight session in which the device has been successfully initialized. The overall mechanism assumes that Device data are always consumed by the subscribed CERTIFLIGHT portal. Any processing on such data is moved to the post-flight phase. The steps of the sequence are the followings:

1. The end-user turns on the Device to start the flight session.
2. The Device establishes a secure communication channel with the Device Gateway.
3. The Device Gateway notifies all the services subscribed to the specific Device data that new data is going to be sent.

Until Device is active:

4. The Device starts receiving the Galileo OSNMA signals and verifies that on-board generated data is authentic.
    a. Once verified, the Device signs the localization (PVT) and related data with its identity key-pair.
5. The Device submits the authenticated and counter-signed data to the Device Gateway
6. The Device Gateway checks the data signature with the Device public key and
    a. forward it to CERTIFLIGHT and the subscribed services,
    b. notifies nearby GA/UAS Devices
7. The CERTIFLIGHT portal provides feedback to the user about the received data (e.g., show on a map)
8. The CERTIFLIGHT portal submits data to the blockchain service in order to register it permanently and gathers integrity references for the report.

If and when user requests a basic report:

9. The CERTIFLIGHT report issues a basic report containing data obtained from the live session of the Device.

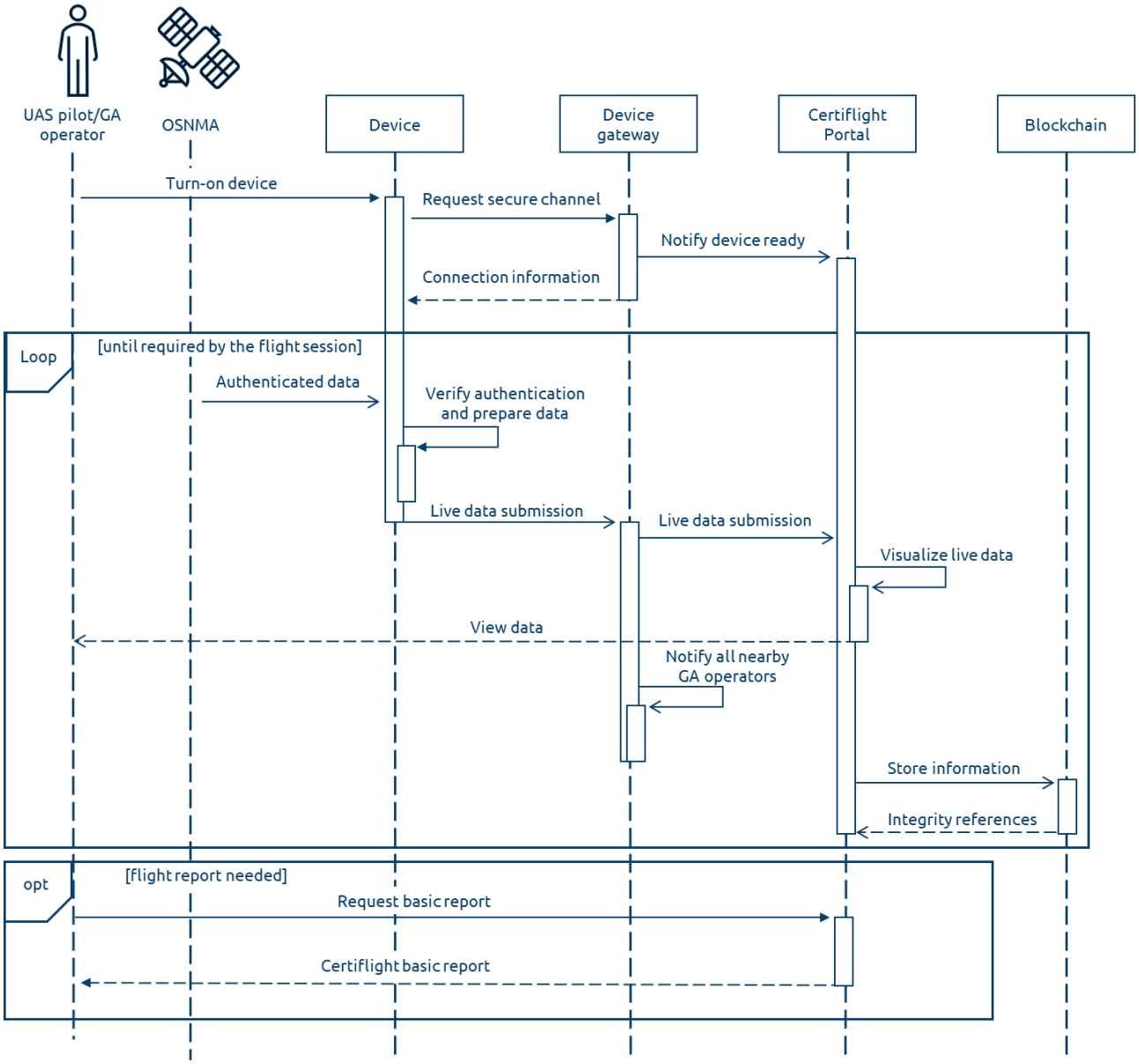


Figure 4-5 In-flight workflow - Basic report generation

4.2.4 In-flight workflow – authenticated tracking

The diagram describes the sequence of operations which happen during a flight session in which the device has been successfully initialized and configured to transmit authenticated GNSS positioning data. The Device data here are consumed directly by the USSP that subscribed the Device Gateway. The very same data are also subscribed by CERTIFLIGHT portal that, in a parallel process, ensures that all data are secure stored to the Blockchain Node. In this way, the USSP that receives authenticated tracking data is also aware that such data are also available for basic report generation through CERTIFLIGHT services.

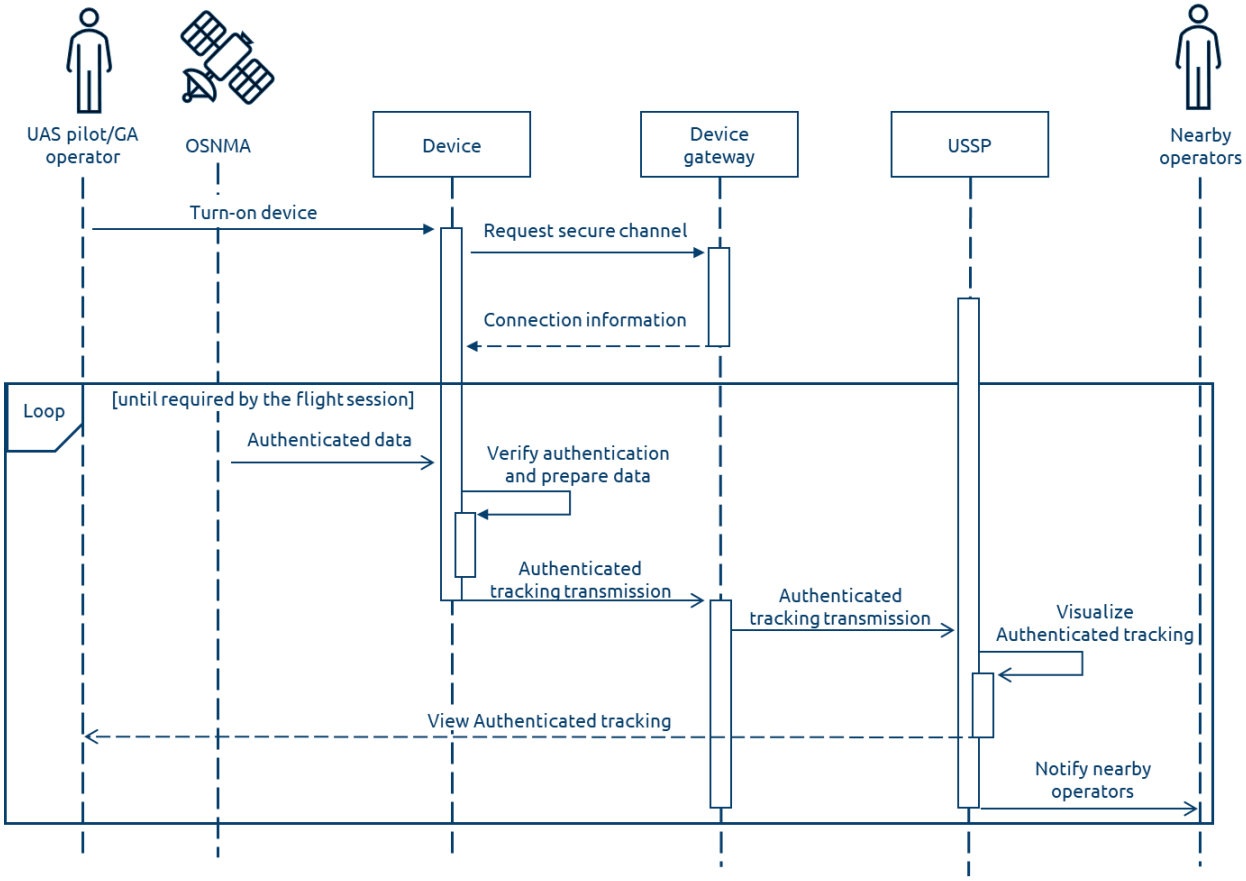
The steps of the sequence are the followings:

1. The end-user turns on the Device to start the flight session.
2. The Device establishes a secure communication channel with the Device Gateway.

3. The Device Gateway notifies all the services subscribed to the specific Device data that new data is going to be sent.

Until required by the flight session:

4. The Device starts receiving the Galileo OSNMA signals and verifies that on-board generated data is authentic.
5. The Device starts to transmit the authenticated tracking positioning data to the Device Gateway
6. The Device Gateway transmits data to the USSP according to the Interface mechanism identified. This operation assumes that the USSP is registered on the Device Gateway or that the UTM Box user (through Device Gateway) has access to the specific USSP with specific API.
7. The USSP portal provides feedback to the user about the received data (e.g., show on a map) with specific graphics or other means to differentiate a simple track displayed from an authenticated track (i.e., different colors of tracks)
8. The USSP notifies to other nearby operators the presence of authenticated UAS or manned Traffic generated by the UTM Box.



4.2.5 Post-flight workflow – generation of full flight report

The diagram shows the sequence of actions designed to happen at the end of a flight session, or anyway when the user needs to issue a full report or consult the result of the post-processing algorithms.

The way in which data are uploaded from the Device to the CERTIFLIGHT portal may still change according to the Device hardware and software implementation.

The steps of the sequence are the followings:

1. Data are exported and uploaded to the CERTIFLIGHT platform.
2. The CERTIFLIGHT portal verifies data authenticity using the Device identity.
3. The supported post-processing algorithms (GSD and APP) are run on the full data. In the same way the metric generator will work with the full list of parameters collected after UTM Box onboard data upload.
4. Full data, along with the post-processing algorithm outcome, is registered to the blockchain service, which provide references to demonstrate data integrity.
5. The successful outcome of the export operation is notified to the user.
6. The user can request the report containing the full data related to the selected flight session.

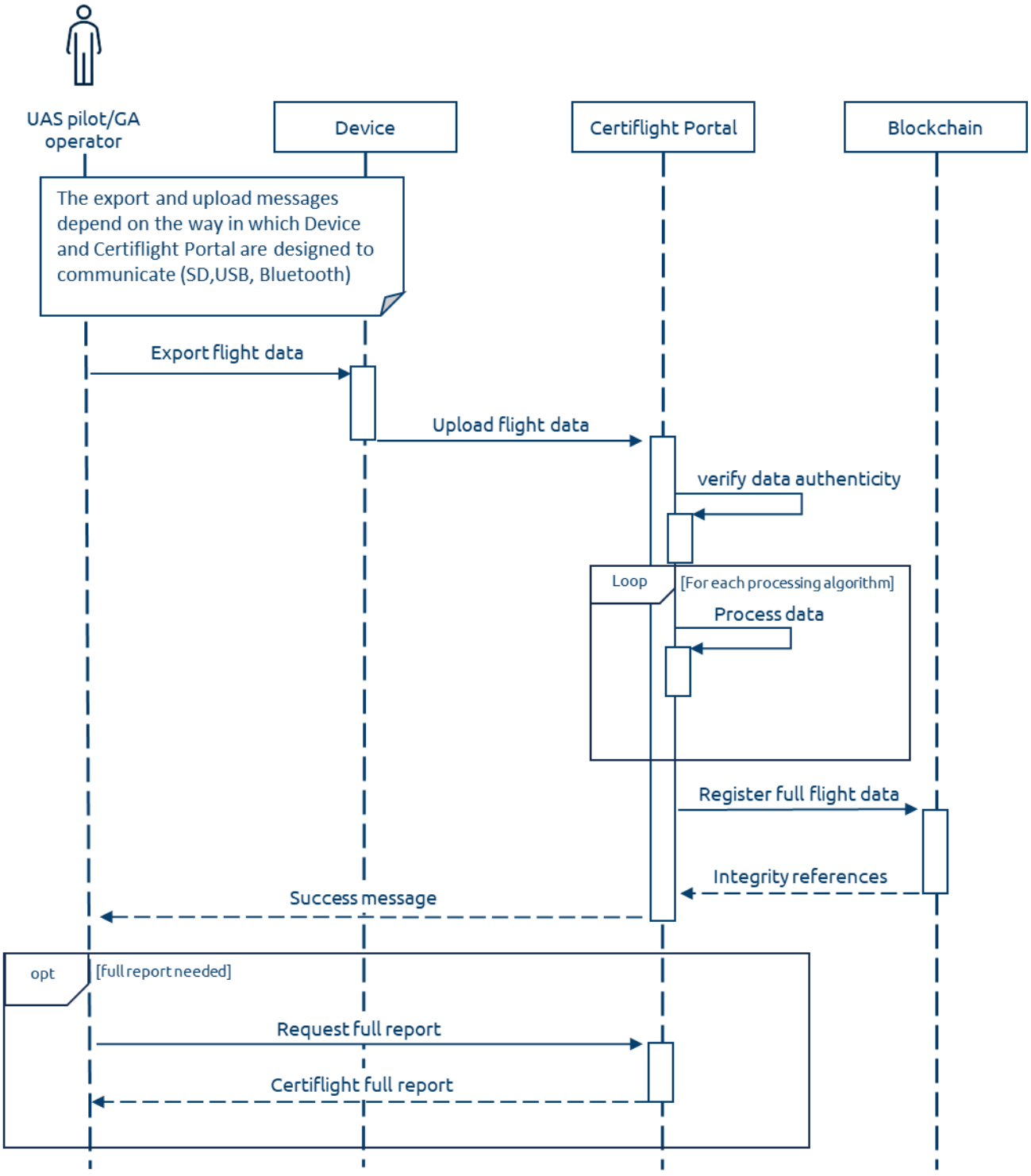


Figure 4-6 Post-flight workflow - Generation of full report