D2.3-U-space regulation compliance and standards

DELIVERABLE DETAILS			
Deliverable Nr	**Lead Beneficiary**	**Dissemination Level**	**Status**
D2.3	EUSC-IT	PU	CONTROLLED
Edition	**Revision**	**Issue**	**Document Code**
01	01	01.01	D2.3_01.01
File Name	D2.3- U-space regulation compliance and standards_01.01.docx		
Ref. Template	D0.0-Certiflight Document Template_01.00.dotx		

DOCUMENT HISTORY					
Issue	**Date**	**Status**	**Author**	**Partner**	**Change Description**
00.01	03/04/2023	DRAFT	P.J. Capasso J. Marangoni	EUSC-IT	First Draft
00.02	20/04/2023	DRAFT	P.J. Capasso J. Marangoni	EUSC-IT	Second Draft
00.03	28/04/2023	DRAFT	D. Leanza	DTA	Contribution to section 5 and 6
00.04	10/05/2023	DRAFT	CERTIFLIGHT Team	CERTIFLIGHT Team	Integration of Use cases, Regulatory aspects
00.05	15/05/2023	DRAFT	P.J. Capasso J. Marangoni	EUSC-IT	Third Draft
00.06	19/05/2023	DRAFT	F. Russo	TOP	Fourth Draft
00.07	31/05/2023	DRAFT	P.J. Capasso J. Marangoni	EUSC-IT	Fifth Draft
00.08	09/06/2023	DRAFT	F. Russo R. Restaino	TOP	Revision of sections 4, 5, 7
00.09	09/06/2023	DRAFT	P.J. Capasso	EUSC-IT	Sixth Draft
01.00	16/06/2023	CONTROLLED	CERTIFLIGHT Team	CERTIFLIGHT Team	General revision and integration of the document
01.01	12/07/2023	CONTROLLED	A.Mennella V.M. Ascione	CERTIFLIGHT Team	Modification and integration according to DRS

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 (Unmanned Aircraft System) 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	This Regulation amends 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	This Regulation amends Regulation (EU) 923/2012 as regards 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 Implementing Regulation (EU) 2019/947	This Regulation lays down detailed provisions for the operation of UAS as well as for personnel, including remote pilots and organisations involved in those operations.
RD 6	CERTIFLIGHT – D2.1 Users needs and Use cases identification	This deliverable identifies the high-level users' needs through the description of a series of use cases where CERTIFLIGHT solution may provide significant added value to stakeholders.
RD 7	Warsaw Declaration – "Drones as a leverage for jobs and new business opportunities"	This document urges for further development of the significant potential of drone services to support EU (European Union) competitiveness and global leadership and calls for swift development of a drone ecosystem, that is simple to use, affordable, commercially and operationally friendly, yet capable of addressing all societal concerns such as safety, security, privacy and environmental protection.

		https://www.easa.europa.eu/en/newsroom-and-events/news/high-level-conference-drones-leverage-jobs-and-new-business-opportunities
RD 8	SESAR – U-space Blueprint	This document sets out the vision for the U-space, which aims to enable complex drone operations with a high degree of automation to happen in all types of operational environments, particularly in an urban context. https://www.sesarju.eu/u-space-blueprint
RD 9	CORUS – D6.3 U-space Concept of Operations	This document describes from users' perspective how operations should occur in Very Low Level (VLL) airspace, supported by U-space.
RD 10	Commission Implementing Regulation (EU) 2023/203	This Regulation amends Regulation (EU) 2021/664 as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations.
RD 11	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.
RD 12	EUROCONTROL – U-SPACE Services Implementation Monitoring Report	This report assesses the progress made in implementing the U-Space services enabling VLL drone operations in the Single European Sky (SES) Member States Area. https://www.eurocontrol.int/publication/u-space-services-implementation-monitoring-report
RD 13	CORUS-XUAM – D4.1 U-space ConOps	This document represents the new edition of the U-space Concept of Operations extending edition 3 of the ConOps delivered in October 2019 by the CORUS project [RD 9].
RD 14	ISO 23629-12:2022	This standard contains requirements for UTM (UAS Traffic Management) service providers. This document includes compliance monitoring, safety, security, privacy and other organisational requirements for providers in the context of UTM services.
RD 15	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 16	ASTM F3411-22a - Standard Specification for Remote ID and Tracking	This standard covers the performance requirements for remote identification (Remote ID) of Unmanned Aircraft Systems (UAS).
RD 17	Commission Implementing Regulation (EU) 2020/639	This Regulation amends Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight.

RD 18	ENAC – Regolamento UAS-IT	This Regulation aims to: i) complete the legal framework of Regulation (EU) 2019/947 for the parts for which such Regulation refers to national provisions; ii) define the requirements applicable to private or State UAS conducting activities that fall in the provisions of paragraph 3a) of Article 2 of Regulation (EU) 2018/1139 but for which the competent State Administrations have not issued special regulations pursuant to Article 748 of the Navigation Code.
RD 19	ENAC – Circolare ATM-09A	This Circular defines the criteria for the implementation of geographical zones in Italy, in accordance with the provisions of Article 15 to Regulation (EU) 2019/947, as well as the airspace reserve procedures, for UAS operations requiring reserved airspaces and UAS operations in airports.
RD 20	CZECH REPUBLIC CAA – General Measure LKR10–UAS	This Public Decree establishes the restricted area LKR10–UAS for the purpose of applying additional conditions to all types of Unmanned Aircraft (UA) operations falling within the scope of Commission Implementing Regulation (EU) 2019/947.
RD 21	BELGIUM CAA – Royal Decree RPAS	This Decree regulates the use of Remotely Piloted Aircraft Systems (RPAS) in the Belgian airspace.
RD 22	ISO/IEC 27001	This standard contains the requirements for setting up and operating an information security management system.
RD 23	ETSI EN 303 645	This standard intends to prepare consumer Internet of Things (IoT) devices to be protected against the most common cybersecurity threats.
RD 24	European Commission (EC) - Cyber Resilience Act	This Act is a proposal for a regulation on cybersecurity requirements for products with digital elements that bolsters cybersecurity rules to ensure more secure hardware and software products.

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.

SUMMARY

ABSTRACT 8

1 SCOPE OF THE DOCUMENT 9

1.1 ACRONYMS 9

2 U-SPACE CONCEPT AND REGULATORY FRAMEWORK 15

3 U-SPACE SERVICES IMPLEMENTATION 18

4 IMPLEMENTATION OF CERTIFLIGHT SERVICE (SW) 29

4.1 NETWORK REMOTE ID AND DATA EXCHANGE AMONG USSPS 29
4.2 BLOCKCHAIN IMPLEMENTATION 30
4.3 INFORMATION SECURITY MANAGEMENT 31

5 GUIDELINES AND RECOMMENDATIONS FOR THE DESIGN AND DEVELOPMENT OF EGNSS/IOT UTM BOX (HW) 33

5.1 OSNMA IMPLEMENTATION 33
5.2 GUIDELINES TO AVOID DEVICE TAMPERING 34
5.3 INTERFACE WITH UAS AND PAYLOADS 35
5.4 USERS AND OPERATORS' POINT OF VIEW 36

6 USE CASES' REGULATORY ASSESSMENT 38

7 MATCHING LEGAL ASPECTS WITH THE SERVICE DEVELOPMENT 43

LIST OF FIGURES

FIGURE 1-1 WORK BREAKDOWN STRUCTURE 9
FIGURE 2-1 WARSAW DECLARATION ON NEW BUSINESS OPPORTUNITIES WITH DRONES 15
FIGURE 2-2 U-SPACE TIMELINE 16
FIGURE 2-3 EU U-SPACE REGULATIONS 17
FIGURE 3-1 U-SPACE SERVICES FROM EU REG. 664/2021 18
FIGURE 3-2 NETWORK IDENTIFICATION SERVICE IMPLEMENTATION [RD 12] 19
FIGURE 3-3 GEO-AWARENESS SERVICE IMPLEMENTATION [RD 12] 20
FIGURE 3-4 TRAFFIC INFORMATION SERVICE IMPLEMENTATION [RD 12] 21
FIGURE 3-5 UAS FLIGHT AUTHORISATION SERVICE IMPLEMENTATION [RD 12] 22
FIGURE 3-6 CONFORMANCE MONITORING SERVICE IMPLEMENTATION [RD 12] 23
FIGURE 3-7 WEATHER INFORMATION SERVICE IMPLEMENTATION [RD 12] 24
FIGURE 3-8 SESAR U-SPACE LEVELS [RD 8] 26
FIGURE 3-9 SESAR U-SPACE SERVICES [RD 9] 26
FIGURE 3-10 ISO UTM SERVICES 27
FIGURE 4-1 CERTIFLIGHT DATA PROVISION TO USSPS 29
FIGURE 5-1 THE ROADMAP SHOWN IN THE OSNMA INFO NOTE 33
FIGURE 5-2 SESIP SCHEME 34
FIGURE 5-3 DJI PSDK APPLICATIONS 35
FIGURE 6-1 OPERATIONS IN SPECIFIC CATEGORY 41
FIGURE 7-1 PARTIES INVOLVED IN THE CERTIFLIGHT SERVICE (RED ARROW REPRESENTS AN AGREEMENT) 44
FIGURE 7-2 USE CASES GROUPED BY OFFERED FEATURES 45

LIST OF TABLES

TABLE 1-1 ACRONYMS LIST 14
TABLE 3-1 CERTIFLIGHT U-SPACE SERVICES 28
TABLE 5-1 UTM BOX REQUIREMENTS 37
TABLE 6-1 UAS OPERATIONS CATEGORIES' SPECIFICATIONS 40
TABLE 6-2 CERTIFLIGHT USE CASES' CATEGORIES OF OPERATIONS 42

Abstract

The present document represents the deliverable D2.3 “U-space regulation compliance and standards” of the CERTIFLIGHT project.
It has been produced under Work Package WP2 “Users’ needs for U-space and System Specification”.
The main objective of WP2 is to identify users’ needs and system requirements specification, through the description of a series of use cases.
The activity considers the actual U-space regulations and monitors the main standardization groups’ outcomes for full compliance and applicability of the service on the market.
This document provides an overview about the U-space regulation and standards related to the CERTIFLIGHT concept. Moreover, it describes the preliminary aspects related to the implementation of the service and the development of UTM (Unmanned Aircraft System Traffic Management) box.

1 Scope of the document

The CERTIFLIGHT project proposes the implementation of the U-space service for the legal certification of tracks generated by UASs flights, through the introduction of a new disruptive EGNSS/IoT (Internet of Things) digital system.

The objective of this document is to analyse the regulatory aspects related to CERTIFLIGHT service, with reference to the actual EU U-space regulations 2021/664 [RD 1], 2021/665 [RD 2], 2021/666 [RD 3], EU UAS regulations 2019/945 [RD 4], 2019/947 [RD 5] and UAS/U-space standards.

The document starts with a general overview of the U-space concept and its related services, then provides some guidelines and recommendations for the design of the EGNSS/IoT UTM BOX and the development of CERTIFLIGHT service, lastly indicates the UAS operations category for each use case defined in D2.1 Users needs and Use cases identification [RD 6], up to finish with an assessment in terms of legal validity of the added value offered by CERTIFLIGHT service.

This document represents one of the inputs for WP3 “CERTIFLIGHT solution design & realization” as showed in the study logic of Figure 1-1, hereafter reported.

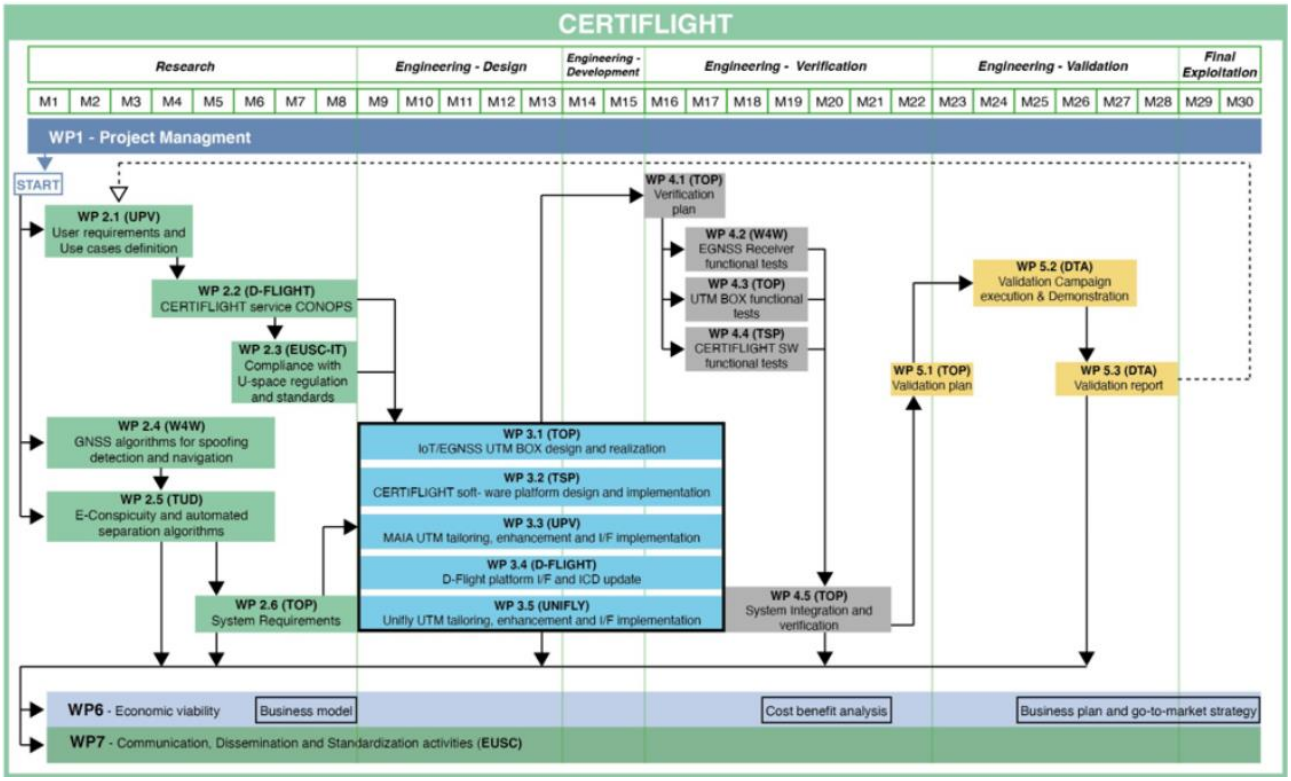

Figure 1-1 Work Breakdown Structure

1.1 Acronyms

Acronyms	Description
ADS-B	Automatic Dependent Surveillance - Broadcast

AGL	Above Ground Level Automatic Dependent Surveillance - Broadcast
AI	Artificial Intelligence
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
API	Application Programming Interface
ASD-STAN	AeroSpace and Defence Industries Association of Europe - Standardisation
ASTM	American Society for Testing and Materials
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
BVLOS	Beyond Visual Line Of Sight
CAA	Civil Aviation Authority
CE	Conformité Européene
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIS	Common Information Service
ConOps	Concept of Operations
D	Deliverable
DAA	Detect And Avoid
DL	Deliverable Leader
DLT	Distributed Ledger Technology

DSS	Discovery and Synchronization Service
EASA	European Union Aviation Safety Agency
EC	European Commission
EGNOS	European Geostationary Navigation Overlay Service
EGNSS	European Global Navigation Satellite System
EM	ElectroMagnetic
EN	European Norm
ENAC	Ente Nazionale per l'Aviazione Civile (Italian CAA)
ETSI	European Telecommunications Standards Institute
EU	European Union
EUOS	European Observatory for ICT Standardisation
EUROCAE	European Organisation for Civil Aviation Equipment
EUSPA	European Union Agency for the Space Programme
EVLOS	Extended Visual Line Of Sight
FLARM	FLight alARM
GA	General Aviation
GCS	Ground Control Station
GDPR	General Data Protection Regulation
GM	Guidance Material
GNSS	Global Navigation Satellite System
HW	Hardware
ICD	Interface Control Document

ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INATBA	International Association of Trusted Blockchain Applications
IoT	Internet of Things
ISG	Industry Specification Group
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunication Union – Telecommunication
JRC	Joint Research Centre
JTC	Joint Technical Committee
LUC	Light UAS operator Certificate
MS	Member State
MTOM	Maximum Take-Off Mass
NAA	National Aviation Authority
Net-RID	Network Remote Identification
OASIS	Organisation for the Advancement of Structured Information Standards
OS	Open Service
OSNMA	Open Service Navigation Message Authentication
PC	Project Coordinator
PDL	Permissioned Distributed Ledger

PDRA	Pre-Defined Risk Assessment
PII	Personally Identifiable Information
PMP	Project Management Plan
prEN	projected European Norm
PSA	Platform Security Assurance
PSDK	Payload SDK
RF	Radio Frequency
RMZ	Radio Mandatory Zone
ROS	Robot Operating System
RPAS	Remotely Piloted Aircraft System
RTOS	Real-Time Operating System
SBAS	Satellite Based Augmentation System
SC	Steering Committee
SDK	Software Development Kit
SES	Single European Sky
SESIP	Security Evaluation Standard for IoT Platforms
SIS	Signal-In-Space
SMA	SubMiniature version A
SME	Small to Medium Enterprise
SMS	Safety Management System
SORA	Specific Operations Risk Assessment
SSR	Secondary Surveillance Radar

STS	Standard Scenario
SW	Software
SWaP-C	Size, Weight, Power and Cost
TC	Technical Committee
TMZ	Transponder Mandatory Zone
TOE	Target Of Evaluation
UA	Unmanned Aircraft
UAM	Urban Air Mobility
UAS	Unmanned Aircraft System
USS	UAS Service Supplier
USSP	U-Space Service Provider
UTM	UAS Traffic Management
VHF	Very High Frequency
VLL	Very-Low Level
VLOS	Visual Line Of Sight
WG	Working Group
WP	Work Package

Table 1-1 Acronyms list

2 U-space concept and regulatory framework

The High-Level Conference on 'Drones as a leverage for jobs and new business opportunities' took place in Poland in 2016 and concluded with the so-called 'Warsaw Declaration' [RD 7] emphasising the significant potential of drone sector and requiring the development of a safe, secure and sustainable drone ecosystem.


MINISTRY OF INFRASTRUCTURE AND CONSTRUCTION

EASA

Civil Aviation Authority

HIGH LEVEL CONFERENCE ON DRONES

Drones as a leverage for jobs and new business opportunities

23-24 November, Warsaw, Poland

WARSAW DECLARATION

"Drones as a leverage for jobs and new business opportunities"

Warsaw - 24 November 2016

The Polish Minister of Infrastructure and Construction Mr Andrzej Adamczyk hosted the Warsaw High Level Conference also attended by the European Commissioner for Mobility and Transport Ms Violeta Bulc, the Executive Director of European Aviation Safety Agency Mr Patrick Ky, the acting President of the Polish Civil Aviation Authority Mr Piotr Samson, the Executive Director of the SESAR Joint Undertaking Mr Florian Guillermet, a number of Directors General of Civil Aviation from the EU Member States, representatives of ICAO, international associations, European bodies, Agencies, together with leaders of the industry. The conference called for a number of well-coordinated actions to develop the EU drone ecosystem and to deliver it by 2019, building on the guiding principles given in the Riga Declaration.

Partners

LOTNISKO CHOPINA WARSZAWA

Media patronage

TVP INFO

Rynek Infrastruktury

Figure 2-1 Warsaw Declaration on new business opportunities with drones

A flexible framework of safety regulation at EU (European Union) level based on the operation centric approach was expected. After Warsaw Declaration, the U-space vision has been introduced and developed by the European Union. The main target of the U-space design is to facilitate any kind of mission in any type of environment and in any class of airspace ensuring the safety throughout the operation. In this respect, SESAR JU (Joint Undertaking) drafted the U-space Blueprint in 2017 [RD 8], to start making U-space operationally possible. In this document, 4 sets of services have been identified to support UAS (Unmanned Aircraft System) operations and EU aviation strategy. The two-years CORUS project developed a Concept of Operations (Conops) for U-space [RD 9]. An initial architecture for the airspace with a detailed definition of the airspace types for UAS operations at very low-level and the services that ensures safe and efficient operations is provided in this Conops. It considers both the needs of the UAS industry and those of society as a whole. Several U-space projects in Europe are conducting first trials and demonstration campaigns. To support the SESAR JU's vision of delivering the Digital European Sky, some demonstrators are expected to be launched in 2023 and to run until 2026. The final target is the full integration of UAS operations in urban environment. To achieve this target, developments in technologies and regulations are crucial.

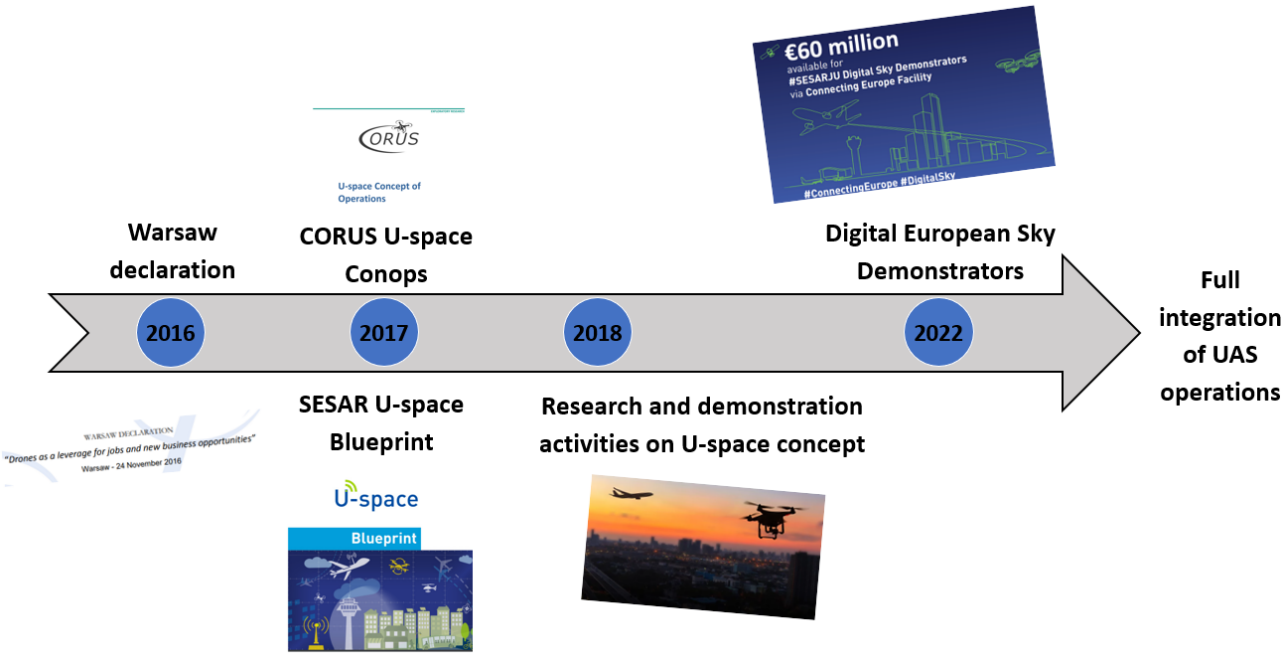

Figure 2-2 U-space timeline

U-space airspace and U-space services may support the UAM (Urban Air Mobility) concept. The European Commission [RD 1] has defined:

- U-space airspace: a UAS geographical zone designated by Member States, where UAS operations are only allowed to take place with the support of U-space services; and
- U-space service: a service relying on digital services and automation of functions designed to support safe, secure and efficient access to U-space airspace for a large number of UAS.

Operations in U-space airspace will be acceptably safe through airspace design, dynamic reconfiguration of the U-space airspace, electronic conspicuity of manned aircraft and U-space Service Providers certification.

The European U-space regulatory package [RD 1, RD 2, RD 3] has created the conditions necessary for both drones and manned aircraft to operate safely in the U-space airspace. The Commission Implementing Regulation (EU) 2021/ 664 provides the regulatory framework concerning U-space. This Regulation applies, within the U-space airspace, to operators of UAS, U-space service providers and providers of common information services. It identifies the mandatory and additional U-space services required in U-space airspace. The Commission Implementing Regulation (EU) 2021/ 665 establishes that within the designated U-space airspace in a controlled airspace, Air Navigation Service Providers (ANSPs) remain responsible for providing air navigation services to operators of manned aircraft. Specific communication procedures and structures should be established between appropriate Air Traffic Service (ATS) units, U-space service providers and single common information service providers. Lastly, the Commission Implementing Regulation (EU) 2021/ 666 provides the requirements for communication, SSR transponder and electronic conspicuity in U-space airspace. The aeronautical information publications shall contain the airspaces designated as RMZ, TMZ or U-space airspace. These Regulations apply from 26 January 2023. The Commission Implementing Regulation (EU) 2023/203 [RD 10] has amended Commission Implementing Regulation (EU) 2021/664

as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations. This Regulation sets out the requirements to be met by the organisations and competent authorities in order: (a) to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes; (b) to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety; (c) to respond to, and recover from, those information security incidents. Authority requirements and organisation requirements for the management of information security are provided respectively in Annex I and Annex II to Implementing Regulation (EU) 2023/203.

Figure 2-3 EU U-space Regulations[1]

The U-space regulations provide a high-level framework for the U-space to enable the initial UAS operations without specifying the required means to enable harmonised implementation of the U-space, therefore the Acceptable Means of Compliance (AMC) and Guidance Material (GM) are fundamental. EASA has published its first set of AMC and GM to the U-space regulatory framework in December 2022 [RD 11]. The latest developments by industry and U-space stakeholder have been considered in the development of the AMC/GM to the U-space regulatory framework, that represent the state of the art of the U-space concept, systems and technology.

The U-space is designed to:

- Mitigate the risk of collision with manned aircraft and between UAS and subsequent air and ground risks;
- Enable efficient and fair usage of the airspace;
- Enable safe dense and complex drone operations.

U-space is supported by a set of new services, provided in a digital and automated manner, inside some portions of airspace. In the next section the different U-space services identified by regulations and standards are listed.

[1] https://www.easa.europa.eu/en/regulations/U-space

3 U-space Services implementation

A different number of U-space services has been defined by European Commission and other bodies (e.g. standardisation bodies, European projects, etc.). As abovementioned, Regulation 664/2021 [RD 1] defined seven U-space services. It established four mandatory U-space services: network identification service, geo-awareness service, UAS flight authorisation service, traffic information service; two additional services that might be required by Member State (MS): conformance monitoring service and weather information service; and the common information services that MS shall ensure that are made available for every U-Space airspace. These services may be provided by one or several U-space service providers.

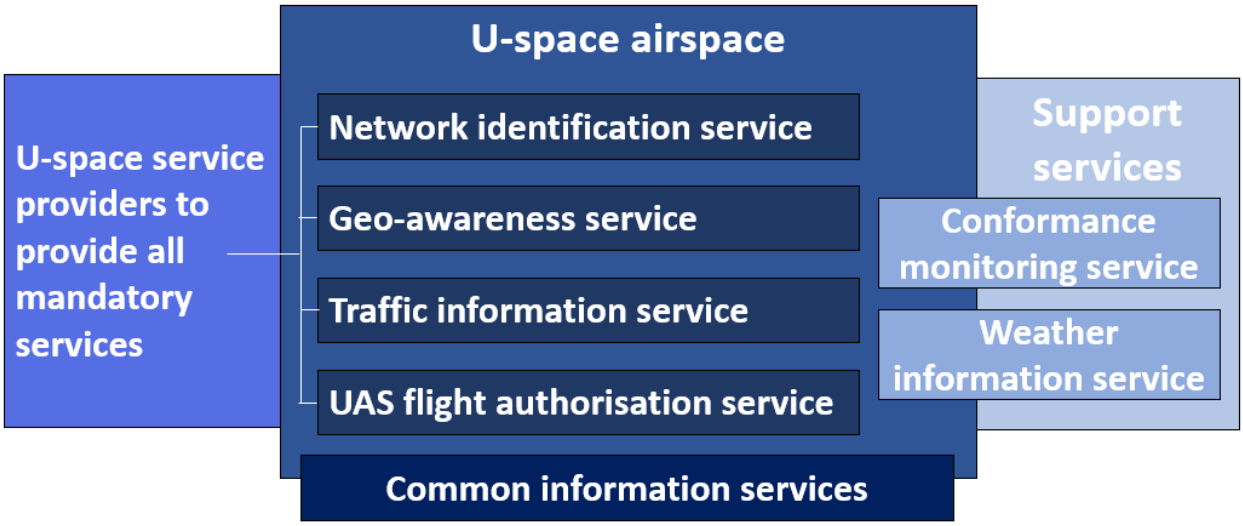

Figure 3-1 U-space services from EU Reg. 664/2021

The network identification service continually processes and provides to the authorised users the UAS remote identification during the entire flight. The geo-awareness service provides information about UAS geographical zones. The UAS flight authorisation service checks and accepts the UAS flight authorisation, then notifies the UAS operator about the acceptance or rejection. The traffic information service provides information about possible conspicuous air traffic in proximity of the UAS position or planned route. The weather information service collects weather information from trusted sources and provides this information to the UAS operator. The conformance monitoring service enables the UAS operator to check the compliance with the requirements stated in Article 6(1) of [RD 1] and the terms of the UAS flight authorisation. Lastly, the MS shall provide the data referred to in Article 5(1) of [RD 1] as part of the common information services of each U-space airspace.

At the end of 2022, EUROCONTROL conducted an implementation analysis of the U-Space services [RD 12]. For the services identified in the Regulation (EU) 664/2021, it provided the results provided below.

Network Identification service: the implementation of this service has been identified to be 'Completed - Ready for implementation' in 4 Member States and has been reported 'Ongoing' in 3 States. Considering the reported plans of implementation, the service is expected to continue at an increased pace.

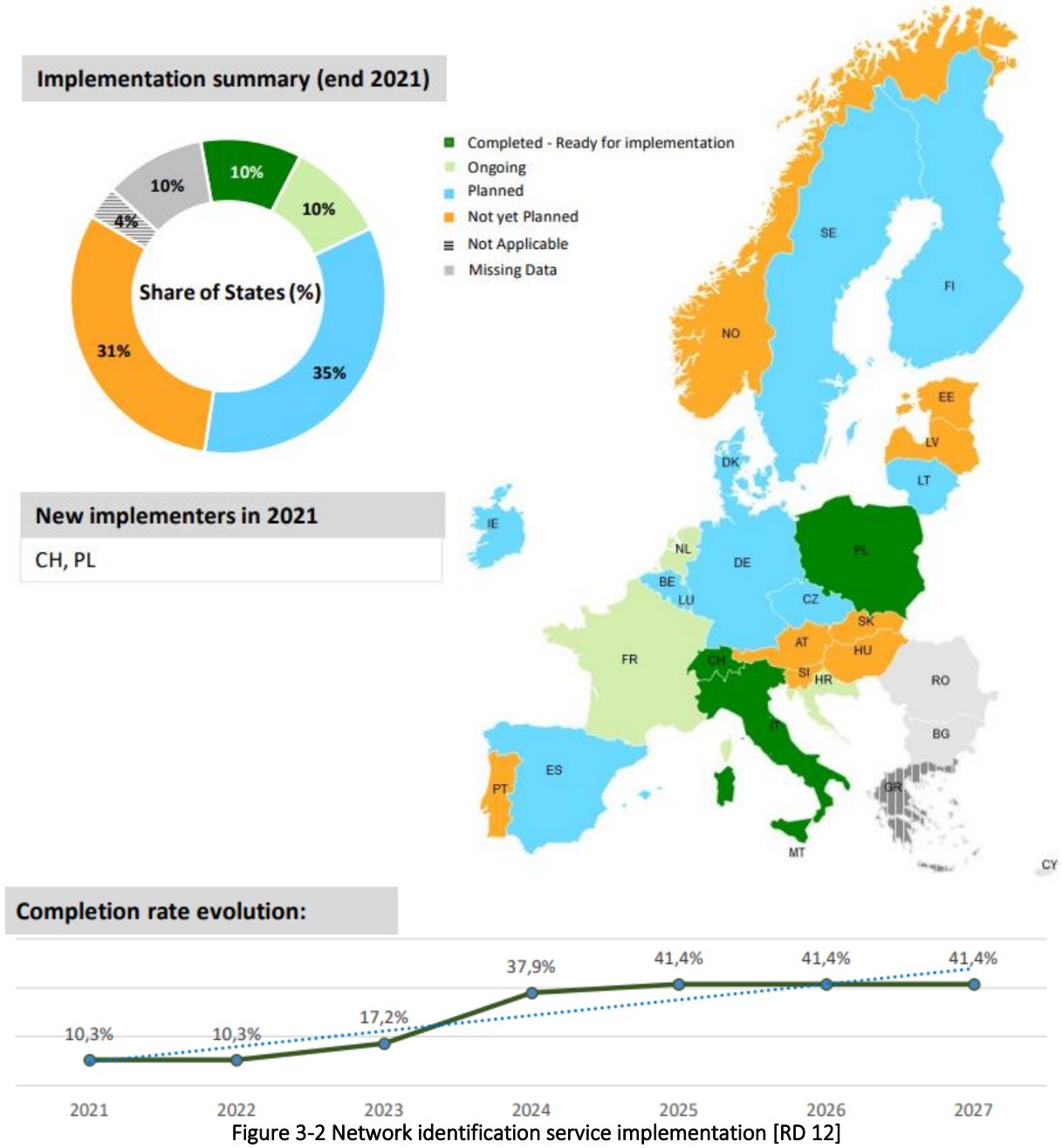

Figure 3-2 Network identification service implementation [RD 12]

Geo-awareness service: the implementation of this service is 'Completed - Ready for implementation' in 6 Member States. Moreover, 9 Member States are currently in the process of implementing the service declaring it 'Ongoing', and 5 of them have reported it 'Planned'.

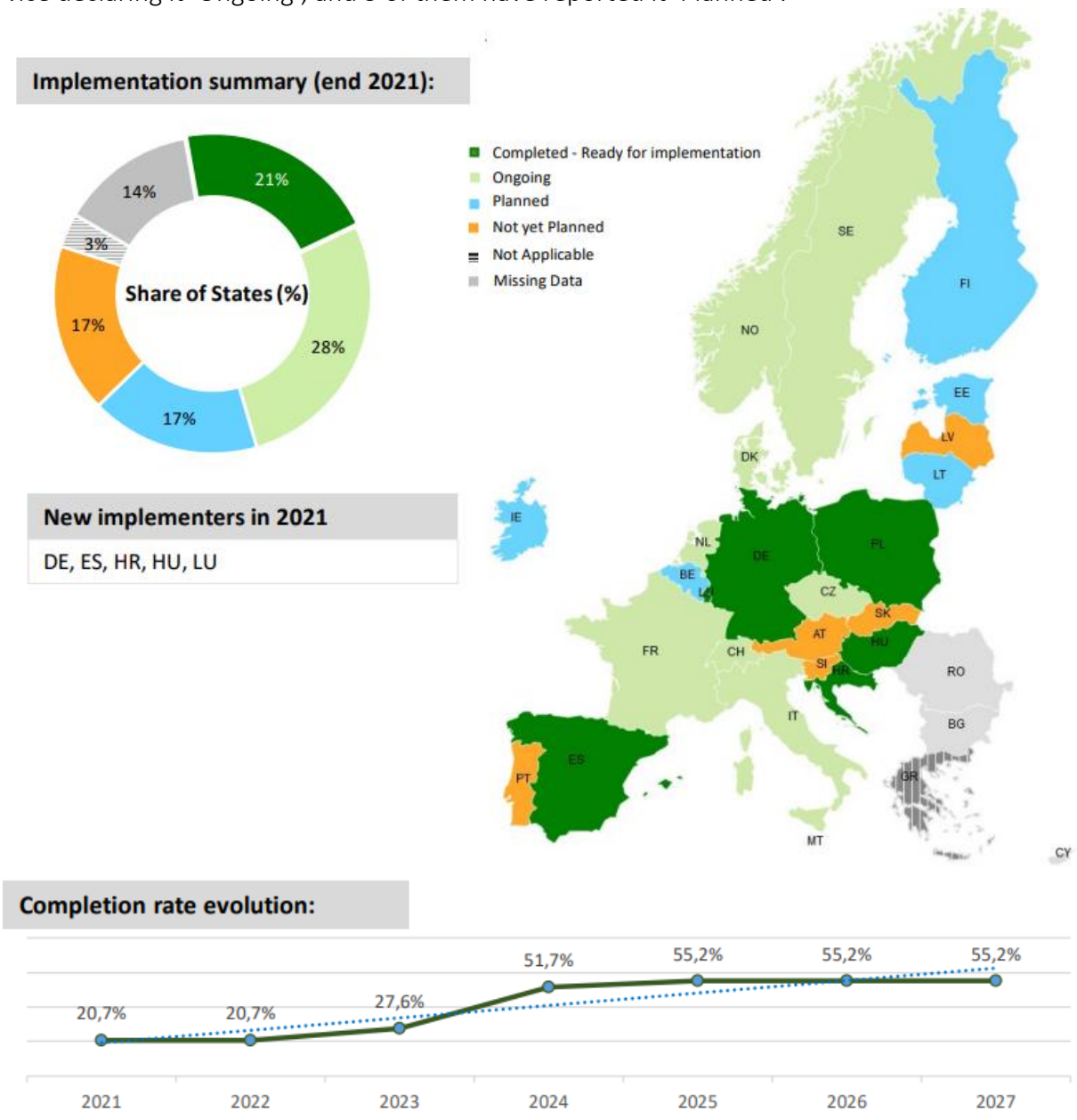

Figure 3-3 Geo-awareness service implementation [RD 12]

Traffic Information service: this service is 'Completed - Ready for implementation' in 3 Member States and under an 'Ongoing' operational progress only in France. While 7 Member States foresee an upcoming integration of the USSP and CIS service, 15 other Member States haven't provided any implementation dates, decision pending on the adoption of the U-Space regulation.

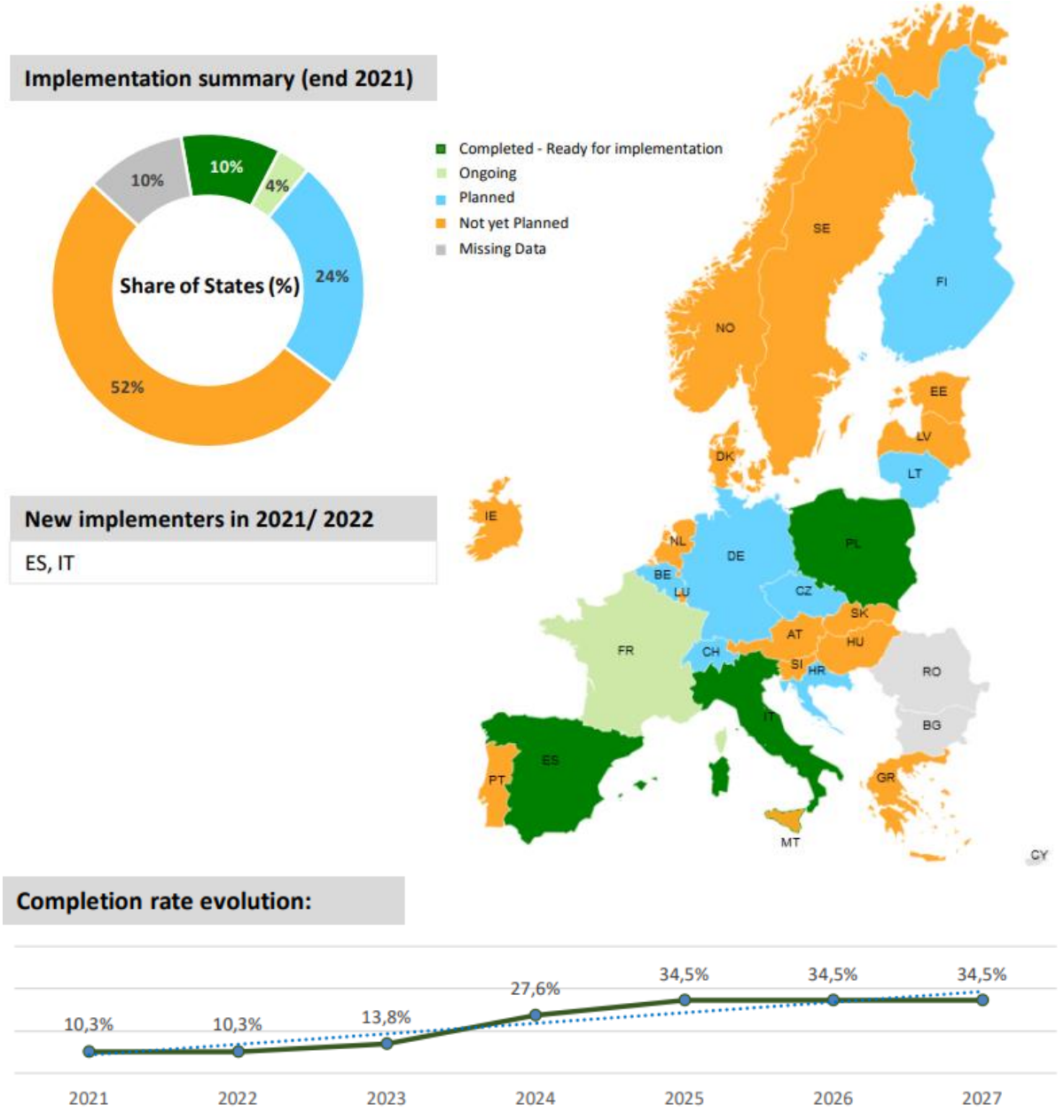

Figure 3-4 Traffic information service implementation [RD 12]

UAS flight authorisation service: this service is 'Completed - Ready for implementation' in 6 Member States and under an 'Ongoing' operational progress in France, Ireland and Italy. A progressive planning of this service is expected to be applied in several Member States, whereas 11 Member States have no planning view yet integrated.

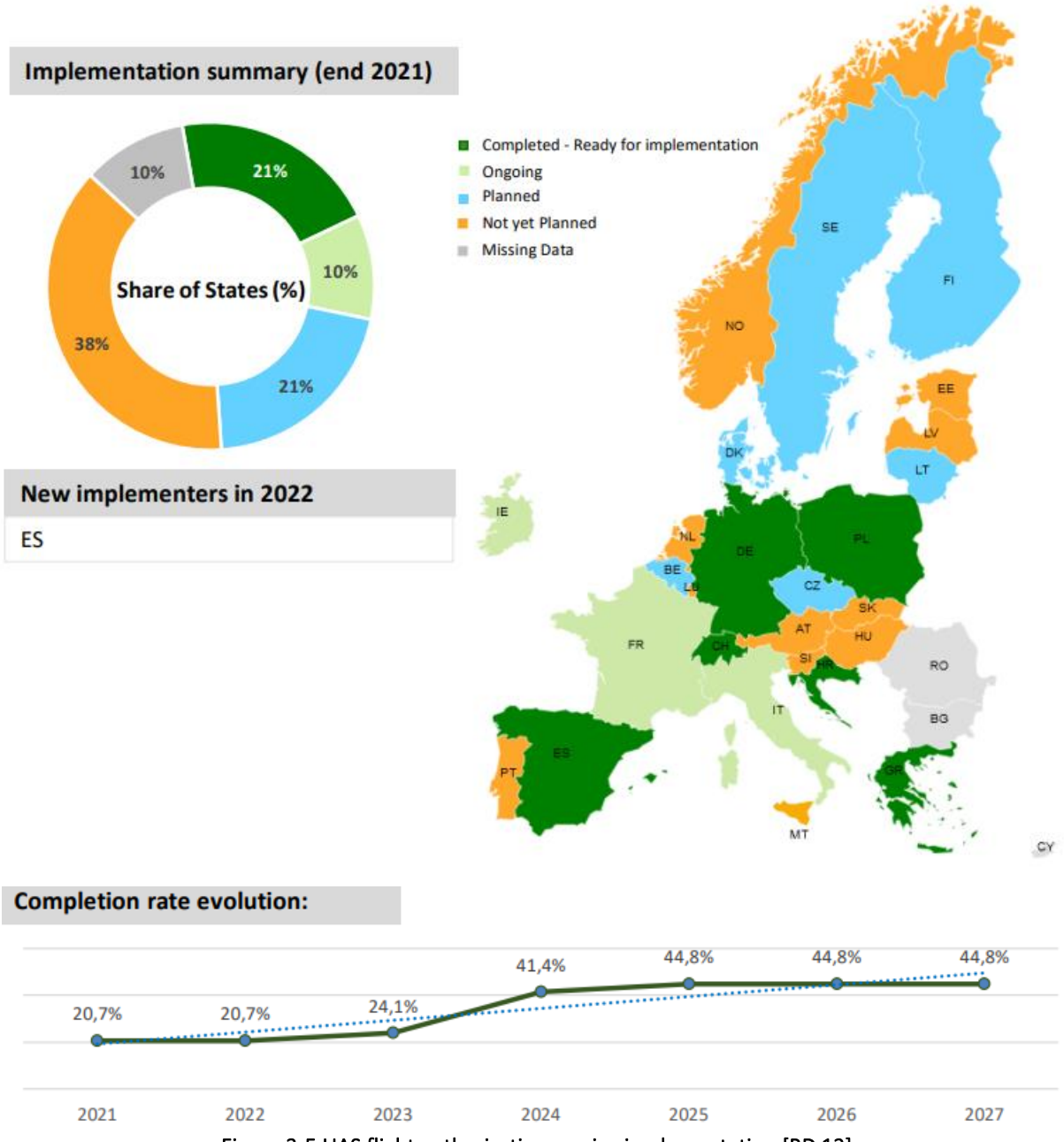

Figure 3-5 UAS flight authorisation service implementation [RD 12]

Conformance Monitoring service: the implementation of this service is 'Completed - Ready for implementation' only in Poland, 'Ongoing' in 4 Member States and declared 'Planned' in 7 Member States. Due to the still high number of States reporting 'Not yet Planned', it is not yet possible to predict an achievement date.

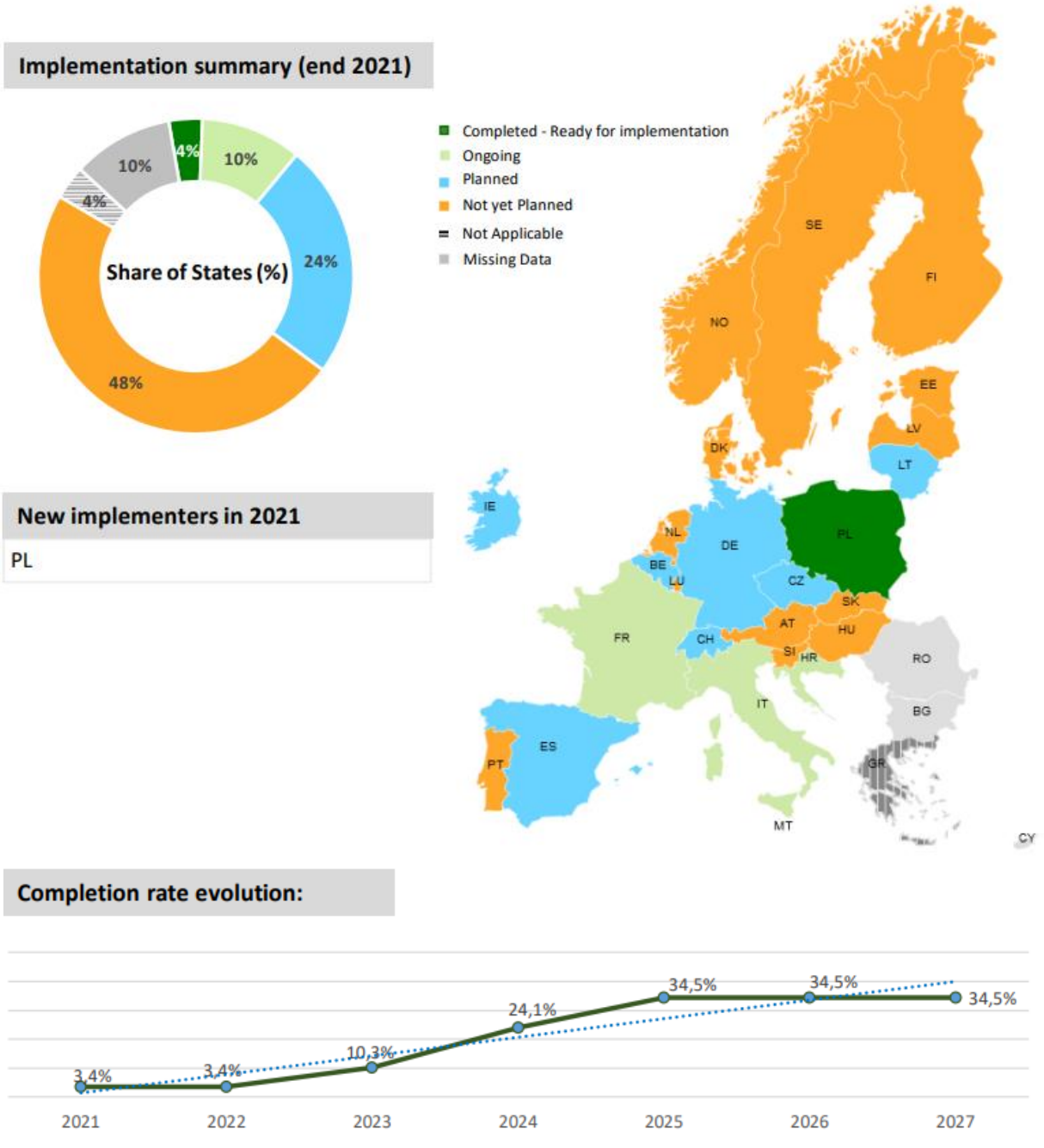

Figure 3-6 Conformance monitoring service implementation [RD 12]

Weather information service: the implementation of this service is 'Completed - Ready for implementation' in 8 Members States; while the service is 'Ongoing' in 3 Member States, and 4 Member States have claimed it 'Planned'. On the other hand, 11 member States have no plans of implementation yet.

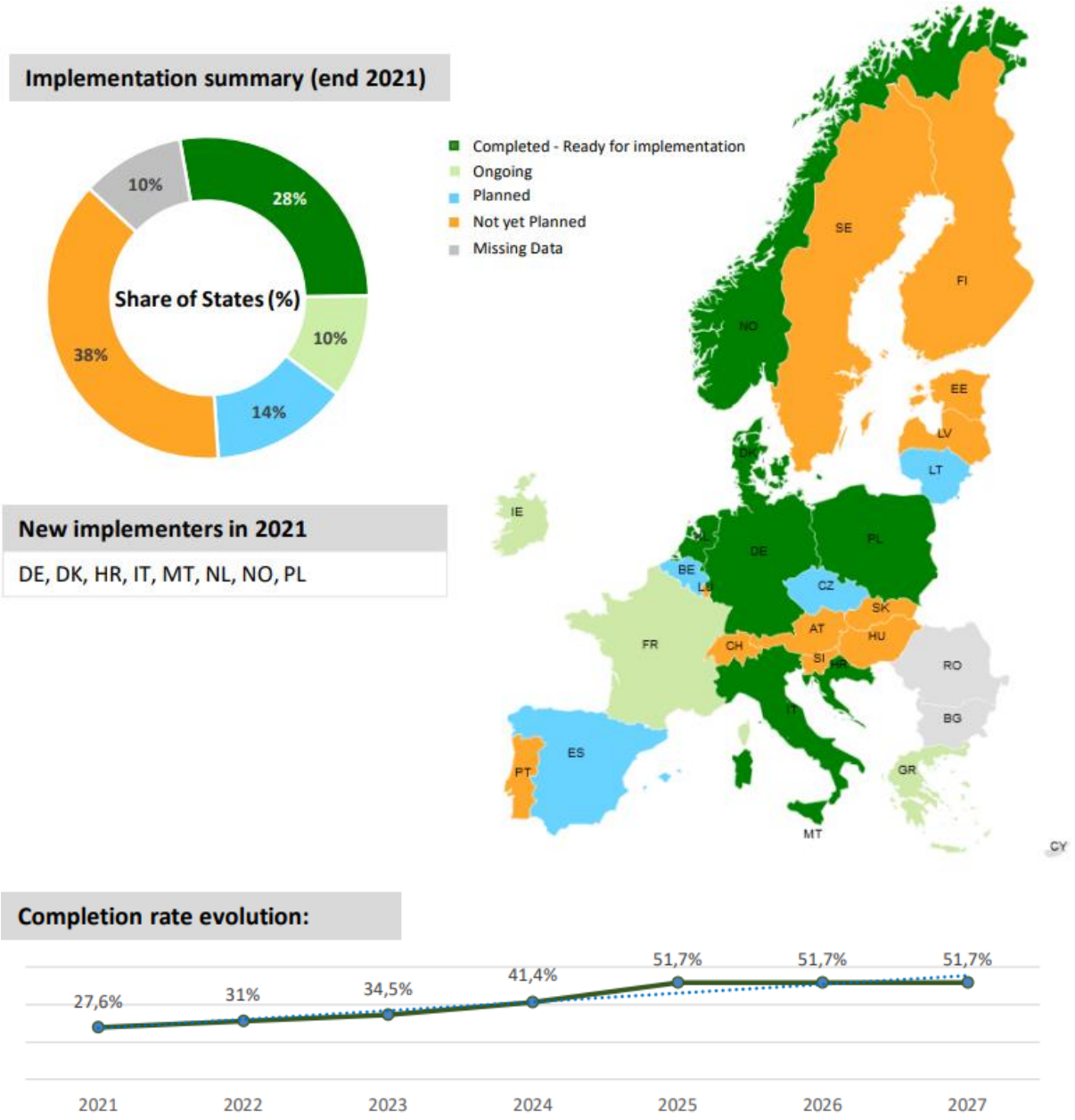

Figure 3-7 Weather information service implementation [RD 12]

The U-space services implementation survey conducted by EUROCONTROL [RD 12] provides the maturity of preparation for implementing not only the mandatory services defined by Reg. (EU) 664/2021 but also all the U-Space services defined in the SESAR U-Space Blueprint. In fact, more services have been identified in CORUS Conops for U-space linked to the four sets of U-space services defined in SESAR U-space Blueprint: U-space foundation services, U-space initial services, U-space advanced services, U-space full services. Increasing the level of drone automation and connectivity, it is possible to move from U-space foundation services to U-space full services. The progressive deployment of U-space is linked to available services and enabling technologies.

CORUS D6.3 U-space Concept of Operations [RD 9] provides an initial architecture for the U-space airspace with a detailed definition of the services provided to ensure safe and efficient operations. The ConOps considers both the needs of the UAS industry and those of the society as a whole. A new edition of the U-space Concept of Operations has been published by the CORUS-XUAM project [RD 13] and it differs for three reasons: i) this edition attempts to meet the needs of Urban Air Mobility, including both goods and passenger air transport in urban areas; ii) the European Union has passed various regulations relating to U-space which have to be taken into account; iii) research projects have completed details missing in the previous editions which are incorporated.

U-space is defined by SESAR as a set of new services and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. These services rely on a high level of digitalisation and automation of functions, whether they are on board the drone itself, or are part of the ground-based environment. U-space provides an enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, ATM/ANSP and authorities. U-space is therefore not to be considered as a defined volume of airspace, which is segregated and designated for the sole use of drones. U-space is capable of ensuring the smooth operation of drones in all operating environments, and in all types of airspace (in particular but not limited to VLL airspace). It addresses the needs to support all types of missions and may concern all drone users and categories of drones U-space.

The progressive deployment of U-space is linked to the increasing availability of blocks of services and enabling technologies. Over time, U-space services will evolve as the level of automation of the drone increases, and advanced forms of interaction with the environment are enabled (including manned and unmanned aircraft) mainly through digital information and data exchange. As abovementioned, SESAR has defined 4 set of services [RD 8]:

- U1 foundation services: the main objectives of which are to identify drones and operators and to inform operators about known restricted areas. With the deployment of U1, more drone operations are enabled, especially in areas where the density of manned traffic is low. The U-space foundation services include e-registration, e-identification and geo awareness.
- U2 initial services: the main objective is to support the safe management of beyond the visual line of sight (BVLOS) operations and a first level of interface and connection with ATM/ATC and manned aviation. With the deployment of U2, the range of operations at low levels will increase, including some operations in controlled airspace. Drone flights will no longer be considered on a case-by-case basis, and some BVLOS operations will become routine. The U-space initial services will include at minimum the following: tactical geo-fencing, emergency management, strategic deconfliction, weather information services, tracking, flight planning management, monitoring, traffic information, drone aeronautical information management and procedural interface with ATC.

- **U3 advanced services:** the main objective is to support more complex operations in dense areas and may include capacity management and assistance for conflict detection. Indeed, the availability of automated 'detect and avoid' (DAA) functionalities, in addition to more reliable means of communication, will lead to a significant increase of operations in all environments and will reinforce interfaces with ATM/ATC and manned aviation.
- **U4 full services:** it focuses on services offering integrated interfaces with ATM/ATC and manned aviation and supports the full operational capability of U-space based on a very high level of automation.

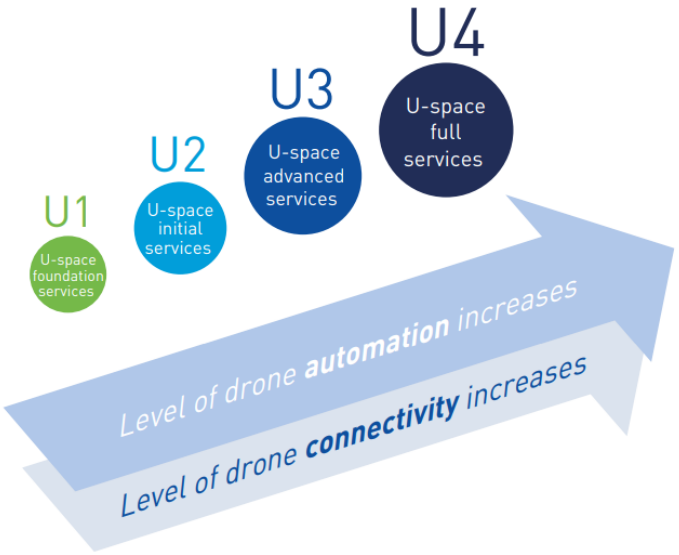

Figure 3-8 SESAR U-space levels [RD 8]

The Figure 3-9 shows the list of all U-space services related to the safety and/or security introduced by CORUS [RD 9].

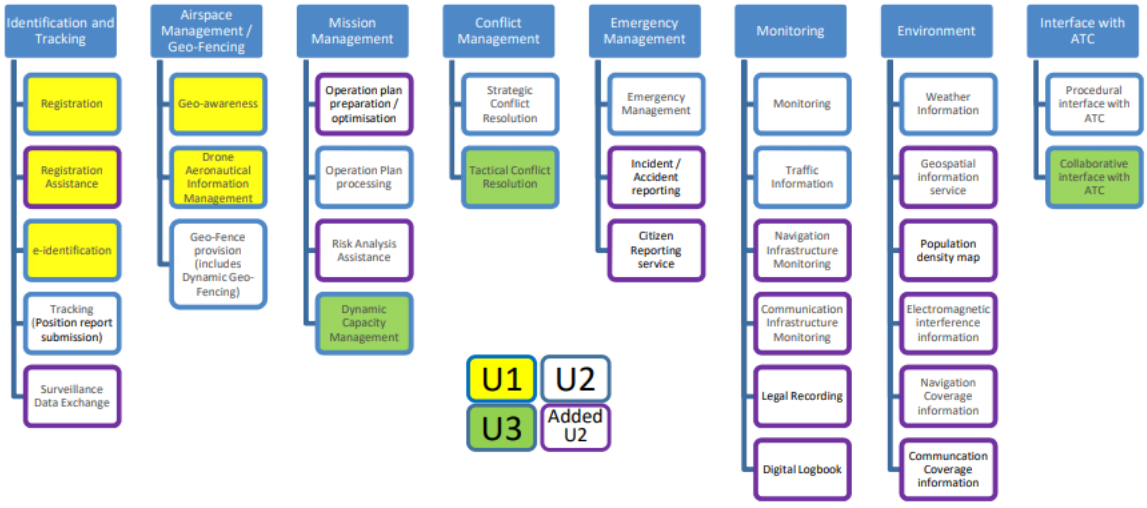

Figure 3-9 SESAR U-space services [RD 9]

CORUS-XUAM D4.1 U-space ConOps [RD 13] has introduced some services (e.g. vertical conversion service, vertical alert and information service). It represents the new edition of the U-space Concept

of Operations extending the edition 3 of the ConOps delivered in October 2019 by CORUS project [RD 9].

Lastly, ISO classified 30 U-space services into Safety-critical UTM services, Safety-related UTM Services and Operation support services in ISO 23629-12 [RD 14].

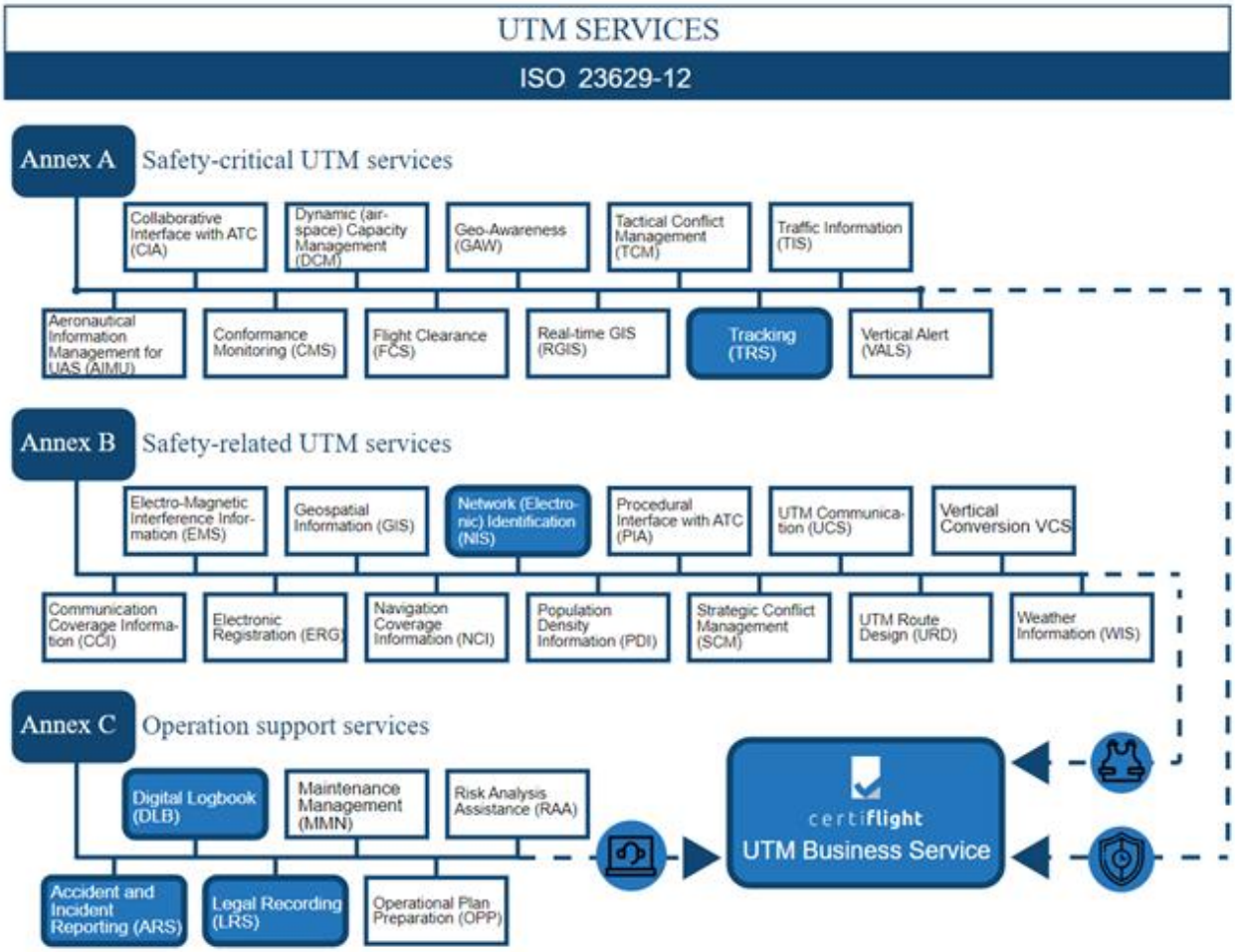

Figure 3-10 ISO UTM services

Key enabling EGNSS/U-spaces services are needed to support safe and efficient navigation of UAS especially in BVLOS conditions, where most of the business of UAS operations is expected. The UTM services showed in Figure 3-10 are those present in the list of the three ISO 23629-12 standard annexes where CERTIFLIGHT proposes to contribute implementing a new class of business service (blue blocks in the figure above).

The enhanced service would provide digital information also to some other U-space services already identified, but not yet implemented by UTM technology providers or U-space Service Providers (USSPs), so contributing to fill existing gaps. CERTIFLIGHT service exploiting GNSS data and additional information generated by other U-space services (i.e., geo-awareness) paves the way for another generation of U-space services more oriented to the business side instead than to safety as the services regulated through Commission Implementing Regulation 2021/664. Possible new business oriented and not safety-critical services developed by CERTIFLIGHT include Smart Contract activation, real time UAS flight data for fleet management purposes (e.g., on behalf of the Fleet Manager of

logistic companies), Certified flight Report generation (e.g. for law enforcement agencies) and in general authenticated UAS tracking data when traceability would need to be legally demonstrated, for purposes beyond the safe management of air traffic. The main UTM services related to the CERTIFLIGHT concept are:

UTM/U-Space Service	ISO 23629-12	SESAR U-level	U-space EU regulatory package
Tracking	Safety-critical	U2	Not mentioned but might be inferred in the description of the Traffic Information Service, Article 11 of EU 2021/664
Network Identification	Safety-related	U1	Article 8 of EU 2021/664
Legal Recording	Operation support	Added U2	Not mentioned but might be inferred by Article 15 of EU 2021/664
Digital Logbook	Operation support	Added U2	N.A.
Accident and Incident Reporting	Operation support	Added U2	Partially covered by Article 15(d) of EU 2021/664

Table 3-1 CERTIFLIGHT U-space services

Tracking service
This service provides tracking information as regards drone position using location reports and combining multiple sources.

Network identification service
This service allows the continuous processing of the remote identification of the UAS throughout the duration of the flight and provides the remote identification of the UAS to the authorised users in an aggregated manner.

Legal recording service
This restricted-access service supports accident and incident investigation by recording all input to U-space and giving the full state of the system at any moment.

Digital Logbook service
This service extracts legal recording information in order to produce reports for users.

Accident and Incident Reporting service
This secure and access-restricted service allows drone operators to report incidents and accidents, maintaining reports for their entire life-cycle.

4 Implementation of CERTIFLIGHT service (SW)

CERTIFLIGHT project proposes a new U-space service for the legal certification of tracks generated by UASs and aircrafts flights, through the introduction of a new disruptive EGNSS-IoT digital system. CERTIFLIGHT features a software platform that offers to its customers (UAS Operators, GA Pilots) a digital service for the generation of certified reports of flight tracks and the flight logs of UASs and GA aircrafts, especially for safety related and commercially valuable applications, paving the way for a new class of U-space business services that include the activation of Smart Contracts (i.e. contracts activated when specific conditions are met as flying specific routes for drone parcel delivery). In addition, the recorded tracks may be useful for enforcement (i.e., sanctions for airspace infringement) as well as for possible accident or incident investigations.

To implement the CERTIFLIGHT service and in particular to design the software architecture and user interfaces, the developers can comply with the standards and follow the guidelines described in following paragraphs. The outcomes of standardisation activities will be summarized in the deliverable D7.9 Standardization activities contribution report of CERTIFLIGHT project.

4.1 Network Remote ID and data exchange among USSPs

The CERTIFLIGHT solution aims to implement the e-conspicuity concept and the interoperability of the data among U-space Service providers (USSPs).
To achieve this objective CERTIFLIGHT has to provide dedicated API (Application Programming Interface) to stakeholders. This API can be developed relying on current standards and guidelines.

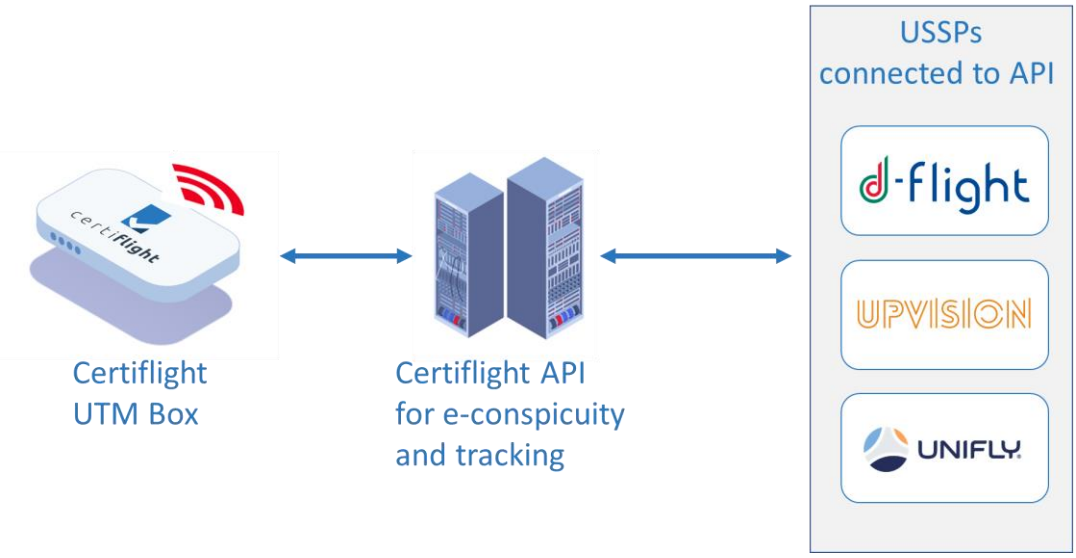

Figure 4-1 CERTIFLIGHT data provision to USSPs

According to the Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space:

- USSPs should provide the UAS network remote identification in the geographic proximity of UAS operations that are supported by the provision of their services.
- USSPs should exchange network remote identification data with all the service providers that share the same U-space airspace. The resulting aggregated data should cover all available network remote identification data in the U-space airspace concerned.

The AMC and GM to regulation 2021/664 suggests the ASTM 3411-22a [RD 16] for the implementation of the network remote ID service and data exchange among USSPs.
Considering the architecture proposed in the ASTM 3411-22a, the CERTIFLIGHT service can be classified among Network Remote ID service providers, which is defined by the standard as:

- Network Remote ID (Net-RID) service provider, n—a logical entity denoting a UTM system or comparable UAS flight management system that participates in Network Remote ID and provides data for and about UAS it manages.

Moreover, as regard the data exchange among USSP, the ASTM 3411-22a describes a standardized discovery mechanism, referred to as the Discovery and Synchronization Service (DSS), the primary functions of which is to identify USSs (UAS Service Suppliers) with which data exchange is required, and to verify that a USS considered relevant information from other USSs when necessary. The Discovery and Synchronization Service proposed in ASTM 3411-22a standard may be used as a reference to achieve this objective. In absence of EU standards on the implementation of EU regulation 945-947/2019 and 664/2021, the ASTM 3411-22a will be taken as reference. However, it is expected at EU level, the publication of a standard from EUROCAE, which is moving on this topic within the WG105-SG3: Network Remote ID, that probably will absorb many of the recommendations of the ASTM standard. This working group will be strictly monitored by the Consortium during the design and implementation phase of the CERTIFLIGHT UTM box: EUSC-IT and TOP are active members of WG105-SG3 and are following and contributing to its activities

4.2 Blockchain implementation

Currently there's still a lot of fragmentation in the blockchain ecosystem: standards are not available, and each technology has its own API. However even if there are no standards on this technology, it is likely that the EU will have an active role in the blockchain standards community, engaging and working closely with all relevant bodies around the world.

The technology standards landscape is complex, covering a large number of supra-national, national and industrial organisations. Some of the more important organisations in the European and global blockchain standards landscape include:

- StandICT: Provides a European ICT Standardisation Observatory (EUOS) and a Facility to support participation of European experts on international standardisation (StandICT.eu).
- European Standardisation Organisations: Important European standards organisations relevant to blockchain include the European Telecommunications Standards Institute (ETSI, in particular the ISG PDL), the European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardization (CENELEC), in particular through their Joint Technical Committee 19 (JTC-19).
- Supra-national and industry organisations: Important global organisations relevant to blockchain standards include ISO (in particular ISO TC-307), ISO/IEC JTC-1 and ITU-T.
- National standards bodies: Most national IT standards bodies also are or are expected to be working on blockchain topics.
- Open Standards bodies: Include IEEE, the Organisation for the Advancement of Structured Information Standards (OASIS) and the Internet Engineering Task Force (IETF).

- INATBA: Through various of its working groups, the International Association of Trusted Blockchain Applications also contributes to the standards discussion on a European and global level.

The Consortium will monitor the organizations listed above during the design and implementation phase of the CERTIFLIGHT platform: EUSC-IT with the support of TSP, project partner expert in blockchain technology, will inform TOP whenever a standard is published or amended.

There are many other national and industrial organisations involved in blockchain-relevant standards work on topics such as digital assets, token specifications, blockchain governance, security token standards, and more. The wide range of bodies working on blockchain standards ensures that a great deal of skill and expertise around the world is dedicated to this work. But there is a danger of fragmentation in the standards landscape. Technology standards can cover a wide range of topics, some of which are not directly related to the technology itself. In the blockchain context, the following topics are particularly relevant:

- Interoperability: Ensuring the different blockchain and DLT protocols and platforms can exchange data and seamlessly communicate with each other;
- Governance: Best practice and standards in governing blockchain projects as well as blockchain consortia working on decentralised platforms;
- Identity: Promoting a common identity framework and/or interoperable identity among different blockchain protocols and platforms;
- Security: Ensuring a secure operation of the different nodes, networks and services;
- Smart contracts: Supporting best practice and standards to ensure smart contract technology is safe and secure.

4.3 Information security management

The CERTIFLIGHT solution has to guarantee the trustability of the information, so for its own nature the security of the data is a critical issue in the project. On these regards, the CERTIFLIGHT can follow the good data protection practices of the ISO/IEC 27001 [RD 22], which is an international standard to manage information security. ISO/IEC 27001 requires that management:

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts; and
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Also, on this topic, in June 2020 the European Telecommunications Standards Institute (ETSI) released the ETSI EN 303 645 standard [RD 23], which provides a set of baseline requirements for security in consumer Internet of things (IoT) devices. It contains technical controls and organizational policies for developers and manufacturers of Internet-connected consumer devices. The standard is intended to be complemented by other more specific standards. As many consumer IoT devices handle Personally Identifiable Information (PII), implementing the standard helps with complying to the General Data Protection Regulation (GDPR) in the EU.

The Cybersecurity provisions in this European standard are:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data

Moreover, it is important to highlight the recent proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act [RD 24], which intends to bolster cybersecurity rules to ensure more secure hardware and software products.

According to EU Commission assessments, currently these products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

In fact, while existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs.

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

The development of the Cyber Resilience Act will be carefully monitored by the consortium through Task T7.3 of CERTIFLIGHT project, given the huge impact it could have on the project.

5 Guidelines and recommendations for the design and development of EGNSS/IOT UTM BOX (HW)

The core of the system is a digital EGNSS/IoT device installed on UASs and GA manned aircraft, equipped with an OSNMA Galileo/EGNOS enabled receiver, capable to guarantee the authenticity of their position information at the origin, without the possibility to be counterfeited or spoofed. Tracking information is cyphered for transmission to CERTIFLIGHT platform in real time and permanently stored to a private Blockchain node, unalterable once stored. Galileo OSNMA service acts as unique global enabler for this service, ensuring the authenticity of positioning data at the origin.

Radiated tests for EM characterization are required by the UTM Box manufacturer for the obtainment of the CE trademark. Drones already on the market are supposed to have out-of-band emissions already within the regulatory EM mask. Therefore, considering the availability of the JRC facilities for emission testing on the UTM Box and for the test foreseen for the resilience of OSNMA GNSS receiver, an additional radiated test might be performed by CERTIFLIGHT project on the target drone while in transmission, for an additional EM characterization.

5.1 OSNMA implementation

For a correct implementation of the CERTIFLIGHT solution, the consortium must be aware of European Union Agency for the Space Programme (EUSPA) documentation on this service.

The Galileo Open Service Navigation Message Authentication (OSNMA) – Info note provides all the fundamental information such the service characterisation, the roadmap for implementation and references of relevant documents.

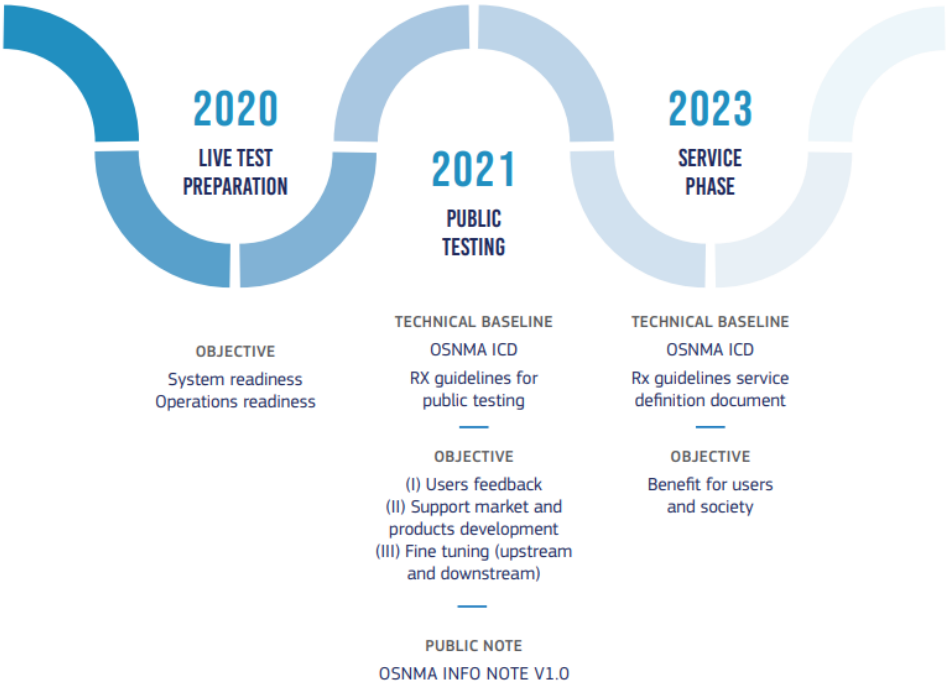

Figure 5-1 The roadmap shown in the OSNMA info note[2]

[2] GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) Info Note: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf

Moreover, EUSPA has recently published two documents:

- Galileo Open Service Navigation Message Authentication (OSNMA) Signal-in-Space (SIS) Interface Control Document (ICD).
  This document contains, together with the Galileo Open Service Signal-In-Space Interface Control Document (OS SIS ICD), all information on the OSNMA SIS and specifies the interface between the Galileo Space Segment and the Galileo User Segment.
- Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines. This document provides the guidelines for the user segment implementation of the OSNMA functionality and should be considered as a complement to the OSNMA SIS ICD. It specifies the user capabilities and steps to be implemented to verify the authenticity of the Galileo navigation message. These guidelines are drafted in a generic way and are not tailored for any specific platform or application.

5.2 Guidelines to avoid device tampering

The guidelines to avoid the tampering of the device are focused to firmware level protection. Since the design foresees to use ST microelectronics components, it's important to mention the solution proposed by the latter called STM32Trust. STM32Trust relies on several security certification schemes to increase the level of confidence in the security implementations, including:

- Platform Security Assurance (PSA) defined by Arm®
- Security Evaluation Standard for IoT Platforms (SESIP) defined by Global Platform

Arm® has introduced the concept of a IoT security framework in 2017 and it is a co-founder of PSA Certified – a framework and an independent third-party evaluation scheme to build-in the right level of device security. PSA Certified has scaled to become one of the fastest growing, most valued security ecosystems, globally, and continues to break down the barriers to security.
The Security Evaluation Standard for IoT Platforms (SESIP), published by GlobalPlatform, defines a standard for trustworthy assessment of the security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains. TrustCB has used this standard to develop and operate the "TrustCB SESIP scheme".
TrustCB operates a SESIP scheme to enable implementers of IoT platforms to demonstrate that a specific Target of Evaluation (TOE) provides specific functionality and services for use by an IoT application than can be installed on the platform and to protect platform assets against state-of-the-art attackers.

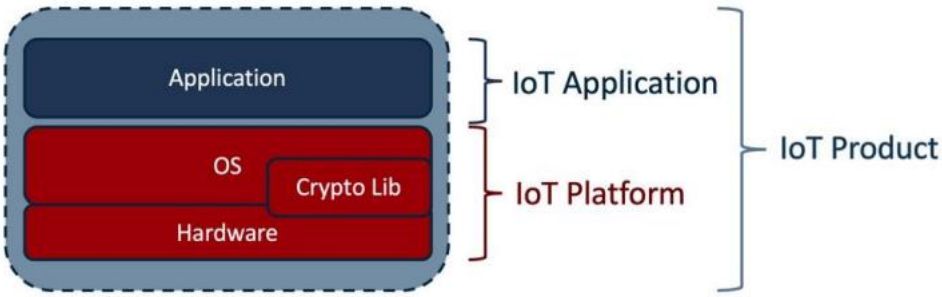

Figure 5-2 SESIP scheme[3]

[3] The primary source of information and the TrustCB scheme procedures and documents can be found at https://trustcb.com/iot/sesip/

An IoT-Platform, defined as Connected Platform in [SESIP], is the hardware/software providing an operating environment for an IoT Application. IoT Platforms parts can be developed and evaluated separately, for example by evaluating the cryptographic library, an OS, hardware, and then combining them. In terms of the Common Criteria, the IoT Platform (part) identified in the ST is the TOE.

An IoT Application, defined as Connected Application in [SESIP], is the software running on the IoT Platform adding domain-specific functionality. An IoT Platform together with an IoT Application in total form an IoT Product (Connected Product), providing the user with a complete functionality. From the platform point of view, there is only one IoT Application, even if this IoT Application is separated in many different applications parts from the IoT Application developer point of view.

5.3 Interface with UAS and Payloads

The Authenticity level 2 presented in D2.1 [RD 6] foresees a direct connection with drones. This paragraph describes two possible ways of integration: the first with DJI professional drones and the second using the MAVLink protocol.

The CERTIFLIGHT UTM box may sync the OSNMA data with DJI professional drones by using the development kit provided by DJI and named Payload SDK (PSDK). This development kit is used by design payload to be mounted on DJI drones by using the resources such as power supply, communication link and status information on DJI drones. DJI states that based on the functional interface provided by PSDK developers can easily combine specific structural design, hardware design, software logic implementation, and algorithm optimization.

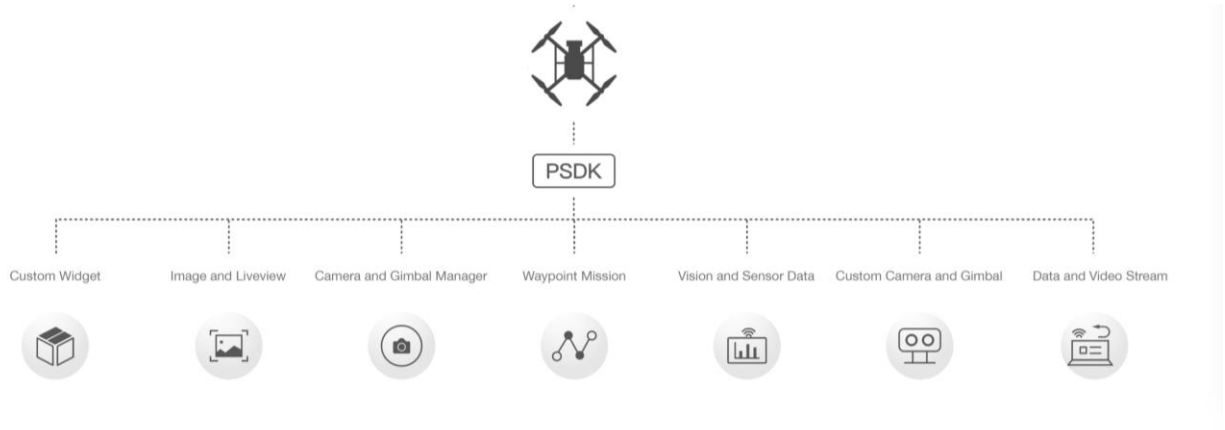

Figure 5-3 DJI PSDK applications[4]

The DJI Payload SDK is compatible with a wide range of software and hardware platforms Applications developed using PSDK can run on mainstream embedded hardware platforms, such as STM32, etc., and can also run on mainstream embedded operating systems and software architectures, such as Linux, ROS, and RTOS.

An alternative to DJI PSDK is MAVLink, which is a very lightweight messaging protocol for communicating with drones (and between onboard drone components). MAVLink follows a modern hybrid publish-subscribe and point-to-point design pattern: Data streams are sent / published a

[4] https://developer.dji.com/doc/payload-sdk-tutorial/en/basic-introduction/whats-psdk.html

topic while configuration sub-protocols such as the mission protocol or parameter protocol are point-to-point with retransmission.

5.4 Users and operators' point of view

Unmanned Aircraft Systems (UASs) are going to be increasingly adopted for example to inspect infrastructures, to enable precision farming in agriculture, to capture aerial video footages of critical areas for proactive response in the Public Safety sector. UASs, including related tracking technologies, play a primary role in the activities of both private and public organizations and thanks to recent technology developments, they have become more effective, more affordable and easier to fly. From point of view of users and operators, in order to facilitate the development of these technologies as per CERTIFLIGHT project, it is needed to support the development and the integration of suitable UTM Box to be installed mainly on low size UASs. The terminal shall be small in size and designed so as not to create significant aerodynamic drag or add excessive mass to the aircraft. Furthermore, large size drones for long endurance operations and GA aircrafts are powered by commercial engines such as turbo propeller or turbojet, while drones with size from micro to medium use battery as the power source with a limited flight autonomy depending on the weight of the drone and the payloads configurations. This is one of the main concerns of using drones for this kind of application where a not large size drone is required. High duration battery, reduced dimension and weight of the UTM Box should be taken into account and these aspects are not negligible for a low size drone. Improvements related to the size of box (miniaturization) could be needed so as not to exceed weight constraints that could affect power consumption and flying time of the UAS.

UTM box solutions, are needed to improve the usability and authenticity of positioning allowing the drone-based services to take place. Therefore, a fundamental pillar is the development of an UTM Box with reduced SWaP-C (Size, Weight, Power and Cost):

- The UTM Box should be of small size and weight;
- The UTM Box should need low power supply;
- The UTM Box size and weight should be reduced and with a suitable form factor in order to be easily installed;
- The cost of the UTM Box should meet user willingness to pay.

Moreover, the UTM Box will have a separated GNSS antenna which may be perceived as a hurdle by end users. This antenna will be fixed on the drone or on the top of the UTM Box for better usability. The UTM Box GA version will have a separated antenna for GNSS and another one for the VHF signals (e.g., FLARM in/out, ADS-B in). However, the UTM Box will be compact, with the antennas directly connected to the RF SMA connector. This will minimize the usability issues. Such feedback was collected during the first Advisory Board of CERTIFLIGHT project by UAS and GA pilots and this proposal appears as the best trade-off between usability and performance.

User/Operator: Main UTM Box requirements	
Size & weight	• Small size and weight
Degree of mobility / portability	• Handhelds terminals to be easily installed
Power consumption	• Low power consumption • Powered by the UAS battery or self-powered

Other requirements	• Environmental conditions of operations: -30 / + 50 gr. C. • Useful life of the box: Years / Standard useful life of a device • Separated antenna connected by a RF SMA connector and fixed on the drone or on the top of the UTM Box
Maximum cost	• Based on user willingness to pay

Table 5-1 UTM box requirements

6 Use cases' regulatory assessment

The use cases that will be demonstrated during the project have been identified and initially described in CERTIFLIGHT D2.1 Users needs and Use cases identification [RD 6]. They will provide the possibility to test CERTIFLIGHT platform and verify the proper implementation of some UTM services.

According to the Regulation (EU) 2019/947 [RD 5], UAS operations fall into one of three possible categories:

- "Open" – UAS operations with a low risk to society that do not need any regulatory approval. These include small UAS, often multicopters, flying in VLOS (Visual Line Of Sight) at less than 400 ft Above Ground Level (AGL). These UAS may in no case have an MTOM (Maximum Take Off Mass) > 25 kg (4kg over populated areas).
- "Specific" – UAS operations with a medium risk to society. These typically include a relatively small UAS flying above urban areas, or large UAS flying over non-populated areas, or peculiar flight performances or airspaces where conflicting traffic may be present (e.g. controlled airspace, flying above 400 ft AGL).
- "Certified" – UAS operations with a high risk to society. In this case, the entire range of aviation regulatory processes (i.e. airworthiness, licensing of remote pilots and requirements for the organisation of the operator) applies.

According to Art. 40 of Delegated Regulation (EU) 2019/945 [RD 4], in case of transport of people, the UAS must be certified, i.e. a valid Certificate of Airworthiness issued by the State of Manufacture, based on a Type Certificate issued by EASA, must be available. In the 'Certified' category the remote pilots shall be licenced, and the operator's organisation shall be certified. This regulation [RD 4] defines the requirements related to the design and manufacture of UA in relation to the conditions and rules that are stated in Implementing Regulation (EU) 2019/947 when operating an UA. Particularly, it contains the UAS requirements related to specific characteristics and functionalities required to reduce the flight safety risk, respect of the privacy, protection of personal data, security and environment associated with the UAS operation. In particular, it includes the classes of UAS and the requirements for direct remote identification and Geo-awareness services.

As abovementioned, Regulation 2019/947 splits UAS operations in three categories based on a principle of proportionality: each category is associated to a given risk level and is regulated by a different set of limitations/requirements. The risk related to each category takes into account technical features of the UAS (e.g., Maximum Take Off Mass), operational aspects (e.g., maximum operational altitude and flight conduction) and remote crew competencies.

The three types of UAS operation categories are: OPEN (low risk), SPECIFIC (medium risk) and CERTIFIED (high risk). Their limitations and requirements are listed in the table below.

UAS operation category		Limitations/Characteristics
OPEN	*A1 (over the people)*	1. MTOM (Maximum Take-Off Mass): < 900 g or energy transmitted to the human head is less than 80 J. 2. Flight conduction: VLOS (Visual Line Of Sight).

UAS operation category		Limitations/Characteristics
		3. Maximum operational height: 120m AGL (Above Ground Level) from the closest point on the surface of the earth. When flying an unmanned aircraft within a horizontal distance of 50 meters from an artificial obstacle taller than 105 meters, the maximum height of the UAS operation may be increased up to 15 meters above the height of the obstacle at the request of the entity responsible for the obstacle. 4. Horizontal distance: no distance limits from urban area but not flying over uninvolved persons. 5. Maximum operating speed: < 19 m/s. The A1 OPEN category does NOT allow the transport of people or flying over assembly of people. Moreover, carrying of dangerous goods and dropping any material is NOT allowed.
	A2 (close to people)	1. MTOM: < 4 kg. 2. Flight conduction: VLOS. 3. Maximum operational height: 120m AGL from the closest point on the surface of the earth. When flying an unmanned aircraft within a horizontal distance of 50 meters from an artificial obstacle taller than 105 meters, the maximum height of the UAS operation may be increased up to 15 meters above the height of the obstacle at the request of the entity responsible for the obstacle. 4. Horizontal distance: 30 meters from uninvolved people. This distance can be reduced to a minimum of 5 meters from uninvolved persons when operating an UA with an active low speed mode function. The A2 OPEN category does NOT allow the transport of people or flying over assembly of people. Moreover, carrying of dangerous goods and dropping any material is NOT allowed.
	A3 (far from people)	1. MTOM: < 25kg. 2. Flight conduction: VLOS. 3. Maximum operational height: 120m (400ft) AGL from the closest point on the surface of the earth. When flying an unmanned aircraft within a horizontal distance of 50 meters from an artificial obstacle taller than 105 meters, the maximum height of the UAS operation may be increased up to 15 meters above the height of the obstacle at the request of the entity responsible for the obstacle. 4. Horizontal distance: at least 150 m from residential areas. The A3 OPEN category does NOT allow flying over assembly of people. Moreover, carrying of dangerous goods and dropping any material is NOT allowed.

UAS operation category	Limitations/Characteristics
SPECIFIC	Operations exceeding the limitations settled by the OPEN category can be performed in the SPECIFIC category but when the risk is too high the operation falls into CERTIFIED category. 1. Flight conduction: VLOS/EVLOS (Extended Visual Line Of Sight) and/or BVLOS (Beyond Visual Line Of Sight). 2. MTOM: no limitations. 3. Operational height: no limitations. 4. Maximum characteristic dimension: no limitations except < 3 m when flying over assemblies of people. The SPECIFIC category does NOT allow the transport of people or carrying of dangerous goods if it represents a high risk for third parties in case of an accident. GM1 to Article 6 of Commission Regulation (EU) 2019/947 states that, in case the payload is ensured and transported by a crash-proof container, the operation falls in the Specific category.
CERTIFIED	Operations exceeding the operative limits settled by the SPECIFIC category falls into the CERTIFIED category (Art. 6 of Commission Implementing Regulation (EU) 2019/947). As stated in Art. 40 of Commission Delegated Regulation (EU) 2019/945, UAS operations characterized by the following characteristics fall in the CERTIFIED category: 1. Maximum characteristic dimension: no limitations. 2. Transport of people: allowed. 3. Carrying of dangerous goods: allowed.

Table 6-1 UAS operations categories' specifications

According to Article 5 of Commission Regulation (EU) 2019/947, to operate in the specific category an operational authorisation is required. When applying to a competent authority for an operational authorisation, the operator shall perform a risk assessment in accordance with Article 11 of [RD 5] and submit it together with the application, including adequate mitigating measures. A risk assessment can be conducted by using SORA methodology identified as AMC to Article 11 to [RD 5].

Other possible ways to operate in Specific category are:

- Submit an operational declaration to the competent authority of the MS (Member State) of registration in order to carry out an operation complying with an STS (Standard Scenario). Appendix 1 of the Commission Implementing Regulation (EU) 2020/639 [RD 17] provides all the requirements that the UAS operator shall meet in order to perform operations under STS-01 and STS-02; whereas Appendix 2 of this Regulation gives the template of an operational declaration.
- Obtain an operational authorization after having demonstrated compliance with the requirements of a PDRA (Pre-Defined Risk Assessment). EASA published 5 PDRAs as AMC (Acceptable Means of Compliance) to [RD 5].

- Obtain a LUC (Light UAS operator Certificate) after showing compliance with the requirements provided in Part C to [RD 5]. The LUC is issued by the NAA (National Aviation Authority) after checking the organisation and, particularly, the SMS (Safety Management System) in place, and it allows the operator to self-assess the risk of its operation and self-authorise it. After approving the UAS operator complies with requirements stated in Part C to [RD 5], the NAA provides UAS operations specification (operator name, UAS model, type of UAS operations, special limitations).

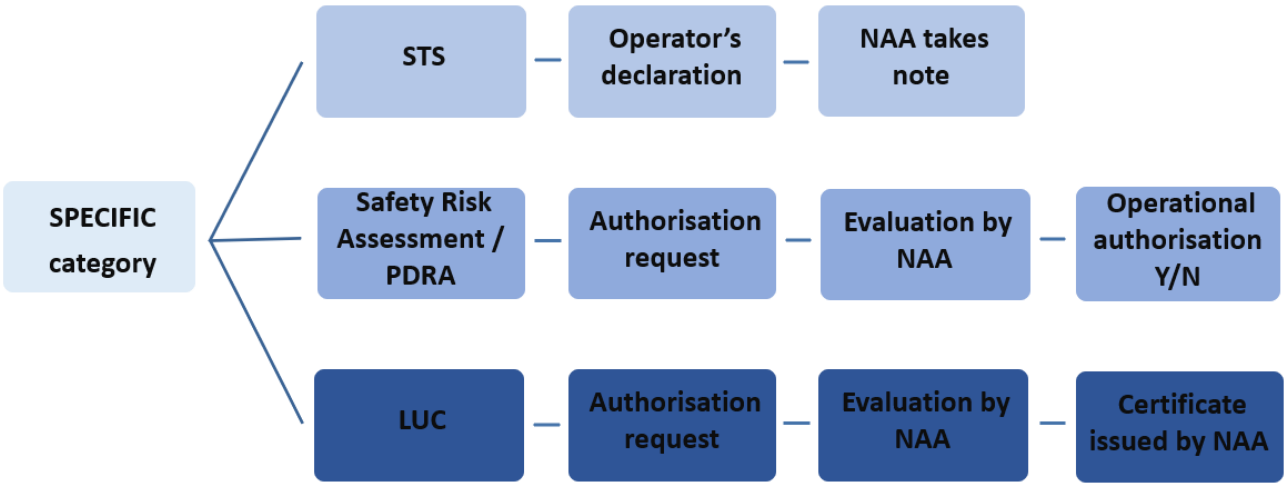

Figure 6-1 Operations in Specific category

All the use cases expected during the project, listed in D2.1 [RD 6], are provided in the following table where the related UAS operation category is indicated.

Use case title	Owner	Category	Regulatory Aspects
Highly Automated UAS operations	TOP	Open (A3)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC)
Last mile delivery operations	TOP	Open (A3)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC)
Airspace Infringement / E-Conspicuity	DTA	Specific (operational declaration: IT-STS-02)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC) • Circular ATM-09A (ENAC) • Operational procedures of Flight Test Center in Taranto-Grottaglie, rev.2, 20/05/2021 • R148: AIP ITALIA ENR 5.1.2 "Regulated Zones"
Agriculture applications	DTA	Open (A3)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC)
Industrial applications	UPV	Specific (operational authorisation: risk	• EU Regulation 2019/947 • General Measure LKR10–UAS (Czech Republic CAA)

Use case title	Owner	Category	Regulatory Aspects
		assessment through SORA methodology)	
Port surveillance with UAS	UNIFLY	Open (A2) & Specific (operational authorisation: risk assessment through SORA methodology)	• EU Regulation 2019/947 • Royal Decree RPAS (Belgium CAA)
Platform Interoperability	UPV	Specific (operational authorisation: risk assessment through SORA methodology)	• EU Regulation 2019/947 • General Measure LKR10–UAS (Czech Republic CAA)
Fisheries	TOP	Open (A2)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC)
Airport runway inspection	DTA	Specific (operational authorisation: risk assessment through SORA methodology)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC) • Circular ATM-09A (ENAC) • Operational procedures of Flight Test Center in Taranto-Grottaglie, rev.2, 20/05/2021
Accident investigation	TOP	Open (A2)	• EU Regulation 2019/947 • Regulation UAS-IT (ENAC)

Table 6-2 CERTIFLIGHT use cases' categories of operations

The U-space regulatory framework [RD 1, RD 2, RD 3] introduced to harmonize the conditions necessary for manned and unmanned aircraft to operate safely in the designated airspace for UAS operations provides 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. The UTM services implemented through CERTIFLIGHT platform and their relationship with respect to U-space European Regulations are provided in Table 3-1.

7 Matching legal aspects with the service development

CERTIFLIGHT introduces a new service based on fully 'automated' contractual arrangements, opening up new scenarios and opportunities with a considerable impact on the performance of operators in the sector and their profits.

The project aims to exploit the technological progress in the sphere of legal services, helping institutions in providing tools capable of pursuing the key principles envisaged in U-space, for instance automation and digitalization. In particular, the CERTIFLIGHT solution aims to be recognised as a tool for:

- Determining the parties' liability; and
- Activating specific contractual terms also conditional to UAS flight trajectories and position information.

Currently this technology is not specifically regulated by law. However, it can be accepted by the parties of the agreement, as a tool for the verification and compliance with the negotiation and a way of execution of the contract.
The technology, and in particular the telemetry of vehicles and aircraft, is already used in some comparable situations to assess responsibilities and execute contracts. Some examples are the black boxes of traditional aviation and the transponders used for electronic toll collection.
In addition, the telemetry boxes used in the automotive market by some insurance companies to offer lower insurance fees, also has many similarities with the devices envisioned for CERTIFLIGHT.
Indeed, such telemetry boxes, in combination with AI cloud algorithms, are capable to better estimate the risk of each driver based on driving data collected and their driving style.
These telemetry boxes are often proposed in combination with dash cams that have been already recognized as an efficient tool during legal disputes in case of accidents.

In this context, the blockchain technology has the precise role to freeze the content of that contract over time and thereby facilitating the resolution of any disputes that may arise.
The blockchain can be framed as a general-purpose technology, by which is meant that it can be exploited for a wide range of uses; it is, in fact, both a database and a network, a tool for storing information and 'a programmable platform on which further applications can work'.
In the blockchain a recognized distinction can be done between passive ledger and active ledger.
The blockchain used as a 'passive ledger' is similar to a database with the classic purpose of storing information but endowed with the peculiarities of this technology compared to 'traditional' databases. Among the peculiarities of blockchain that make it an attractive technology for 'passive ledgers' there is, firstly, the immutability of the recorded data. Secondly, blockchain can be used as an 'active ledger', i.e. as a technology that allows a network of users to carry out exchange transactions. In particular, the users of a second-generation blockchain can create digital assets other than the blockchain's 'native' cryptocurrency, the so-called 'tokens', as well as software programmes through which tokens can be exchanged on the basis of pre-set conditions (so-called Smart Contracts). We refer to the smart contract as a tool used in conjunction with blockchain technology, thus considering the smart contract as a particular 'second-level application' based on the underlying blockchain infrastructure.

The huge interest of the today's economy in blockchain is a matter of fact, although 'doing business' with Distributed Ledger Technologies (DLT) is still not easy, due to the 'usual' problems of

bureaucracy. Indeed, the greatest effort is to bring CERTIFLIGHT down to the institutions that have characterised European and international contracting for decades. Therefore, CERTIFLIGHT can be configured as contract for service provision, with important benefits in term of certainty, transparency, predictability and reliability, saving also a considerable amount of resources in the negotiation and contract execution phases. Moreover, it can speed up performance and significantly reduce the likelihood of non-performance by the parties or the occurrence of disputes between them.

However, to better understand the impact of CERTIFLIGHT in the legal sphere it is important to question about the parties involved in the service provision. The nominal case of CERTIFLIGHT may foresee three parties involved in the service:

1. Technology provider, which is CERTIFLIGHT that sells the flight track certification service including the UTM transponder and certification portal.
2. Flight operator, which buys the CERTIFLIGHT solution to enhance its value proposition and get addition protection against possible legal disputes.
3. Auditor, the subject interested in the right execution of the agreement, which recognize the use of CERTIFLIGHT technology as a tool for liability determination and contract execution. The auditor should have direct access to the CERTIFLIGHT platform.

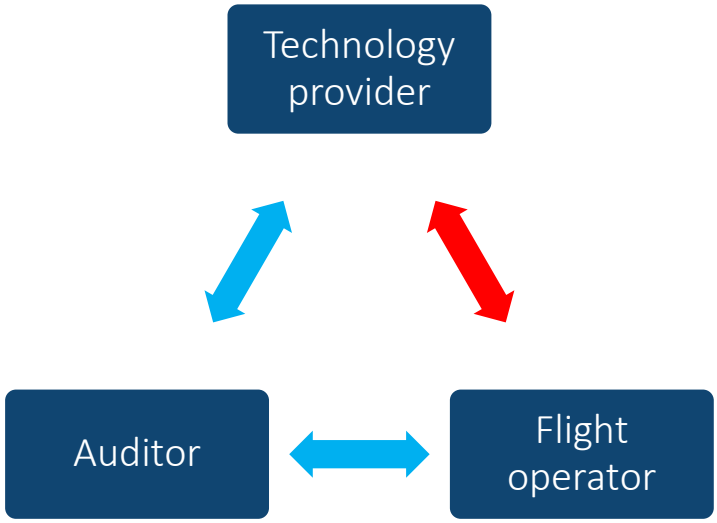

Figure 7-1 Parties involved in the CERTIFLIGHT service (red arrow represents an agreement)

The figure 7-1 shows the two-ways relationships between each of the parties.
The red arrow highlights the agreement between the technology provider and the flight operator, while the non-contractual relationship with the auditor is in light blue.
In the bilateral relationship between supplier and flight operator, the findings will be certain and not contestable. Instead, responsibilities will not only be defined and classified, as in any service provision relationship, but will also be easily identifiable.

An example might be the flight operator's unconventional use of the supplied device. In this case, the Auditor, i.e. the person who has an interest in the correct execution of the contract and the appropriate use of CERTIFLIGHT technology, will be able to enjoy the following benefits:

- Increased transparency of contractual terms
- Recovery of efficiency through certain automations

- Reduced risk of divergent interpretation
- Increased evidential value
- Interoperability

Moreover, it's important to specify that the party "auditor" may assume different shapes depending on the use cases and the features identified in the deliverable D2.1 [RD 6].

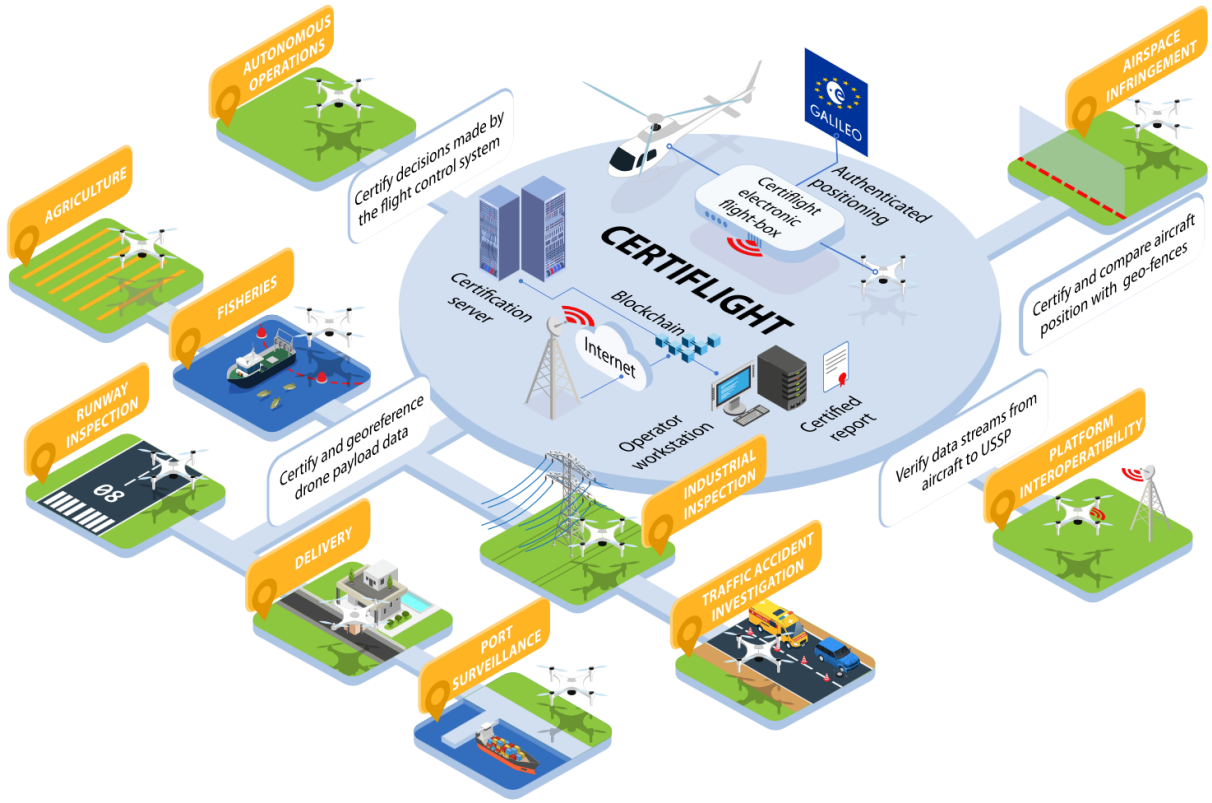

Figure 7-2 Use cases grouped by offered features

Looking at Figure 7-2, for instance, in the group of "certify and georeferenced drone payload data" feature, the "auditor" could either be a customer of the flight operator or an authority. But if the interested feature is "certify ad compare aircraft position with geo-fences" the auditor is probably the Authority.
This means that CERTIFLIGHT technology can be part of private or public agreements, with different regulation behind.
Be aware of the needs and relationships among these parties is fundamental to match the legal aspect in developing the CERTIFLIGHT service.

Lastly, in the near future, through blockchain implementations, there will be an upheaval in the regulatory framework of legal systems, and rather than total reforms there will be a need to shape their laws and legal institutions.