Annex II to Invitation to Participate 'Descriptive document for the EGNOS Service Data Access Facility (SDAF)'

Reference:

GSA-EGN-SDAF-SPC-A09521

Issue/Version: 1.0

Date: 07/05/2021

Change log:			
Issue/ Version			
1.0	First release		

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The present document details the needs of the European GNSS Agency (GSA) in relation to the procurement of the Service Data Access Facility (SDAF), highlighting the scope and objectives of the SDAF procurement.

Pursuant to point 7 of Annex I of the Financial Regulation, this documents defines the minimum requirements of the required solution, allowing the Candidates to decide whether to request to participate in the innovation partnership procedure.

The present document is annexed to the Tender Specifications (Annex I) for the procurement procedure GSA/IP/23/20.

2 Acronyms and Abbreviations

Table 1 - Abbreviations

Abbreviation	Definition
ANSP	Air Navigation Service Provider
API	Application Programming Interface
AR	Acceptance Review
CCF	Central Control Facility
CFI	Customer Furnished Item
DC	Data Center
DFMC	Dual Frequency Multi Constellation
DGNSS	Differential GNSS
EC	European Commission
ECSS	European Cooperation for Space Standardization
EDAS	EGNOS Data Access Service
EDAS SP	EDAS Service Provider
EGNOS	European Geostationary Navigation Overlay Service
EOW	End of warranty

Abbreviation	Definition
EU	European Union
EUCI	EU classified information
EUSPA	European Union Agency for Space Programme
ESA	European Space Agency
ESP	EGNOS Service Provider
EWAN	EGNOS Wide Area Network
FDIR	Fault Detection Isolation and Recovery
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System (e.g. GPS, Galileo, GLONASS etc.)
GSA	European GNSS Agency
GSC	GNSS Service Centre
IP	Innovation Partnership
MCC	Mission Control Centre
MSI	Maritime Safety Information
NOTAM	Notice to Airmen
NTRIP	Network Transport of RTCM via Internet Protocol
RINEX	Receiver INdependent EXchange
RTCM	Radio Technical Commission for Maritime Services
SAA	Security Accreditation Authority
SC	Service Center
SDAF	Service Data Access Facility

Abbreviation	Definition
SIS	Signal In Space
SISNET	Signal In Space through Internet
TS	Technical Specification

3 Applicable and Reference Documents

Table 2 - Applicable Documents

Applicable Documents:		
Type	**Title**	**Reference**

Table 3 - Reference Documents

Reference Documents:		
Type	**Title**	**Reference**
[RD.1]	https://egnos-user-support.essp-sas.eu/new_egnos_ops/	EGNOS User Support Web
[RD.2]	EDAS Service Definition Document, issue: 2.2, date: June 3, 2019	EDAS SDD
[RD.3]	Agile software development handbook	ECSS-E-HB-40-01A, Date: 7 April 2020

Candidates are informed that the following documents will become applicable in the next phases of the procurement procedure:

- SDAF High Level Requirements Document (HLRD)
- EGNOS Product Security Requirements (including requirements on Security Development and Accreditation Plan, security risk analysis, hardening/lock-down, vulnerability, patch management, etc.)
- EGNOS V2 System to EDAS External Interface Requirements Document.

- EGNOS V2 System to EDAS Interface Control Document
- EGNOS V3 System to EDAS External Interface Requirements Document.
- EGNOS V3 System to EDAS Interface Control Document
- SDAF to GSC System Interface Requirements Document / System Interface Control Document
- EURONOTAM Interface Control Document
- MCC V3 Site Interface Requirement Document / Site Interface Control Document
- GSC Site Interface Requirement Document / Site Interface Control Document
- NTRIP Package - Network Transport of RTCM via Internet Protocol, RTCM 10410.1 / RTCM 10410.0, Date 28/06/2011
- SISNeT User Interface Document, E-RD-SYS-31-010 is. 3.1, 15/05/2006 (TBC)
- RTCM Standards, RTCM 10403.3, RTCM 10403.1, RTCM 10402.3
- RINEX Standards, Versions 3.x, 2.x and IONEX.

Note: An Interface Requirements Document contains the specifications of the interface, whilst its associated Interface Control Document provides detailed information and definitions for the implementation of such interface.

4 Context

4.1 SDAF Contribution to EGNOS objectives

The objectives of EGNOS for the next decade are summarised below:

- deliver high quality, continuous, safe and secure EGNOS Services;
- ensure smooth transition from EGNOS V2 to EGNOS V3 infrastructure with no or minimum impact on the users (in terms of service interruption);
- Ensure security of the EGNOS service provision;
- increase the robustness and level of services with the augmentation of Galileo and provision of Dual-Frequency Multi-Constellation (DFMC) services;
- foster the use of EGNOS with the development of new applications and services (maritime service for instance);
- enlarge the number of EGNOS Users communities;
- extend the geographical coverage of EGNOS Services (to Africa and Eastern Neighbourhood countries).

With regards to the first objective above mentioned, three EGNOS services are currently provided: 1) the Open Service (OS) – free, open to the public and used by mass-market receivers and common user applications; 2) the Safety of Life Service (SoL) - for safety-critical transport applications, including civil aviation, which require enhanced and guaranteed performance and an integrity warning system; and 3) EGNOS Data Access Services (EDAS) - offered on a controlled access basis (i.e. via the Internet) for customers requiring enhanced performance for professional use.

The above-mentioned services are complemented by other data dissemination services such as the EGNOS Prediction Service which provide predictions/notifications/warnings on the service status via dedicated networks.

With regards to the third objective above mentioned, the EGNOS Infrastructure is subject to a security accreditation process defined in the Regulation (EU) 1285/2013 on the implementation and exploitation of European satellite navigation systems. A Security Accreditation Authority (SAA) is responsible for the EGNOS accreditation, i.e. to verify that EGNOS comply with the applicable security rules and regulations as established by the Council and the European Commission. The SAA take 'security accreditation decisions' in particular on the approval of the EGNOS security accreditation strategy, the authorisation to operate EGNOS and associated Hosting Sites in their different configurations and for the various services.

The Service Data Access Facility will contribute to EGNOS with the following objectives:

- it will support the delivery of the EDAS and other EGNOS data dissemination services,
- it will secure and control the access of users to EGNOS data through the Internet,
- it will be introduced in the EGNOS infrastructure to ensure smooth transition from V2 to V3,
- it will have to comply to the EGNOS applicable security rules and regulations with justifications feeding the overall EGNOS security accreditation process.

4.2 Description of the EGNOS infrastructure

EGNOS V2 and V3 share the same architectural concept even though they are two different systems:

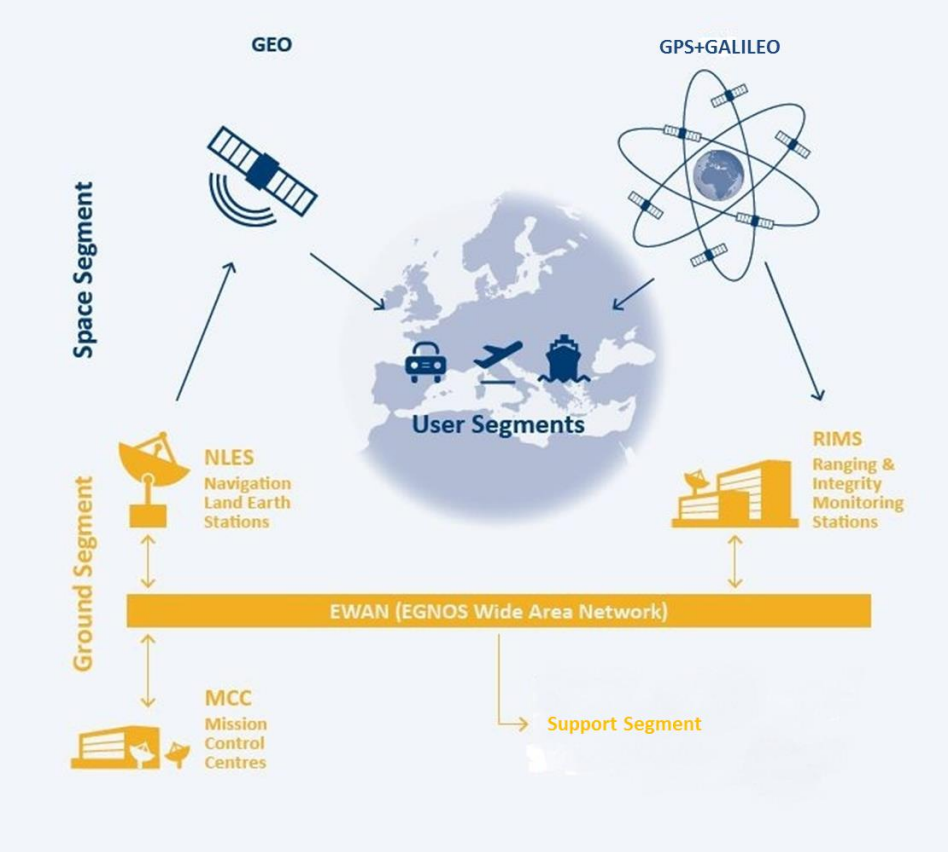

Figure 1 - EGNOS High level architecture

The EGNOS space segment, composed of EGNOS geostationary (GEO) satellites, broadcast corrections and integrity information to be applied to the GPS constellation in EGNOS V2 and to the GPS and Galileo constellations in the future EGNOS V3. The coverage area is primarily the EU-Member States, Norway and Switzerland Flight Instrument Regions (FIRs).

The EGNOS ground segment is in charge for the computation of the integrity measurements and wide area differential corrections. To this purpose a set of Ranging and Integrity Monitoring Stations (RIMS) are deployed and operated within and beyond the European Union territories. The RIMS collect the GPS, Galileo (for V3) and EGNOS GEO raw pseudo-range measurements. The network of RIMS is connected to two Mission Control Centres (MCCs) (of which one is master) where the integrity, differential corrections, ionospheric delays are computed by the Central Processing Facility (CPF). This information is sent in a message to the Navigation Land Earth Stations (NLES) to be uplinked in a GPS-like signal to the two GEO satellites. The ground segment is operated from the Central Control Facility (CCF) located in the MCCs. All EGNOS sites are connected through an EGNOS Wide Area Network (EWAN).

The EGNOS infrastructure is complemented by:

- The EDAS server which supports the provision of EDAS services based on data provided by EGNOS system and interfaces with the EuroNOTAM tool;
- The EuroNOTAM tool which prepares Notice to Air Men proposals (an equivalent tool will be developed for maritime users);
- The service provision user interface (I/F) tools, i.e. the EGNOS User support website and helpdesk;
- The service performance monitoring tools used to monitor the provided level of services;
- Other tools required for the EGNOS service provision.

Information on the current EDAS solution will be made available in Phase II of the tender process for the possible use in the SDAF solution and without prejudice to its innovative character.

The SDAF will be introduced in the EGNOS infrastructure replacing the EDAS server to support the provision of EDAS, EGNOS NOTAM proposals services and other EGNOS data dissemination services.

The European GNSS Service Centre, GSC, is the element of the European GNSS infrastructure acting as the single interface between the system established under the Galileo programme and progressively other elements of the EU space programme (such as specific EGNOS services). P art of SDAF infrastructure will be hosted in the GSC premises. In addition, the SDAF will interface with the GSC infrastructure to enable the provision of EDAS services.

5 Needs of the Agency

The objective of the present procedure is to procure the Service Data Access Facility (SDAF) with the following minimum requirements:

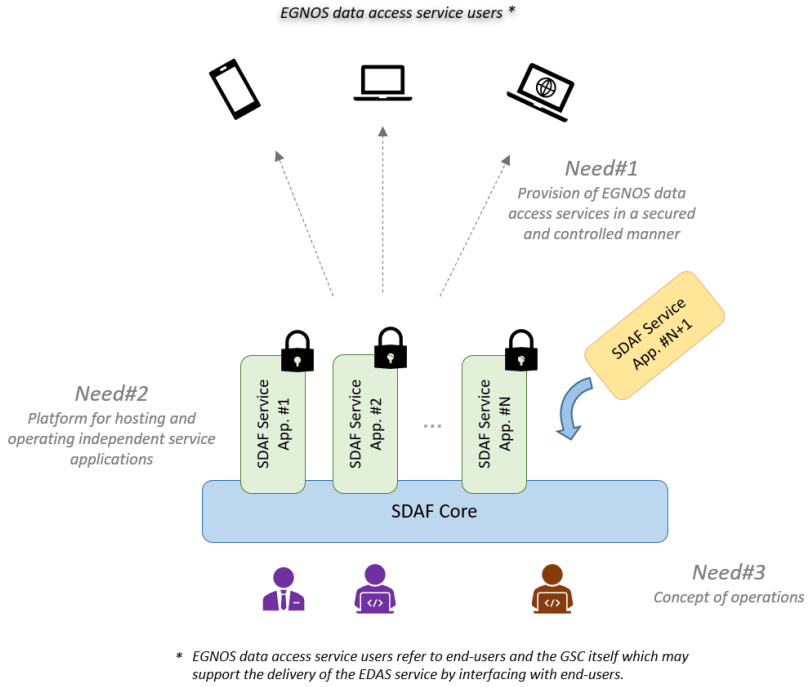

Figure 2: SDAF Needs

5.1.1 Need#1: Provision of EGNOS data access services in a secured and controlled manner

The SDAF shall provide EGNOS data access services, in a secured and controlled manner, to users connected to the Internet or dedicated terrestrial lines.

For all services provided by the SDAF, the EDAS Service Provider has the full control of the SDAF user access management. As such, the EDAS Service Provider is responsible to approve, manage and potentially revoke per user and/or service any access to data provided at the output of the SDAF.

The EGNOS data access services delivered through SDAF can be divided into three main categories according to users and entity delivering the service:

- EDAS services:

  These services are provided by applications designed/developed/procured by the EDAS Service Provider.

  These services are delivered directly to EDAS users:

  - In real-time: Broadcast of EGNOS near real-time data formatted according to required EDAS formats and protocols (e.g. NTRIP caster)
  - In non-real time: Transfer of files (e.g. through FTP/secured FTP) containing EGNOS data formatted according to required EDAS formats.

- Privileged EGNOS data access services supporting ESP Services (meaning all the EGNOS services except EDAS public/privileged services):

  These services are based on applications designed/developed/procured by the EGNOS Service Provider.

  They are delivered to a list of privileged users identified by the EGNOS Service Provider, including the EGNOS Service Provider itself which uses them to support its activities. Typical applications are related to EGNOS Service Prediction: delivery of the NOTAM proposals, delivery of the Maritime Safety Information.

- Privileged EGNOS data access services supporting other EGNOS Services:

  These services are based on applications designed/developed/procured by the EDAS Service Provider.

  They are delivered to privileged users:

  - In real-time: Broadcast of EGNOS near real-time data formatted following standard formats and protocols (e.g. NTRIP) or as raw data following EGNOS system output format
  - In real-time under low latency mode: allowing to retrieve EGNOS data under SDAF control with a very low latency introduced by the SDAF in order to feed real time external applications
  - In non-real time/on-demand: Transfer of files (e.g. through FTP/secured FTP) containing EGNOS data formatted according to required formats.

The EGNOS data access services delivered through SDAF are accessed by:

- The EDAS users who have access to all or part of the services publicly declared in the EDAS Service Definition Document. For further information on EDAS the candidates are invited to consult the EGNOS User Support Webpage [RD.1] and the EDAS Service Definition Document [RD.2].
- The privileged users who are granted by the EGNOS Programme with an ad-hoc access to data/services which may not be provided as part of the publicly declared EDAS services.

  On top of the EGNOS Service Provider, GSA, ESA, ANSPs, NOTAM Offices, EGNOS Product Manufacturer and Maintainers are some examples of such privileged users.

It is envisaged that the European GNSS Service Centre (GSC) may implement a common front-end interface for the delivery of E-GNSS services (including EDAS) directly to end users.

The Table 4 shows the services described above. It does not intend to provide the final configuration of services delivered by SDAF, which will be an outcome of the SDAF design during the innovation partnership execution.

The SDAF solution shall be scalable both in terms of number of users accessing to SDAF services and of provided services.

Table 4 – SDAF based services

Service	Service type	Description
#01: Real Time EDAS	Public (EDAS SP)	This service provides real-time EGNOS data streams in RTCM format following the NTRIP protocol. The EGNOS data provided mainly comprises: - GPS and Galileo observations and navigation data collected by the entire network of EGNOS stations. - EGNOS augmentation messages transmitted by the EGNOS geostationary satellites. - Differential GNSS (DGNSS) and RTK (Real-Time Kinematic) messages allowing users to implement advanced positioning techniques. Each user is able to access simultaneously to a limited number of streams defined by the EDAS Service Provider.
#02: Non Real Time EDAS	Public (EDAS SP)	This service provides historical EGNOS data files available for download. The historical EGNOS data files are generated based on the data collected from the EGNOS stations and published in different formats.
#03: Real Time Privileged Data Dissemination	Privileged (EDAS SP)	This service provides real-time EGNOS data to privileged users in RTCM format following the NTRIP protocol. The difference with respect to the Service #01 relies on the service configuration (e.g. data streams, authorised users, unlimited number of streams per user, supported versions of NTRIP protocol, etc.)
#04: On-demand Privileged Data Dissemination	Privileged (EDAS SP)	This service provides offline EGNOS data products (i.e. EGNOS files) to privileged users by making them available for download or via offline media (e.g. USB, CDROM, etc.). The EGNOS data available to the users may include: - data which have been archived on the SDAF from the EGNOS system output interface; - data which have been archived on the SDAF from the EGNOS archive - data products generated by SDAF.
#05: EGNOS System Data Dissemination	Privileged (EDAS SP)	This service provides EGNOS real-time data following the EGNOS system output interface format
#06: SISNeT (TBC)	Public (EDAS SP)	This service provides EGNOS SIS messages and other navigation data (e.g. ephemeris, ionospheric) following the SISNET protocol. Note: the inclusion of SISNeT service among the list of services delivered by SDAF is still to be confirmed.
#07: EGNOS Service Prediction	Privileged (EGNOS SP)	This service provides service notifications/warnings/predictions on EGNOS service status (NOTAM for aeronautical users, MSI for maritime users).

Note: The type of EGNOS data delivered publicly through EDAS may evolve all along the service lifetime.

In terms of performance, these services shall be provided with high availabiliy (typically 99.9%) and shall allow the concurrent distribution to serveral users (up to 1500). For the near real-time services a latency in the order of [100-500] milliseconds is expected.

5.1.2 Need#2: Platform for hosting and operating independent service applications

The second fundamental need of the SDAF is to provide a service oriented solution enabling the update/addition of services by developing and deploying new applications (or upgrading the existing ones) into the SDAF Product.

As indicated above, two actors will provide services by using the SDAF Product: the EDAS Service Provider and the EGNOS Service Provider.

The SDAF solution needs to ensure independent service provision among all the services delivered through SDAF by offering the capability to:

- supervise each SDAF service independently from the others and detach the operations of the service applications from the underlying core infrastructure operations;
- perform operations (e.g. commanding, managing service configurations, service upgrades, etc.) over one or several SDAF services without impacting the users' experience of the other services;

The SDAF shall consist of a core infrastructure providing services (hardware/software) according to well-defined API(s) to Service Applications, which are in charge of delivering abovementioned services to users.

Candidates are invited to innovate in the design of such solution. Cloud/microservices/service oriented architectures could be some approaches to be studied to satisfy these needs.

The SDAF shall be supplied with built-in service applications in charge of delivering services identified in Table 4. The SDAF shall be able to host other service applications, developed by the SDAF manufacturer or "third-parties" during the lifetime of the SDAF operations.

Hosting of EGNOS Service Prediction tools in the SDAF

The Service Prediction tools are those tools/products providing predictions/notifications/warnings on service status/availability/degradations used to fulfil the obligations towards users having signed EWAs (EGNOS Working Agreements), i.e. generation of NOTAMs, of maritime MSI, etc.

The EuroNOTAM tool is an existing Service Prediction Tool. It supports the delivery of NOTAM proposals to aeronautical users (i.e. NOTAM Offices) complementing the SoL service.

An equivalent tool will be developed for providing Maritime Safety Information to maritime users.

The development/operations/maintenance of the Service Prediction tool supporting the SoL service is under the responsibility of the EGNOS Service Provider.

The EGNOS Service Prediction tools may be hosted by SDAF. Confirmation of such scheme will be provided in Phase II of the tender process. If confirmed, SDAF shall provide the required resources, functionalities and services to host these Service Prediction software tools. The Contractor may be requested to integrate into the SDAF the Service Prediction software tools provided as CFIs.

5.1.3 Need#3: Concept of Operations

The SDAF Product shall be deployed in two operational sites:

- The **SDAF Data Centre (SDAF-DC)**: This is the centre where the main part of the SDAF infrastructure is deployed and operated. It will be collocated with the EGNOS Mission Control Centre (MCC) in Torrejón de Ardoz (Spain).

  SDAF shall allow to perform the following operational activities from this site:

  - Operations and security monitoring of the SDAF
  - First Level Maintenance which mainly includes FDIR actions or HW LRU replacements as per applicable maintenance procedures
  - Second Level Maintenance which encompasses advanced maintenance activities associated with a deeper expertise on the SDAF system such as root cause analysis, troubleshooting or workaround identification.
  - Service delivery management for "#07: EGNOS Service Prediction" (see point above on Service Prediction Tools hosting).

- The **SDAF Service Centre (SDAF-SC)**: This is the main site for the management of SDAF services and the single point of contact for users of SDAF based services. It will be located in the GNSS Service Centre (GSC) premises in Torrejón de Ardoz (Spain).

  SDAF shall allow to perform the following operational activities from this site:

  - User access management: granting/denying user access to SDAF based services and data
  - Supervision of services delivered by SDAF
  - Other service management activities such as service configuration and service transition (i.e. putting new and changed services into operations, declaring some services *"in test"* or proceeding to the service decommissioning)

Notes:

1. Although SDAF shall be deployed in one SDAF Data Centre and one SDAF Service Centre, the study and factory qualification of the solution shall consider the deployment of a full redundancy concept consisting of two Data Centres and up to two Service Centres. The operations scheme (parallel vs master/backup operations) shall also be an outcome of the SDAF system design study. For information, backup Data and Service Centres will be located in EU countries and not collocated with abovementioned MCC (Torrejón) and GSC premises, respectively.
2. Operational roles in SDAF shall be considered available at working hours (8 hours a week during 5 days) except for operators in the SDAF Data Centre which could be on a 24/7 basis.
3. The SDAF concept shall be compatible with the fact that the security monitoring function performed from the SDAF DC can be performed in the future from an external security monitoring facility located outside the MCC.

6 The Procurement: Innovation Partnership Contract

6.1 Structure of the Innovation Partnership

The Innovation Partnership Contract is envisaged to be structured in two stages.

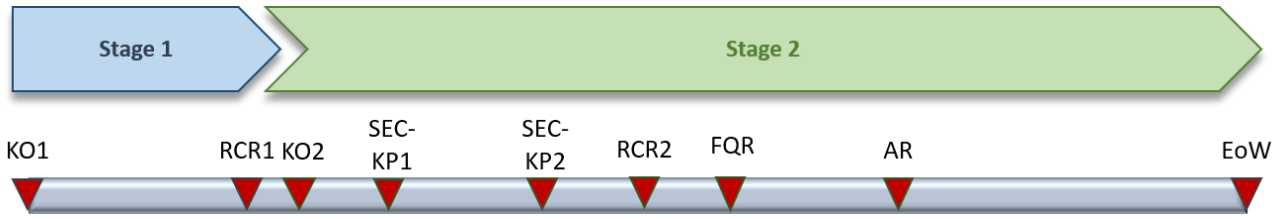

Figure 3: SDAF Innovation Partnership contract and milestones

The main objective for the Stage 1, without being limited to, is to conduct a study to establish a preliminary technical baseline of SDAF including technical specifications, architecture, design and verification approach stemming from the high level specifications of SDAF provided by the Customer.

The Stage 2 comprises various objectives:

- The completion of the study with the aim to baseline the technical specifications, design and verification approach for the SDAF Product.
- The development and testing of the SDAF according to the technical specifications.
- The execution of a formal qualification process leading to the generation of the in-factory qualified SDAF Release.
- The deployment of SDAF in the operational sites and the interconnection with its external interfaces.
- The on-site acceptance of the SDAF System including support to operation for hand over followed by one year of warranty.
- possible maintenance support.

Candidates are required to propose their development methodology taking into account the following:

- The process shall be driven by the milestones and objectives defined in section 6.2.
- Up to RCR2, the Contractor shall present the status of the study through iterations with the Customer. During these iterations the study progress shall be substantiated by the outcomes of prototypes or beta releases of the future product and intermediate analysis results. Iterations methodology is to be proposed by the Contractor and may be based on an Agile approach similar to the one described in [RD.3].

- Dedicated key points or workshops may be needed during the contract execution, for instance to address integration with external interfaces (e.g. the EGNOS system, the GSC), define aspects of the operational concept, training, etc.
- The SDAF is part of the EGNOS infrastructure which is subject to a security accreditation process. As such, the Contractor will be required to produce, implement and enforce: a design including the necessary infrastructure and applications for security, a security plan aimed at feeding at specific milestones the overall security accreditation process managed by the Customer, for which the Contractor will have to ensure the security capability of the product, and thus implement any required changes by the SAA on the design.
- During the on-site integration phase (between FQR and AR), the Contractor will be requested to follow a security process aimed to obtain the authorisation to deploy SDAF in the operational sites and connect it to its external interfaces. In this phase, dedicated testing activities with operational actors' witnessing will be also required to ensure the product will be ready to be operated on-site. The Contractor will also support the SDAF handover process to the operational actors.
- Maintenance support may be also required to the Contractor.
- Elements of innovation of the proposed solutions shall be at any time clearly described and justified.

6.2 Project Milestones

6.2.1 Stage 1

Table 5 – Milestones in Stage 1

Milestone		Objectives
KO1	Kick-Off Stage 1	- Review development roadmap up to the RCR1. - Review the objectives of the first Agile iteration or equivalent proposed methodology related to Stage 1 study - Verify that development environment and resources required to start the Stage 1 are available.
RCR1	Release Consolidation Review #1	- Demonstrate the following objectives are achieved and addressed in the SDAF documentation: ○ the SDAF technical specifications produced by the Contractor cover the customer requirements and provide such traceability; ○ the proposed architecture and design meet the technical specifications (included security) providing justifications; ○ the proposed verification approach cover all the technical specifications. - Review the product development roadmap and confirm the feasibility to achieve, during next stage, the objectives set for the Stage 2.

		- Confirm the SDAF security feared events - Establish a Preliminary Security Risk Analysis to confirm stage 1 answer to the SDAF risk objectives - Demonstrate that risk assessment process and the risk treatment plan are established and documented as to lower the risk at a level consistent with the security requirements.

6.2.2 Stage 2

Table 6 – Milestones in Stage 2

KO2	Kick-Off Stage 2	- Review the objectives of the next Agile iteration or equivalent proposed methodology related to product development. - Review the product development roadmap up to the RCR2 - Authorise the launch of target hardware procurement
SEC-KP1	Security Key Point #1	- Consolidate a Security Risk Analysis based on chosen architecture and technologies validated at the end of Stage 1 RCR1 and with objectives set for stage 2. - Update the risk treatment plan based on the architecture and technologies validated at RCR1 - Establish the product Security Operational Procedures (SECOPS) sustaining the security functions
SEC-KP2	Security Key Point #2	- Establish and confirm through justifications the SDAF security functions. - Update and finalize the Security Operational Procedures (SECOPS) sustaining the security functions - Verify the implementation of the security treatment plan according the security risk analysis and the security assurance activities - Confirm the risk level targeted for RCR2
RCR2	Release Consolidation Review #2	- Approve the technical baseline of the product, i.e. consolidate final version of the SDAF requirements, architecture, security, design and verification documents including its traceability to the Customer´s requirements. - Review the qualification process to be undertaken for the production of the SDAF release.
FQR	Factory Qualification Review	- Verify the outcomes of the qualification process at Contractor's premises. - Demonstrate that the qualified SDAF release is compliant with all the specifications of the product and can be deployed in its operational sites and connected to its external interfaces.
AR	Acceptance	- Demonstrate that the SDAF operates correctly once deployed and confronted

	Review	to the real environment, i.e. that the achieved compliance with the SDAF technical requirements and the demonstration of the technically robustness and operational readiness is maintained on site - Support the handover process to the operations
EOW	End of Warranty	- Verify the warranty objectives are achieved.
MSKP	Maintenance Service key point(s) (if maintenance is required)	- Accepting maintenance support services if required.

In the course of the execution of the innovation partnership contract and in the transition between the stages of the innovation partnership as described under section 5 of the tender specifications, adjustment of technical specifications, functionalities and performance of the SDAF infrastructure may take place. This is to be seen as inherent to the innovation process and not intended to affect equality of treatment between candidates and transparency of the procurement procedure.

For the present procurement the relevant technical, functional and security requirements are defined in the technical specification to be communicated in Phase II of the procurement.

The awarded tenderers will conclude the Innovation Partnership contract with the commitment of Stage 1 of such Contract. The activities performed under Stage 1 constitute an intermediary target of the innovation partnership contract for the purposes of point 7 of Annex I of the FR. Such activities will be compensated according to the payment plan in section **Error! Reference source not found.** and following the successful achievement of the milestones, set out in the innovation partnership contract.

It is underlined that the successful completion of the Stage 1 review milestone(s) is a necessary but not sufficient condition for the activation of the contract Stage 2. The criteria for accessing Stage 2 of the innovation partnership contract are defined in section 5 of the tender specifications (Annex I to the Invitation to Participate).

6.3 Project Deliverables

The deliverable items requested are listed here for information.

The deliverable of the stage 1 are the results of the study, composed of:

- The SDAF Product Documentation including:

  - Technical Specification Document
  - Design Documentation
  - Verification Documentation
  - Operations and maintenance concept.
  - Security Documentation
- Project Documentation (Plans, reports, etc.)

The deliverable of the stage 2 is the SDAF product composed of:

- Two SDAF Data Centre platforms (hardware and software)
- One SDAF Service Centre platform (hardware and software)
- SDAF Test Platform(s) (hardware and software), including development environment and tools.
- The associated SDAF Product Documentation including:
  - Technical Specification Document
  - Design Documentation
  - Verification Documentation
  - Operations and maintenance manuals.
  - Security Documentation
- Source code (documented)
- Training material (training program, manual, etc.)
- Project Documentation (Plans, reports, etc.)

Note: This is non-exhaustive list provided for information only. The list of deliverables will be documented in the ITT SOW (in Phase II of tender procedure as indicated in section 2 of Annex I – Tender Specifications).

6.4 Indicative timeline

An indicative timeline of the SDAF project execution is provided for information:

Table 7 – Indicative timeline of the Contract

Stage	Milestone		Date
Stage 1	KO1	Kick-Off Stage 1	T0
	RCR1	Release Consolidation Review #1	T0+7 months

Stage 2	KO2	Kick-Off Stage 2	T1
	SEC-KP1	Security Key Point #1	*To be proposed by the Contractor*
	SEC-KP2	Security Key Point #2	*To be proposed by the Contractor*
	RCR2	Release Consolidation Review #2	T1+12 months
	FQR	Factory Qualification Review	T1+14 months
	AR	Acceptance Review	T1+17 months = T2
	EOW	End of Warranty	T2+12 months TBC
	MSKP	Maintenance Service key point(s) (if maintenance is required)	Monthly/Quarterly during the maintenance duration

End of Document